A Decade in the Trenches of Cyberwarfare: Ukraine's Story of Resilience

A comprehensive review

February, 2024

FOREWORD

At the 2024 Kyiv International Cyber Resilience Forum, we're at a crucial point in history, reflecting on the lessons from the first global cyberwar which transformed our security understanding. It's an honor to gather in Kyiv, a beacon of digital resilience. Our meeting is vital to discuss the cyberwar's lessons, understand current cyber threats, and plan our future strategy.

Ukraine's unique cyber conflict experience offers invaluable insights for global defence strategies. This forum, a hub for collaboration, has been significantly shaped by the CCDCOE's contributions in understanding various aspects of cyber conflict, guiding our strategic responses.

We're committed to sharing knowledge and maintaining awareness, strengthening our resilience. This publication, based on Ukrainian research, offers deep insights into cyberwarfare and informs our discussions here. We focus on building resilience and strategic responses to enhance our collective defence and international cooperation, aiming for a more secure digital future for all.

Mart NOORMA

Director
NATO Cooperative Cyber
Defence Centre of Excellence
(CCDCOE)

Serhii DEMEDIUK

Deputy Secretary
National Security and
Defence Council of Ukraine

George DUBYNSKYI

Deputy Minister
Ministry of Digital
Transformation of Ukraine

Preface

It is with great pleasure and profound responsibility that I present to you this research report, titled «**A Decade in the Trenches of Cyberwarfare: Ukraine's Story of Resilience**». This report, a culmination of extensive research and analysis, has been crafted under the auspices of the Cyber Diia Team – a non-governmental, non-for-profit public association committed to fostering a resilient and secure digital future for Ukraine.

It is with great pleasure and profound responsibility that I present to you this research report, titled « A Decade in the Trenches of Cyberwarfare: Ukraine's Story of Resilience». This report, a culmination of extensive research and analysis, has been crafted under the auspices of the Cyber Diia Team – a non-governmental, non-for-profit public association committed to fostering a resilient and secure digital future for Ukraine.

At Cyber Diia, we bring together a dynamic coalition of technology companies, innovators, and experts, united in the vision of strengthening Ukraine's digital defences and advancing its technological prowess. In an era where digital threats loom large and cybersecurity becomes synonymous with national security, our mission has never been more critical.

This report is a testament to the indomitable spirit of Ukraine in the face of a decade-long cyberwarfare. It chronicles the complex and evolving landscape of digital threats, while celebrating the resilience and adaptability of our nation. Through this document, we aim to provide insights, reflections, and learnings that not only narrate the story of our struggle and resilience but also offer a blueprint for other nations grappling with similar challenges.

We believe this report will serve as a valuable resource for policymakers, cybersecurity professionals, academicians, and anyone interested in the intersection of cybersecurity, technology, resilience, law and governance.

With gratitude and hope for a secure digital future,

Dr. Andrii Paziuk
Research Project Lead

Executive Summary

Since the pivotal Euromaidan events of 2013, Ukraine has been at the forefront of a new battleground in global geopolitics: the cyber realm. The period from 2013 to 2021 witnessed an escalation of cyberwarfare, a precursor to the full-scale military invasion by Russia in February 2022[1]. This report delves into Ukraine's journey through a storm of cyber incidents, showcasing its resilience in an era where digital warfare is a critical component of geopolitical conflict.

The nature of cyber incidents that Ukraine endured varied, reflecting the sophistication and determination of attackers aiming to disrupt the nation's state functions and economy. Beginning with the strategic use of DDoS attacks during the Euromaidan Revolution, the cyber tactics employed by the aggressors evolved to include malicious code dissemination, sophisticated information gathering, and persistent intrusion attempts. These tactics were indicative of an intent to infiltrate, gather intelligence, and destabilize[2].

Strategically chosen, the sectors targeted in these attacks included government organizations, the IT sector, and the financial and commercial sectors. These attacks were calculated to maximize disruption, aiming to undermine the pillars of Ukraine's governance, economic stability, and digital infrastructure.

The methods employed in these cyber incidents were multifaceted. System compromises and malware distribution were prevalent, underscoring the intent to cause widespread disruption. The use of vulnerabilities and phishing attacks demonstrated a combination of technical skill and exploitation of human factors.
In response, Ukraine demonstrated remarkable resilience. Despite continuous attacks, critical sectors remained operational, adapting swiftly to the evolving cyber threats. This resilience was bolstered by international support, with global partners providing crucial cybersecurity assistance and intelligence.

The period from 2013 to 2021 highlighted the ever-evolving landscape of cyber threats. It underscored the need for a dynamic approach to cybersecurity, prioritizing the protection of key sectors like government and IT due to their significance for national security and societal functionality.

The experience of Ukraine in countering Russian cyber aggression offers a stark reminder of the central role of cybersecurity in modern conflicts. Ukraine's ability to withstand and respond to a diverse range of cyber threats underlines its strength in cyber resilience. To sustain this resilience, ongoing vigilance, international cooperation, and investments in cybersecurity are imperative. This approach ensures Ukraine's capability to confront and counter evolving digital threats in parallel with the physical challenges it faces.

PART I

Background

This report delves into the intense cyberwarfare in Ukraine, a central component of the broader Russian-Ukrainian war. This strife is not merely a territorial dispute but rather a manifestation of Russia's broader ambition to reclaim its sphere of influence following the dissolution of the Soviet Union. The Kremlin views Ukraine's independence and fortitude as significant obstacles to its aspirations, both within the post-Soviet space and on the global stage.

The conflict transcends conventional warfare and merges with the digital domain, exemplifying modern geopolitical conflicts where traditional and digital battlegrounds converge. The full-scale invasion of Ukraine in February 2022 marked a critical escalation in a series of aggressions Russia had been perpetrating since 2014, beginning with the annexation of Crimea and the destabilization of the Donetsk and Luhansk regions. This military aggression was mirrored by a parallel and equally potent cyberwarfare campaign, underscoring the changing nature of warfare in the 21st century[3].

Russia's approach to cyberwarfare is deeply rooted in a doctrine that melds information operations with cyber operations, drawing from Soviet-era disinformation tactics and public opinion manipulation[4]. These strategies have been adapted to the digital age, as evidenced by the evolution of Russian military doctrine, which increasingly emphasizes information warfare while strategically avoiding explicit references to cyber-specific terminologies, suggesting a deliberate ambiguity in Russia's official stance on cyberwarfare[5,6].

A key facet of Russia's cyber strategy is the use of Ransomware as a Service (RaaS), representing a significant shift in the cybercrime landscape. This model not only simplifies attack orchestration but also blurs the lines between state-sponsored activities and criminal enterprises. The symbiotic relationship between Russian state hackers and criminal groups is evident in cases where individuals linked to organizations like Evil Corp have engaged in activities benefiting the Russian state. Entities like the Internet Research Agency, known for their role in the 2016 U.S. elections, highlight the integral part of Russia's expansive propaganda machinery[7]. These agents of influence employ tactics ranging from social media manipulation to overt forms of media control within contested regions.

This report accomplishes three key objectives:

- **Mapping the Cyberwarfare Landscape Over the Last 10 Years:** It provides an in-depth analysis of the cyberwarfare landscape, highlighting key events, tactics, and strategies employed over the past decade.

- **Correlating Physical and Cyber Attacks:** The report establishes a correlation between physical military actions and cyberattacks, illustrating how these two realms of warfare are increasingly intertwined in modern conflicts.

- **Researching the Evolution of Cyberwarfare:** A critical focus of the report is to trace the evolution of cyberwarfare tactics, technologies, and procedures, particularly examining how these have been refined and adapted by Russia during the conflict in general and the active phase of the war in particular, drawing conclusions about the future tools, likely to be employed.

The technique refinement, sector targeting trends, and adaptability of Russian cyber operations are integral components of their strategic approach to cyberwarfare[8]. Understanding these trends is vital for cybersecurity professionals, organizations, and governments in enhancing cyber defences, mitigating risks, and developing policies to protect critical infrastructure, data, and national security in a digitally interconnected world.

PART II

Pro-Russian Cyber Actors and Agents of Influence

In this digital arena, Russia has established specialized units within its intelligence apparatus, particularly the GRU, to conduct sophisticated cyber operations[9]. These units are tasked with a range of activities, from direct cyberattacks to more subtle forms of information warfare. The involvement of various branches of Russian intelligence, including the FSB and SVR, further complicates the landscape. They engage in cyber operations, often leveraging the expertise of private contractors and hackers, creating a shadowy web of state and non-state actors (see **Figure 1**).

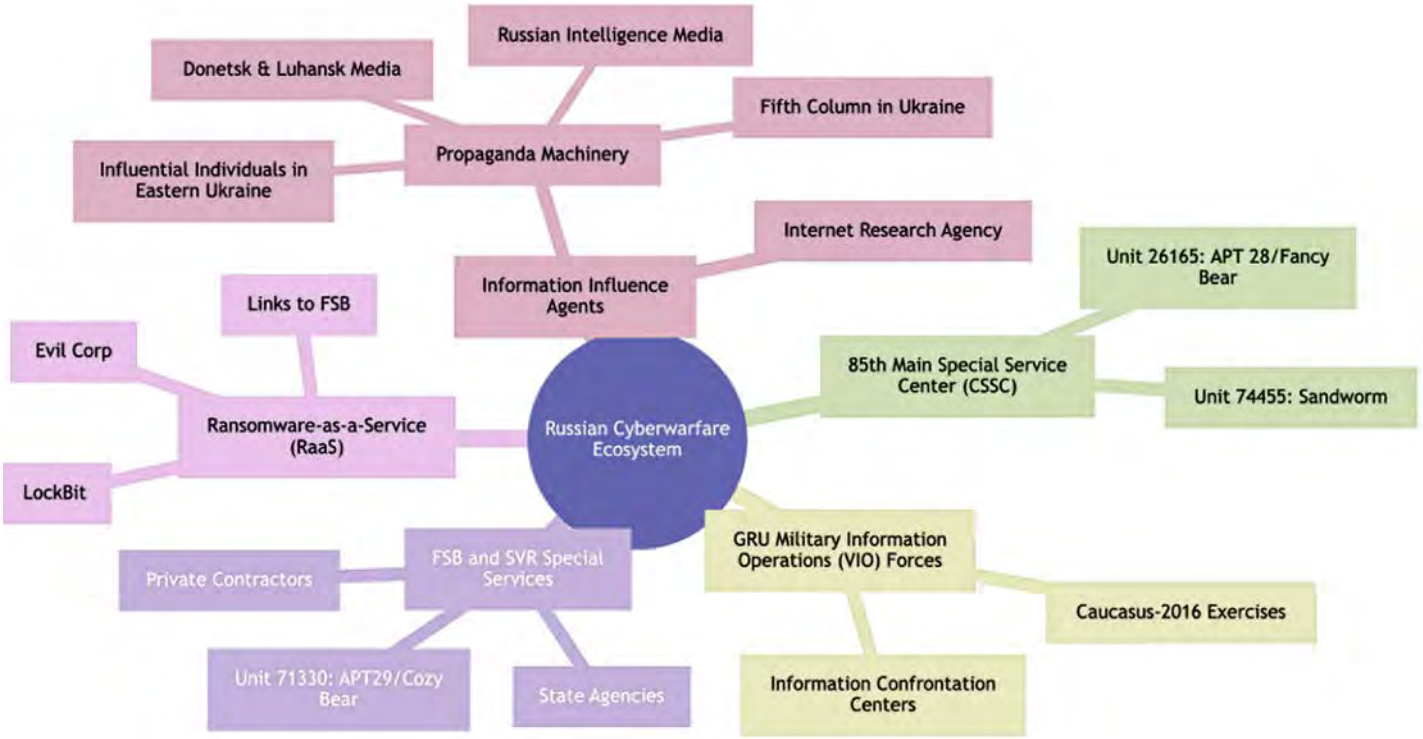


Figure 1 Russian Cyberwarfare Machinery

The international community has responded to these tactical moves with sanctions targeting Russian entities implicated in major cyberattacks, such as NotPetya and SolarWinds. These sanctions demonstrate the global recognition of the severity and far-reaching impact of Russia's adversarial cyber activities as well as provide evidence of robust international response.

As we examine the trajectory of Russian cyber tactics, technologies, and procedures over the past decade, it becomes evident that the Russia-Ukraine conflict is a seminal case in understanding the evolution of cyberwarfare. This conflict is not just about territorial disputes but a broader struggle involving the kinetic, informational, and cyber-technological realms. The insights gained from this conflict are crucial in shaping defensive and offensive strategies to counter multifaceted threats in an increasingly interconnected world.

Russian military information operations, or VOI (Russian acronym for «Military Information Operations»), established by the GRU in 2014, first tested «information warfare» during the «Caucasus-2016» exercises against a hypothetical enemy[10]. This involved the Main Operational Directorate of the General Staff, information operations troops, electronic warfare forces, information counteraction centers in military districts, and experts from the state secret protection service. The formation of these information warfare troops within the GRU was officially announced in February 2017[11].

The cyber activities of the 85th Main Special Service Center (CSSC) of the General Staff of the Russian

Armed Forces (GRU) can be directly linked to military activities. Its officers serve in military units 26165 (Strontium or APT 28/Fancy Bear, Pawn Storm) and 74455 (Iridium or Sandworm)[12]. Other Russian intelligence agencies, the FSB, and the SVR (see fig.1), handle specialized information warfare tasks using various actors such as military units (e.g., unit 71330, APT29/Cozy Bear), state agencies, and private contractors (proxies) specializing in hacking services and information-psychological operations. Russian intelligence services employ various hacking groups, disguising their activities and complicating the legal attribution of cybercrime.

The multitude of names for these hacking groups can be attributed to various factors - ideological, economic, and legal. However, the «self-preservation» aspect cannot be ignored since their activities are monitored by security services and law enforcement agencies of different countries, with sanctions and criminal prosecution from countries like the USA being a deterrent, forcing them to resort to disguising and other methods of concealing criminal activities. In March 2018, the US Department of the Treasury's Office of Foreign Assets Control (OFAC) sanctioned the Russian Federal Security Service (FSB), Main Intelligence Directorate (GRU), and four GRU officers (already listed under Executive Order 13694 in connection with US election interference), and two more GRU officers for «destructive cyber-attacks.» These attacks included the 2017 NotPetya virus attack, which the US Treasury Department called «the most destructive and costly cyber-attack in history.[13]»

In April 2021, under the new Executive Order 14024, OFAC sanctioned six Russian technology companies for supporting the GRU, SVR, and FSB. Announcing the sanctions, the US Treasury Department noted that Russian intelligence services «have conducted some of the most dangerous and disruptive cyber-attacks in recent history, including the SolarWinds cyber-attack [affecting victims] in the financial sector, critical infrastructure, government networks, and many others.»

The increase in the use of Ransomware-as-a-Service (RaaS) marked a significant shift in the structure of cybercrime. Large organized criminal groups, such as Evil Corp and LockBit from Russia, previously developed malware and infrastructure independently, now have the opportunity to purchase advanced services from specialized providers. This simplifies the organization of attacks and reduces their cost. At the same time, some of these groups are closely linked to Russian intelligence services, creating a symbiotic relationship between state and private interests in cybersecurity – Russian state hackers, focused on stealing foreign secrets, can use ransomware to mask their espionage activities. They also may recruit talents from criminal groups. For example, Maxim Yakubets from Evil Corp worked for the FSB and carried out tasks for the Russian state, according to a US indictment.[14]In April 2021, the US Treasury Department's statement introducing new sanctions against Russia explicitly established a link between the FSB and cybercriminals using ransomware. It was stated that the FSB not only supports but also assimilates criminal hackers[15].

Among Kremlin's agents of information influence, the Internet Research Agency, founded by (former) head of the Wagner PMC Yevgeny Prigozhin was involved in interference in the 2016 US elections. Often referred to as a «troll factory» or «troll farm,» this group focused on disinformation through various social media channels. In 2018, the US government indicted the agency and its employees for their attempts to interfere in the presidential elections[16].

The Russian propaganda machine follows Soviet tactics and methods. The propaganda «ecosystem» includes four main categories of influence agents: (i) the Kremlin's so-called «fifth column» in Ukraine, (ii) media of the self-proclaimed Donetsk and Luhansk People's Republics, (iii) Russian media connected with intelligence, and (iv) influential personalities and military correspondents, mainly in eastern Ukraine. Following the invasion, «localized» news sites, newly launched media, and organized groups – some linked to known influence agents – promoted pro-Russian imperial narratives. The Security Service of Ukraine exposed numerous anonymous Telegram accounts, believed to be operated by the GRU, conducting anti-Ukrainian agitation in cities critical in the initial period of the war. [17]

The extensive disinformation campaign waged by Russia during the ongoing conflict with Ukraine has reached significantly new levels during the active phase of war. Central to this campaign are efforts to undermine Ukrainian sovereignty and legitimacy, portraying Ukraine as a neo-Nazi state and accusing it of committing genocide against Russian speakers. This narrative, aggressively pushed through various channels, including state media and internet brigades, aims to justify the invasion and vilify NATO's role in the region.

In response, Ukraine has been actively counteracting Russian weapons of mass influence, which primarily target disinforming Ukrainian citizens as well as citizens of Ukraine's allies. While Ukraine has also been accused of using propaganda, such as the over-optimistic casualty reports and patriotic stories like the «Ghost of Kyiv,» these efforts are comparatively limited. The primary focus of Ukraine's counter-disinformation efforts has been to debunk Russian narratives, highlighting the falsity of claims regarding Ukrainian

Nazism, NATO aggression, and genocide in Donbas. This ongoing battle in the information space is a critical aspect of the wider conflict, with both sides seeking to influence public opinion and international perception of the war.

Several Ukrainian agencies and organizations have been actively involved in debunking Russian disinformation and propaganda efforts. Key among them are: **The Ministry of Digital Transformation of Ukraine, The Ministry of Information Policy of Ukraine, The Center for Strategic Communications and Information Security, The Security Service of Ukraine (SBU), The Ministry of Foreign Affairs of Ukraine, The Office of the President of Ukraine. Additionally, Ukrainian Fact-Checking Organizations** such as StopFake, are crucial in identifying and debunking false information circulated in the media and online platforms. While disinformation is an integral part of digital warfare, in this report, we will concentrate on adversarial cyber activity rather than on disinformation. Our research will focus on the time period from 2013 to 2023, depicting trends and adversarial dynamics.

For the purposes of our study, we will partition the analysis into two parts: (a) The Era of Turmoil and Transformation and (b) The Full-Scale Invasion. The time period from 2013 to 2021 encapsulates the significant political, social, and military upheavals that Ukraine experienced during this period, starting with the Euromaidan protests and the subsequent annexation of Crimea by Russia in 2014, the military conflict in Eastern Ukraine, and leading up to the ongoing challenges and reforms faced by the country up to and including 2021. This era is marked by a significant shift in Ukraine's geopolitical orientation, internal political dynamics, and its struggle for sovereignty and territorial integrity. The period from 2022 to 2023 in Ukraine, is characterized by the escalation of the conflict and the full-scale invasion by Russia. It reflects the significant increase in hostilities and the Ukrainian people's determined response to the challenges posed by the Russian invasion. It showcases not only the military aspect of the war but also the social, political, and economic resilience demonstrated by Ukraine in the face of overwhelming challenges. During this time, Ukraine's struggle for sovereignty, territorial integrity, and its path towards the European integration became more pronounced and received global attention.

PART III

The Era of Turmoil and Transformation of 2013-2021

The timeline with essential cyberwarfare events[18] between 2013 and 2021 is depicted on **Figure 2** and described below.

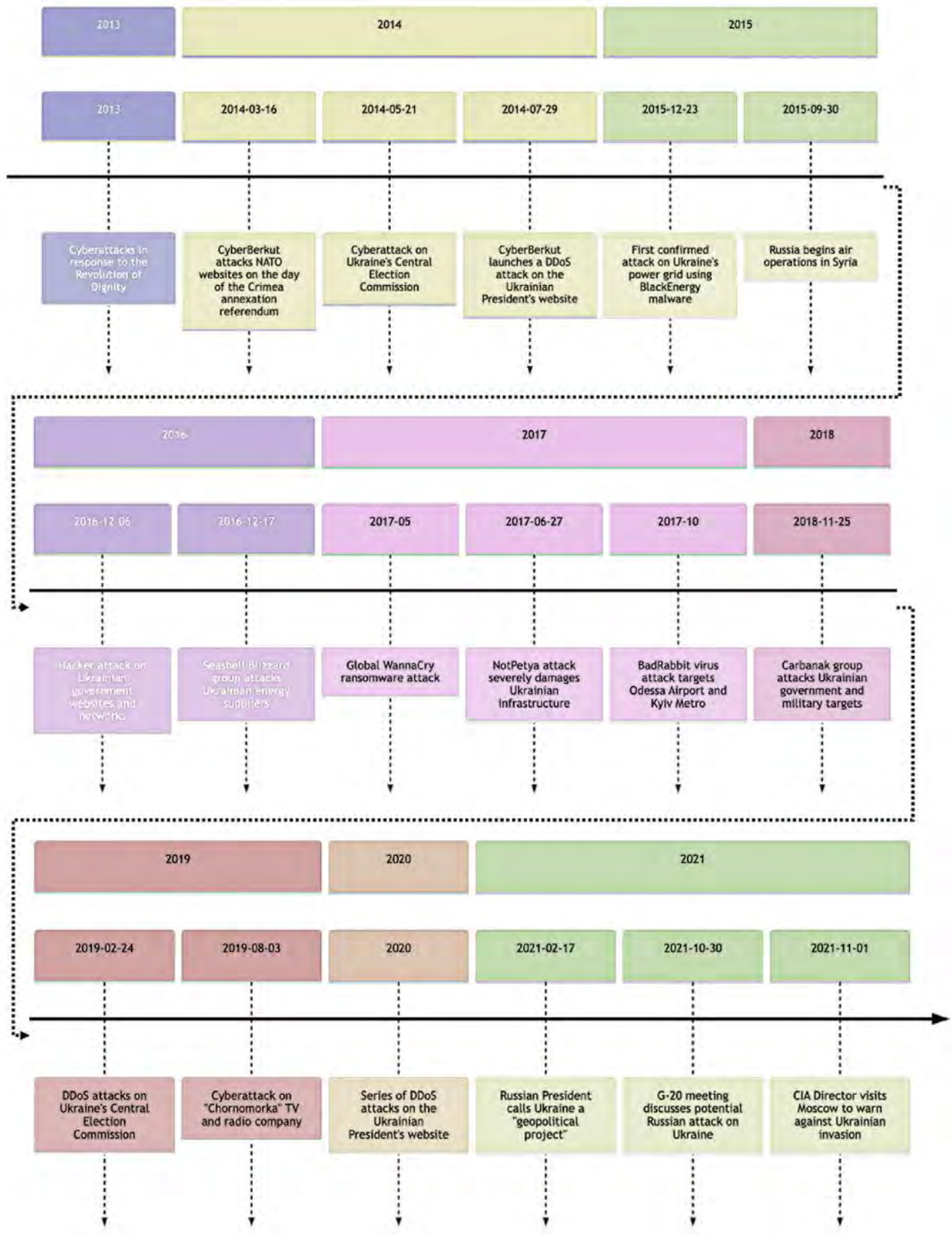


Figure 2 Timeline of Cyber Attacks between 2013 and 2023

2013: Response to the Euromaidan Revolution

In response to the Euromaidan Revolution of 2013[19], which led Ukraine to move closer to the European Union and NATO, Russia employed cyberattacks to paralyze, discredit, and distract the political opponents of the pro-Russian President Yanukovych. This period was marked by significant use of cyber tactics within the broader context of a hybrid approach to warfare. DDoS attacks were used on telecom providers to disrupt the communication of demonstrators, especially during the violent crackdown on protestors in Kyiv's Independence Square (Maidan Nezalezhnosti) in November 2013. These attacks were aimed at impeding the movement's activities and communication capabilities. During the operation in Crimea, Russia integrated electronic warfare, cyber operations, and information campaigns with kinetic actions. Key events included Russian military interference in Ukrtelecom's optical fiber channels, disruption of communications, mobile phone jamming of Ukrainian parliamentarians, government website shutdowns, and DDoS attacks on Ukrainian national security agencies and news outlets.

2014: Escalation and Expansion

On March 16, 2014, the day of the referendum on Crimea's annexation, a Russian hacking group linked to the GRU, CyberBerkut, attacked NATO websites. On May 21, 2014, the same group carried out a cyberattack on the «Elections» information system of Ukraine's Central Election Commission, disrupting key network nodes and other system components. The software displaying current vote counts malfunctioned for nearly 20 hours. On the day of the elections, May 25, mere minutes before polling stations closed, the attackers displayed a vote count on CEC servers indicating victory for a far-right presidential candidate. This disinformation was then broadcasted on Russian TV as the 'Yarosh Card.' CERT-UA found that the first access to the CEC website with this page's address came from an IP address within the range of the Russian channel ORT. On July 29, 2014, the official website of the President of Ukraine was targeted in a powerful DDoS attack by CyberBerkut, rendering it inaccessible for several hours.

2015: Infrastructure Attacks and International Context

On December 23, 2015, the first confirmed attack on a power system occurred when Russian hackers used the BlackEnergy trojan to attack the control systems of the regional electricity hub «Prykarpattya Oblenergo.» This led to the shutdown of about 30 energy substations, leaving 230,000 residents without electricity for 1-6 hours. The attack also affected other regional energy hubs, particularly, «Chernivtsi Oblenergo» and «Kyiv Oblenergo,» but with less severe consequences. The cyberattack involved initial infection through phishing, control system hijacking, IT infrastructure disruption, server and workstation data destruction, and attacks on call center phone numbers to deny service. On September 30, 2015, Russia began an aerial operation in Syria, striking cities in the Homs province. This step was part of a broader military campaign to support the Syrian government. Reports in the media on November 27, 2015, suggested Kremlin's intentions to use the Syrian conflict in negotiations with the West, potentially including the «Ukrainian question» as part of a larger geopolitical deal. However, Ukrainian leadership actively responded to these reports, debunking and highlighting them on the international stage, effectively making their realization impossible.

2016: Increasing Complexity and Impact

On December 6, 2016, a hacker attack on government websites and networks caused delays in budget payments. The attack utilized the KillDisk virus and the BlackEnergy trojan. On December 17, 2016, the Seashell Blizzard group employed high-level techniques to attack energy suppliers, attempting to trigger automatic protection systems and shutdown substations. These multi-phase attacks included spear-phishing, data gathering, network mapping, data extraction, control system hijacking, and the installation of malicious software. One power station near Kyiv was successfully shut down, affecting approximately 600,000 households, impacting every fifth resident of Kyiv. The Ukrainian energy company Ukrenergo responded by switching to manual control and restored power within 75 minutes. This demonstrated the capability and readiness to use cyber means for informational-psychological impact on the civilian population. This was again demonstrated six years later, in an attack on April 8, 2022, using an updated version of the same virus attributed to the Seashell Blizzard group in 2016. The 2022 attack remotely disconnected about 30 substations in western Ukraine, affecting 230,000 people. Ukrainian experts neutralized the attack, switching to manual control within 360 minutes. Before the advisory referendum in the Netherlands on the EU-Ukraine Association Agreement, Russian sources disseminated a video supposedly showing «Azov» fighters burning the Dutch flag. The video was exposed as a Russian fake. On April 6, 2016, 61% of voters participating in the referendum voted against the association agreement with the EU.

2017: Global Impact and National Resilience

In May 2017, the global WannaCry ransomware attack was a worldwide cyberattack using the WannaCry cryptoworm, targeting computers running Microsoft Windows, encrypting data and demanding ransom in Bitcoin. It spread through the EternalBlue exploit. The NotPetya virus attack that began on June 27, 2017, severely damaged Ukrainian infrastructure, targeting the financial system, government networks, energy companies, and even the radiation monitoring system at the Chernobyl Nuclear Power Plant. Although the main target was Ukraine's critical infrastructure, NotPetya spread globally, impacting logistics, healthcare, and other sectors. This malicious software had a global impact, affecting 65 countries and about 50,000 systems, including companies like FedEx, Maersk, and Merck in Europe and the USA, causing damages exceeding 10 billion US dollars. This attack is linked to the Sandworm group, under the influence of the GRU.
The link between WannaCry and NotPetya attacks is notable. The NotPetya virus was complex and multi-staged, starting with the use of the Petya worm family that infected systems through the EternalBlue vulnerability. TeleBots, connected to BlackEnergy-Sandworm and responsible for NotPetya, had previously attacked financial institutions and critical infrastructure in Ukraine using KillDisk. Hackers also gained unauthorized access to networks through VPN tunnels and used various backdoors and tools for network propagation.
Both WannaCry and NotPetya featured common elements, including the use of the EternalBlue exploit to attack Microsoft's Server Message Block (SMB) protocol. NotPetya, in addition to EternalBlue, employed another tool, PsExec, for more effective network propagation[20].

A key element of the attack was file encryption using AES-128 and RSA-1024 algorithms, and for servers running other operating systems, RSA-2048 and AES-256 were used. This attack was characterized by its scale, complexity, and variety of methods for achieving objectives, including the application of encryption, backdoors, and exploitation of software vulnerabilities. These attacks caused major disruptions in the operations of significant global organizations across various sectors, impacting British, Ukrainian, and American firms. This underscores the trend of cybercriminals targeting large organizations, causing widespread disruptions. The challenge of detecting and defending against such attacks poses a significant challenge to existing antivirus programs, requiring continual updates and adaptations of their protection mechanisms.
In October 2017, the BadRabbit virus attack, likely linked to the developers of NotPetya, targeted the Odessa Airport and the Kyiv Metro. The primary goal of the attack was to gain access to confidential and financial data of Ukrainian companies, using the attack itself to mask and distract attention.
2017 was undoubtedly a turning point for cybersecurity in Ukraine. It was the largest cyber intrusion into Ukrainian systems, leading to a rapid growth in Ukraine's cybersecurity market. International companies participated in both mitigating the effects and in a wide range of offerings to protect state and private systems from external interventions. The demand for security services lasted almost a year and contributed to the growth of the private sector, including Ukrainian cybersecurity companies.

Civil society launched numerous initiatives to develop cybersecurity legislation, spread, and improve industry-level experience exchange. The necessary basic law «On the Fundamental Principles of Cybersecurity in Ukraine» was adopted. This law helped identify centers of responsibility and distribute powers in Ukraine's cybersecurity sphere. The establishment of the National Cybersecurity Coordination Center at the National Security and Defence Council of Ukraine (NSDC) was another important step in strengthening the country's cybersecurity by coordinating the efforts of various state bodies and the private sector in the field of cybersecurity.
Throughout this time, there was a problem with coordinating communication between state bodies and the public: each state institution had its comments, and they were not always professional. Starting in the fall of 2017, state bodies began the practice of covering cybersecurity issues with an analytical component. As cyber specialists and their experience in various state structures developed, information about cyberattacks became more systematic, regular, and expert.

2018: Targeted Attacks and Information Warfare

In 2018, the Russia-sponsored Carbanak group carried out coordinated cyberattacks on Ukrainian government and military targets before and during the incident of capturing Ukrainian ships and sailors on November 25, 2018. The attacks aimed to steal information crucial for planning the operation. The malicious software Pterodo used in the phishing attack allowed for data or email theft.
On November 26, after Russia captured Ukrainian vessels, a second coordinated Carbanak attack targeted key Ukrainian government and military facilities to disrupt their operations.

2019: Election Interference and Media Attacks

On February 24 and 25, 2019, Ukraine's Central Election Commission was subjected to DDoS attacks, which experts concluded were carried out from Russian territory. These attacks aimed to block user access to information about preparations for the presidential elections in Ukraine. Using «http flood» technology, which generated constant requests, the attackers complicated the operation of the CEC's information system, preventing ordinary users' access. This cyberattack was organized using a network of websites based on an outdated version of the WordPress system, allowing hackers to generate voluminous requests without the site owners' knowledge. On August 3, 2019, the Security Service of Ukraine, in collaboration with the representatives of the «Chornomorka» broadcasting company, restored the operation of the broadcasting server after a cyberattack. The attack involved blocking and neutralizing key management elements and backup systems of the broadcasting company through malicious software. «Chornomorka,» previously located in Crimea and relocated to Kyiv after the annexation of the peninsula, actively covered topics of the Russian-Ukrainian conflict, likely prompting this cyberattack as part of the information war.

2020: Increasing Political Tensions

From the end of 2019 through 2020, the website of the President of Ukraine experienced a series of DDoS attacks, likely related to the policy of the non-pro-Russian Ukrainian president. These attacks appeared to be an attempt by the Kremlin to limit the spread of the Ukrainian perspective on meetings and negotiations, particularly a phone conversation between the Presidents of Ukraine and Russia on resolving the conflict in Donbas and the Minsk Agreements. The websites of the Presidents of Ukraine and Russia presented «somewhat different versions of the conversation.» These attacks might also have aimed to demonstrate the power of Russian intelligence services and their loyalty to the country's leadership, as well as to diminish the influence and political rating of the Ukrainian president. This was part of a strategy to emphasize dominance in the information sphere and geopolitical confrontation. In October 2020, Russian cyberattacks aimed to compromise local voter registries in Ukraine. These attacks had two main objectives: to hinder the conduct of elections and to collect personal data of voters. The data obtained, including demographic information from the registries, could potentially be used by the Russian authorities to organize pseudo-referendums in the occupied Kherson and Zaporizhzhia regions in September 2022. This indicates strategic planning and the use of collected data for political manipulation and interference in Ukraine's internal affairs.

Early 2021: Preparation for Conflict and Western Support

Actors belonging to the Russian side began preparing for conflict as early as March 2021, targeting organizations in Ukraine and allied countries. This included efforts to penetrate systems to gather intelligence on Ukraine's military potential and its external alliances. By mid-2021, they expanded their activities to attack supply chain providers in Ukraine and NATO countries for broader access. On February 17, 2021, the President of the Russian Federation referred to Ukraine as a «geopolitical project,» claiming that Russia is being forced to pay for this project. He also emphasized the importance of the Nord Stream 2 gas pipeline, underscoring the significance of stable Russian gas supply to Europe. In 2021, in view of the aggressive plans already known to Western intelligence, Ukraine began actively preparing for war, receiving significant military assistance from its allies.

Evolution of Russian Cyberwar Tactics between 2013 and 2021

Analyzing the evolution of Russian cyberwarfare tactics (see **Figure 3**) from 2013 to early 2021, several key trends and strategic shifts become apparent:

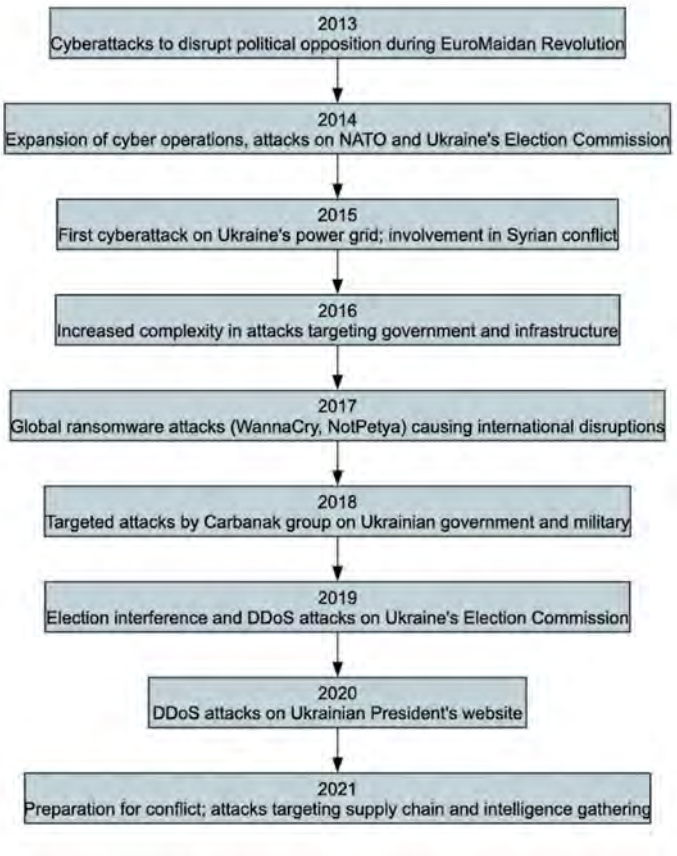


Figure 3 Evolution of Russian Cyberwar Tactical Apparatus

• Integration with Geopolitical Strategy: Initially, Russia's cyber operations appeared to be more reactive and opportunistic, primarily focused on immediate objectives like disrupting communication during the Euromaidan Revolution. Over time, these operations became more integrated with Russia's broader geopolitical strategy. This is evident in the alignment of cyberattacks with significant political and military events, such as the annexation of Crimea and the Kerch Strait incident. By 2021, cyber operations were a key component of Russia's preparation for potential conflict, illustrating a **strategic shift from opportunistic disruption to calculated, long-term planning.**

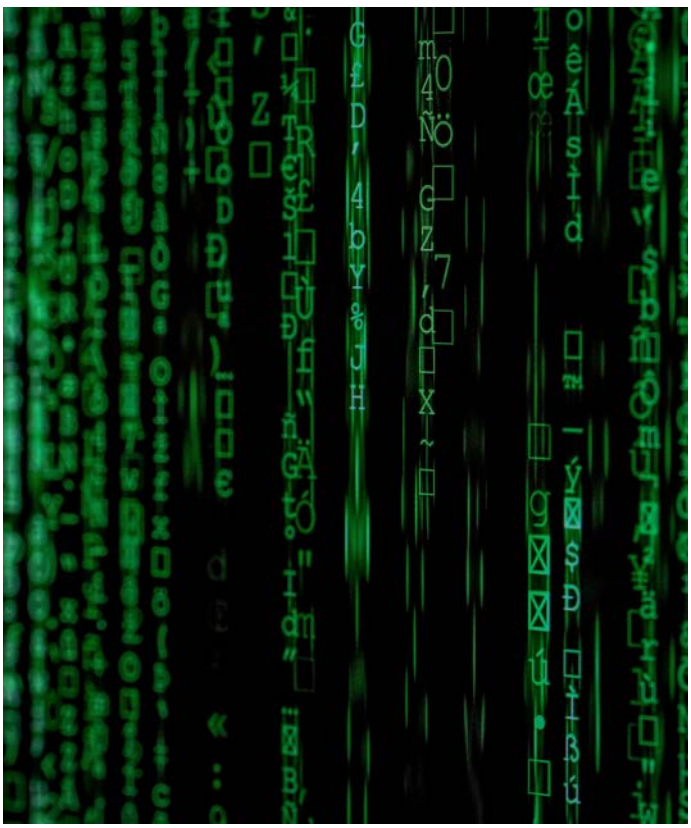
• Sophistication and Scope of Attacks: Early attacks were characterized by their relatively straightforward nature, such as DDoS attacks. However, over the years, there was a clear trajectory towards more sophisticated adversarial techniques. This includes the use of complex malware like BlackEnergy and NotPetya, intentionally targeting not just Ukrainian entities but having global repercussions. The progression from basic disruption tactics to advanced, multi-stage attacks involving data destruction and system hijacking indicates a **significant enhancement in both technical capability and strategic thinking.**

• Shift from Conventional to Hybrid Warfare: The evolution of Russian cyber tactics is a textbook example of the shift from conventional warfare to hybrid warfare. Cyber operations became an integral part of Russia's hybrid warfare strategy, blurring the lines between military and non-military methods. The use of cyberattacks to complement kinetic military operations, as seen in the Crimea and Donbas conflicts, underscores this shift. This integration signifies a **more holistic approach to warfare, where cyber operations are not standalone efforts but part of a larger, multifaceted adversarial strategy.**

• Global Impact and Escalation of Stakes: Initially, Russian cyber operations were regionally focused, primarily targeting Ukraine. However, the global impact of operations like NotPetya marked a significant escalation. This global reach, exemplified by the widespread disruption caused by NotPetya, reflects **an understanding of the interconnected nature of modern societies and economies.** It also demonstrates a willingness to escalate the stakes, affecting nations and organizations not directly involved in the immediate geopolitical conflict.

• Adaptation to International Responses: Throughout this period, Russian cyber tactics also evolved in response to international efforts to counter cyber threats. This includes adapting to cybersecurity measures employed by Ukraine and its allies. The continuous evolution of these tactics in the face of **growing international awareness and defence measures indicates a dynamic approach to cyber operations, constantly seeking to exploit new vulnerabilities and adapt to changing technological landscapes.**

The overarching narrative from 2013 to 2021 shows a clear trajectory from localized, opportunistic cyber activities to globally impactful, strategically integrated adversarial and disruptive operations. This evolution reflects not just an advancement in technical capabilities, but also a strategic recalibration to use cyber operations as a tool of statecraft and a component of broader geopolitical strategy.



PART IV

Full-Scale Invasion of 2022-2023

Full-scale Invasion period signified several notable shifts in Russian adversarial cyber tactics [6] as well as further demonstrated Ukraine's cyber resilience as depicted on **Figure 4**.

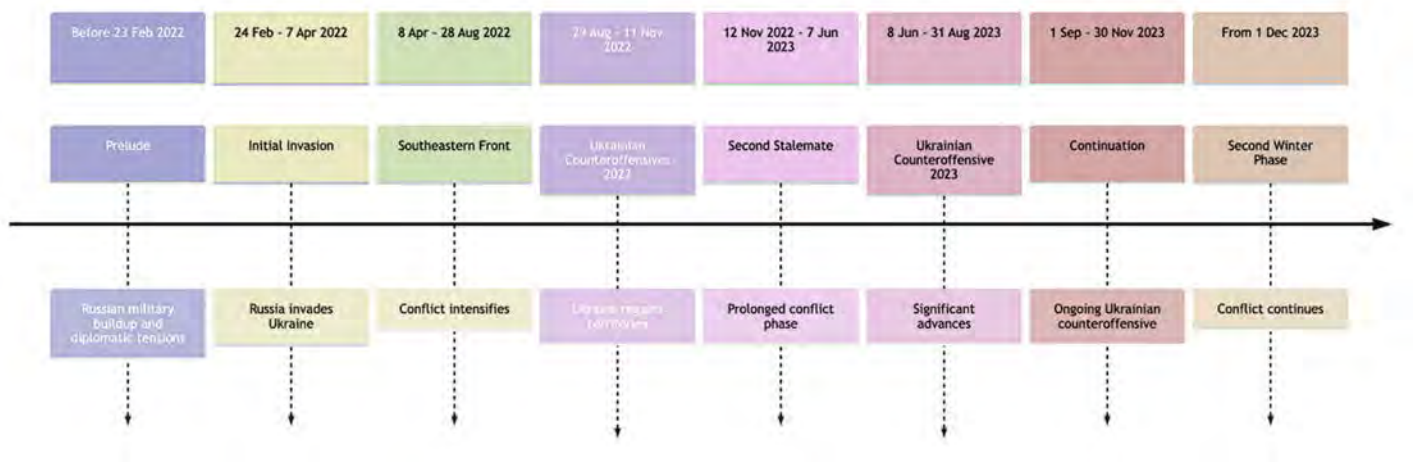


Figure 4 Phases of Russian Full-Scale Invasion in 2022-2023

4.1 Late 2021 and the Prelude to Full-Scale Invasion

In 2021, the prelude to the active phase of traditional war as well as cyberwar in Ukraine began unfolding in a manner reminiscent of a carefully orchestrated play, with actors on the Russian side preparing the stage as early as March. Their primary objective appeared to be infiltrating systems in Ukraine and allied countries for intelligence on military capabilities and external alliances. By mid-2021, their operations had escalated to attacks on military supply chain providers in Ukraine and NATO countries, aiming for broader access. By the end of 2021, the gravity of the situation was evident during the G-20 meeting in Rome on October 30-31, 2021, where President Biden discussed a potential attack on Ukraine with leaders from the UK, France, and Germany. This was followed by a significant visit by the CIA Director William J. Burns to Moscow on November 1, 2021, to warn the Kremlin of the severe consequences of an invasion*.

Meanwhile, the cyber landscape was also heating up. On May 7, 2021, the Colonial Pipeline in the USA suffered a cyberattack by the DarkSide group, leading to heightened cybersecurity measures in the US . Back in Ukraine, the Cyber Incident Response Center documented 41 million suspicious events aimed at unauthorized interventions in information systems in 2021 alone, processing 160,000 critical events and registering 147 cyber incidents [24]. As 2022 dawned, the prelude to the full-scale military invasion was marked by a series of cyberattacks as part of a broader strategy of pressure and destabilization. The BleedingBear attack on January 13, 2022, targeted about 22 state bodies and 70 Ukrainian websites. The defacements condemning Ukrainian nationalism hinted at Russian origins. The DDoS attack on February 15, 2022, and the repeat BleedingBear attacks on key Ukrainian websites on February 23, 2022, exemplified the intensifying cyber aggression[25].

With the onset of the full-scale military invasion on February 24, 2022, the cyber realm became a key battlefield. The attack on the Viasat satellite provider on February 24, 2022, an hour before the full-scale invasion, marked a critical event in the conflict, highlighting the role of cyber operations in modern warfare. The use of the Acid Rain virus to disrupt communication modems across Europe and the Middle East had far-reaching impacts, including disruptions in air turbine operations in Germany and the internet accessibility across several European countries[26]. In response, Ukraine quickly restored communication using alternative satellite networks like Inmarsat and SpaceX, demonstrating the resilience and adaptability in the face of cyber threats[27]. The Viasat incident, akin to the NotPetya cyberattack, stood out for its scale and indiscriminate

*See https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/ for more details.

nature, affecting civilian objects and infrastructure beyond Ukraine's borders, potentially qualifying as war crimes under the jurisdiction of the International Criminal Court.

The attack on the Kyiv Regional State Administration website (among others), coupled with a phishing campaign believed to be from Belarus, underlined the multifaceted nature of this digital war. The Microsoft Threat Intelligence Center noted a significant number of wiper programs in more than a dozen networks in Ukraine, with almost 40 separate destructive attacks identified.

The cyber and armed attacks on physical infrastructure, particularly, on energy facilities, including gas transportation systems and nuclear power plants, demonstrated the severe threats to both Ukrainian civilians and neighboring countries' infrastructure. A collaborative effort by Ukrainian state cyber defence, Microsoft, and ESET averted a cyberattack by the Sandworm APT group on April 12, 2022. This incident, similar to the 2016 Industroyer (i.e., Crashoverride) malware attack in Kyiv, highlighted the evolving nature of cyber threats and the importance of collaborative defence strategies.

The official report by Ukraine's State Service for Special Communication and Information Protection for 2022 provided an analytical overview and conclusions on the changing tactics of cyberattacks in the latter half of 2022. It noted that a significant portion of pre-war cyber operations aimed at controlling strategic resources did not achieve their goals, with about 20-30% of cyberattacks being destructive, while the majority (70%) were complex «spear-phishing» operations for cyber espionage. The most active group in the second half of 2022 was Gamaredon, associated with the FSB, specializing in data theft and numerous intelligence operations. The 74455 unit of the Main Intelligence Directorate (GRU, known also as Sandworm or UAC-0082), also showed increased activity in destructive operations, using wipers and other cyberattack means.

The European Parliament's resolution on March 1, 2022, called for the immediate and full implementation of all decisions to strengthen the EU's contribution to enhancing Ukraine's defence capabilities, including in cybersecurity. The resolution also urged the EU, NATO, and other interested partners to intensify assistance to Ukraine in the field of cybersecurity.

The evolution of tactics, techniques, and procedures in cyber operations, as well as the response of cyber defence forces during the ongoing armed conflict, suggests a dynamic and challenging cyber landscape.

The initial phase of offensive cyber operations in early 2022 witnessed the use of the WhisperGate wiper by the DEV-0586 military unit.

However, the effective response of Ukrainian cyber defenders and the global technology community highlighted the importance of adaptability and rapid response to the changing threat landscape. The collaborative approach in cyber defence, a public-private cyber collaboration, appears to have thwarted Russian cyber efforts, forcing the enemy to develop new malware. The regular emergence of new wiper variants indicates ongoing development of cyber capabilities, underscoring the importance of sustained attention and collaborative defence strategies in the context of cyberwarfare.[29]

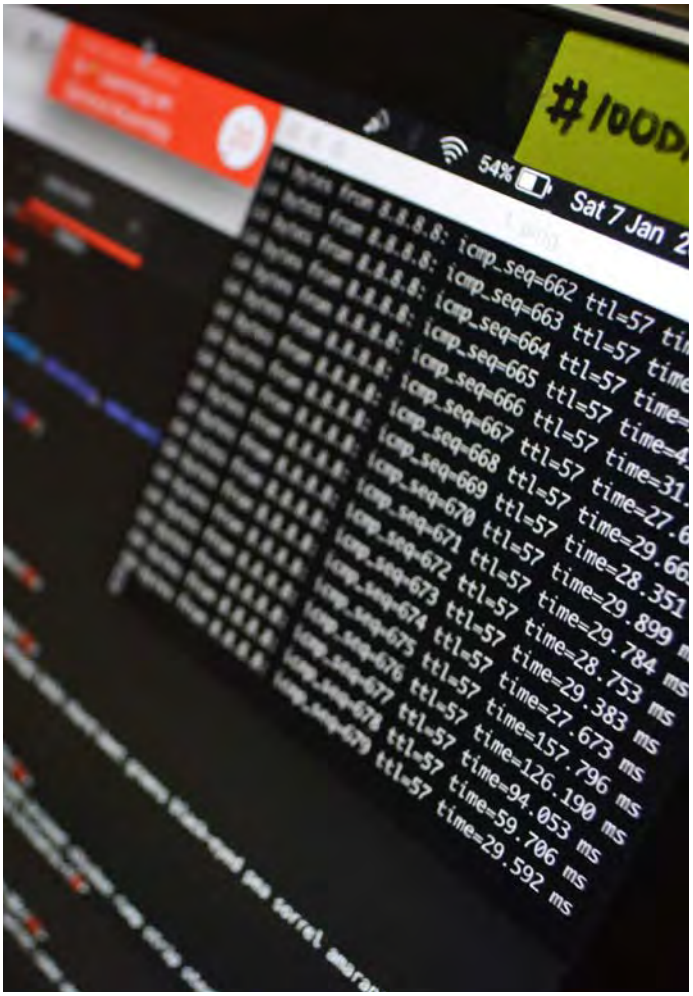
In December 2022, Russia dismissed international condemnation of these actions, stating the continuation of attacks on Ukraine's energy infrastructure. These actions reflect an escalation of aggression and determination in Russia's military campaign against Ukraine. The cyberattack on Kyivstar (Ukrainian telecommunications company, a mobile phone operator) on December 12, 2023, was a significant disruption in Ukraine's communication landscape. At 5:26 AM, Kyivstar detected unusual activity in their computer network, and by 6:30 AM, it was clear that the company was under a powerful cyberattack targeting its core network. The attack left more than 20 million subscribers without mobile communication and internet, also affecting government resources and emergency services. The aftermath involved companies like Microsoft, Cisco, Ericsson, and Ukrainian cyber experts from the SBU, State Special Communication, and CERT-UA.[30] Kyivstar reported restoring mobile internet across Ukraine on December 15, 2023, and fully recovering

all basic services affected by the cyberattack on December 21, 2023[31,32]. The responsibility for the attack was claimed by the Russian hacking group «Solntsepek», later confirmed by the SBU as a hacking unit of the GRU.[33]

The cyberattack on Kyivstar was accompanied by an information-psychological operation aimed at stirring political unrest within the country. Russian agents of influence used this incident to launch false narratives in Telegram channels about blocking communication and the internet in Kyiv for a «state coup» by the «party of peace» led by General Zaluzhny, aiming to oust the "Zelensky regime".
The attack should be viewed in a broader geopolitical context, especially considering the corporate changes in Kyivstar and VEON Ltd. In November 2023, VEON Ltd., the sole corporate rights owner of Kyivstar, announced the joining of former U.S. Secretary of State Mike R. Pompeo was appointed to the Board of Directors of Kyivstar as an independent non-executive director. VEON's commitment to Ukraine, its revival, and reconstruction were highlighted by a $600 million investment over the next three years and the launch of the «Invest in Ukraine NOW» program. VEON also announced its exit from the Russian market, completing the relevant deal on October 9, 2023.[34] The changes in Kyivstar's corporate structure occurred against the backdrop of the arrest of 47.85% of the company's corporate rights, belonging to a sanctioned Russian oligarch, and the consideration of the nationalization of Kyivstar, which Pompeo referred to as a strategic mistake[35]. The cyberattack on Kyivstar, less than two weeks after these publications, was atypical considering the extremely short time frame for its execution. Clearly, the cyber-attack was planned in advance, and only the timing for its implementation was chosen. It is the largest in scale since the NotPetya attack and has caused significant economic damage due to the suspension of banking transactions and business operations, loss of investment attractiveness, theft of sensitive personal account information and telecommunication data records of millions of subscribers of this operator and their correspondents in telephone conversations, as well as political and reputational damage to the interests of the state. The investigation of this cyber incident is still ongoing, so we hope that expert conclusions regarding the tactics, techniques, and procedures used in the cyber attack, as well as other circumstances and interested parties, will be made public. In its direction, indiscriminate application, and severity of consequences for the civilian population in the context of armed conflict, this cyber-attack contains all the qualifying characteristics of a war crime, to become the subject of consideration by the International Criminal Court.

2021 Cyber Incident Landscape: A Comprehensive Analysis

The data from 2021 provides a comprehensive overview of Ukraine's cyber incident landscape during the year preceding the full-scale invasion. It offers valuable insights into the diversity and complexity of cyber threats that the country faced during this period. One of the most striking aspects of the data is the high number of incidents with unconventional tactics, totaling 1,143 incidents. These incidents do not neatly fit into standard cyber threat categories, indicating a highly diverse and multifaceted cyber threat environment in 2021. It is essential to recognize that not all cyber threats can be easily categorized, highlighting the need for a flexible and adaptive cybersecurity strategy, as many attacks are hybrids incorporating elements of several cyber-attack types. These include novel attack methods, hybrid tactics, or attacks that blur the lines between espionage, cybercrime, and hacktivism. Understanding these categories is particularly challenging because it signifies an evolving threat landscape where adversaries continuously adapt and innovate. This complexity underscores the critical importance of robust threat intelligence and analytics capabilities, capable of tackling unconventional tactics.[36]



Information Gathering and Malicious Code

In 2021, Ukraine experienced significant cyber threats in the form of information gathering and the deployment of malicious code. Information gathering, represented by 80 incidents, suggests that adversaries were actively collecting sensitive data, possibly for espionage or reconnaissance purposes. This tactic indicates a strategic interest in gathering intelligence and laying the groundwork for more targeted cyber operations in the future. The prevalence of information gathering incidents was a cause for concern as it signified a persistent interest in Ukraine's affairs by various threat actors.

It was evident that espionage-related activities could have far-reaching consequences, affecting not only national security but also diplomatic relations and economic stability. The sensitive information collected could be used for blackmail, disinformation campaigns, or as a foundation for more sophisticated cyberattacks. Additionally, the deployment of malicious code (e.g., malware, ransomware, backdoors, etc.), with 75 reported incidents, reflected a concerted effort by cyber adversaries to infiltrate and compromise Ukrainian systems. Malicious code can manifest in various forms, such as malware, ransomware, or backdoors. These incidents underlined the importance of strong endpoint security, regular system updates, and robust incident response plans to thwart these attacks effectively. For Ukraine, combating information gathering and malicious code deployment necessitated not only a defensive approach but also proactive threat hunting capabilities. Identifying indicators of compromise and early detection of suspicious activities was instrumental in disrupting adversaries' operations before they escalated into more significant cyber incidents.

Direct Attack Efforts in 2021

While the majority of cyber incidents in 2021 had covert objectives, such as information gathering and deploying malicious code, there were also instances of direct attacks. These direct attacks included intrusion attempts (18 incidents), availability issues (10 incidents), and actual intrusions (8 incidents). These incidents, though less common, highlighted the ongoing risk of direct cyberattacks on critical systems and infrastructure. Intrusion attempts, involving unauthorized access attempts into systems or networks, posed a significant threat to data integrity and security. Cyber adversaries often employed a range of tactics to breach security perimeters, including exploiting vulnerabilities, utilizing brute-force attacks, or leveraging social engineering techniques.

Availability issues, on the other hand, could disrupt digital services and impact the normal functioning of organizations. These incidents were ranging from Distributed Denial of Service (DDoS) attacks to targeted efforts aimed at disrupting critical infrastructure. The presence of these direct attack incidents served as a reminder that cyber adversaries were not limited to covert tactics alone. It accentuated the importance of maintaining robust cybersecurity measures to defend against a wide range of cyber threats, both covert and overt.

Targeted Sectors in 2021: A Critical Examination

The distribution of cyber incidents across sectors in 2021 was not random but rather reflected a calculated approach by cyber adversaries to disrupt key areas. Government and local authorities bore the brunt of these attacks, experiencing 276 incidents. This targeting highlighted a focus on governmental operations and public sector infrastructure. The implications of cyberattacks on government institutions are far-reaching, affecting not only national security but also the delivery of public services. The security and defence sector, with 222 incidents, was another prime target for cyber adversaries. This emphasized attempts to

compromise national security mechanisms, which could include the theft of classified information, disruption of military operations, or compromising critical defence systems. These incidents underscored the potential vulnerabilities in Ukraine's defence infrastructure and the need for heightened cybersecurity measures. Commercial organizations, the financial sector, and the energy sector also faced a considerable number of cyber incidents. These sectors play a crucial role in Ukraine's economy and daily life, making them attractive targets for adversaries seeking to exert pressure or cause widespread disruption. Cyberattacks on these sectors could disrupt financial services, energy supply chains, and commercial activities, leading to economic instability and public inconvenience.
The strategic targeting of these sectors in 2021 highlighted the adversaries' intent to impact Ukraine's economic stability and critical infrastructure. It also emphasized the need for a comprehensive cybersecurity strategy that addresses vulnerabilities across various sectors.

Techniques and Procedures in 2021: A Diverse Arsenal

The variety of techniques and procedures employed in cyber incidents throughout 2021 reflects the adaptability and resourcefulness of cyber adversaries. Phishing, with 82 incidents, and malicious connections, at 33 incidents, were notable for their focus on exploiting human factors and establishing unauthorized network connections, respectively. Phishing attacks often relied on social engineering and deceptive tactics to trick individuals into revealing sensitive information or clicking on malicious links. Malicious connections, on the other hand, could be used to establish unauthorized access points into networks, making them particularly dangerous. Other techniques, though less frequent, were still part of the threat landscape. These included malware distribution, login attempts, and DoS/DDoS attacks. These methods demonstrated a range of attack vectors, from targeting individual user credentials to attempting to overwhelm and incapacitate digital services. The diversity of techniques highlighted the need for a comprehensive cybersecurity response capable of addressing a wide range of potential threats effectively.

Cyber Resilience: Insights and Implications

The data from 2021 offers several insights into Ukraine's cyber resilience before the war. First, the sheer diversity of cyber threats highlights a cyber environment that was complex and challenging. Ukraine's exposure to a wide range of cyber activities could be indicative of a robust engagement with and

understanding of the evolving cyber threat landscape. The focus on critical sectors like government, defence, and key economic industries suggests that Ukraine was aware of and possibly preparing for cyber threats in these areas. The nature of the targeted sectors indicates an understanding of the potential impact of cyber incidents on national security and economic stability. Ukraine recognized the importance of safeguarding these sectors and took measures to defend them. However, the high number of undetermined incidents raised important considerations for Ukraine's cyber threat analysis and response capabilities. Addressing this challenge became a priority for Ukraine in order to enhance the country's ability to identify and mitigate cyber threats effectively.

The pre-war cyber resilience of Ukraine, as depicted by the 2021 data, was marked by a multifaceted and diverse cyber threat environment. The country faced a range of adversarial cyber activities, from espionage and information gathering to the deployment of malicious code. The targeted sectors underscored a focus on government, defence, and critical economic industries, reflecting both the priorities of cyber adversaries and the areas of potential vulnerability. This pre-war period set the stage for Ukraine's cyber resilience as the country entered a more turbulent and challenging phase with the onset of the war in 2022.

4.2 Active Phase of War in 2022-2023

In the active phase of the war, Ukraine experienced a total of 11,922 cyber incidents across various tactics, targeted sectors, and techniques from January 2022 to the end of August 2023 (see **Figure 5**).

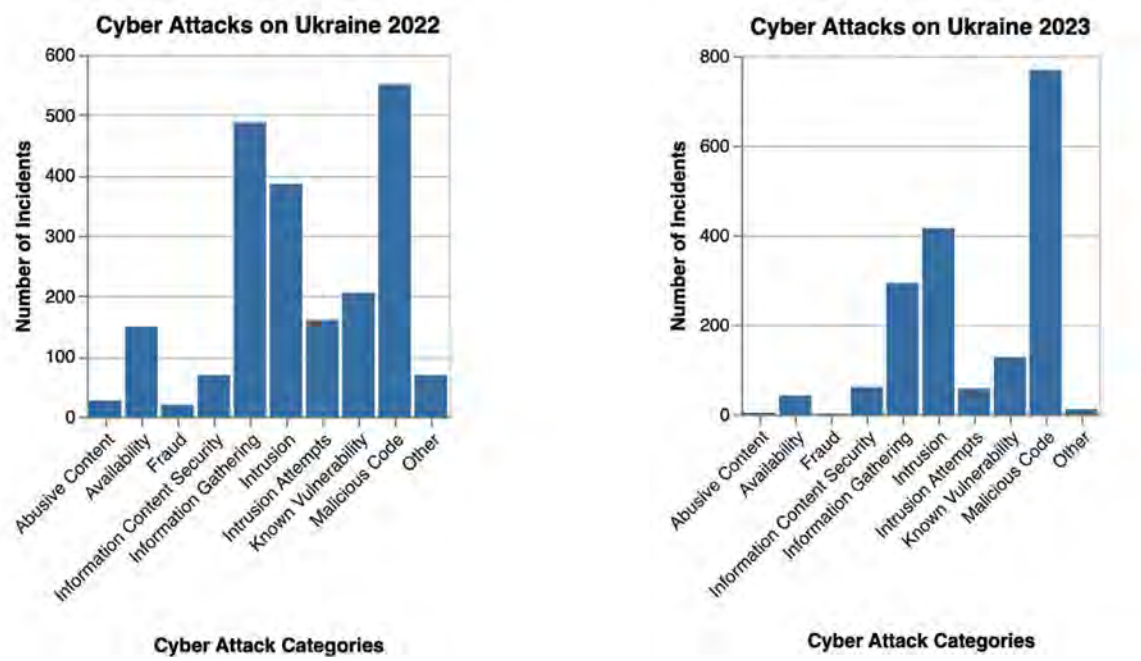


Figure 5 Cyber Attacks in 2022-2023

This indicates a high level of cyber threats coinciding with the physical conflict. The majority of incidents involved malicious code (1,320), followed by information gathering (843) and intrusion (802). The prevalence of these tactics highlights sophisticated and targeted cyber-attacks. Government organizations (578 incidents) and the IT sector (434) were the most targeted, reflecting an attempt to disrupt critical infrastructure and state functions. The financial sector (243) and commercial organizations (218) were also significantly targeted, indicating a broader impact on Ukraine's economy and private sector. System compromise (824 incidents) and malware distribution (755) were the most used techniques, signifying an emphasis on system infiltration and disruption. Vulnerability exploitation attempts (383) and phishing (364) were also notable, pointing to both technical and human-factor exploitations.

The year 2022 witnessed a significant transformation in Russian cyber tactics. Malicious Code incidents saw a substantial increase, surging from 75 incidents in 2021 to a staggering 551 in 2022. This surge in malicious code deployment suggests a more aggressive posture, with cyber actors seeking to exploit vulnerabilities, potentially engaging in activities like deploying ransomware or other forms of disruptive cyberattacks. Information Gathering incidents also experienced a notable surge, rising from 80 in 2021 to 550 in 2022. This increase indicates a heightened interest in collecting sensitive information, possibly for espionage or reconnaissance purposes. Cyber adversaries were actively gathering intelligence, potentially laying the groundwork for more strategic and targeted cyber operations. Intrusion incidents similarly increased from 8 in 2021 to 386 in 2022. These incidents involve unauthorized access to systems or networks, posing a direct threat to data security and integrity. The sharp rise in intrusion attempts underscores the aggressiveness of Russian cyber operations during this period. Conversely, the 'Other' category witnessed a sharp decline, dropping from 1,143 incidents in 2021 to only 69 in 2022. This decline suggests a shift away from experimental or unconventional tactics in favor of more defined and specialized methods. Russian cyber actors appeared to be concentrating their efforts on specific objectives and targets.

In 2023, the data indicates a continuation of certain trends observed in 2022. Malicious Code incidents continued to rise, though at a slower pace compared to the previous year, with 769 incidents recorded. This suggests a sustained interest in deploying harmful software, potentially for disruptive or espionage purposes.
Information Gathering incidents also persisted, although the increase was less pronounced than in 2022, with 293 incidents. The decrease in Information Gathering incidents may indicate a

refinement in tactics or a more selective approach to data collection. The 'Other' category witnessed a further decrease, with only 12 incidents reported in 2023. This significant reduction suggests a strategic shift towards more defined and focused tactics, leaving behind the experimental and unconventional approaches of the past. Intrusion Attempts also decreased from 58 incidents in 2022 to 12 incidents in 2023. This decline may indicate that cyber actors were becoming more selective in their intrusion attempts, focusing on high-value targets.

Cyber Incidents in 2022 and 2023 by Techniques and Procedures

In 2022, there was a significant transformation in the techniques and procedures employed. Phishing incidents surged from 82 in 2021 to 534 in 2022, signifying a concentrated effort to exploit human vulnerabilities and deceive individuals into revealing sensitive information or clicking on malicious links. Malware Distribution also saw a substantial increase, rising from 28 incidents in 2021 to 335 in 2022. This increase indicates a more aggressive approach to deploying harmful software, possibly with the intent to disrupt, damage, or gain unauthorized access to information and resources. Account Compromise incidents rose significantly, from 4 in 2021 to 227 in 2022. This technique involves unauthorized access to user accounts, highlighting cyber adversaries' efforts to infiltrate digital identities and systems. Undetermined Incidents decreased markedly from 1,144 in 2021 to 75 in 2022, reflecting a shift towards more identifiable and targeted attacks. The reduction in undetermined incidents suggests a greater degree of attribution and visibility into cyber operations.

In 2023, certain trends in techniques and procedures persisted while others evolved. Malware Distribution remained a prominent tactic, with 420 incidents recorded. This continued emphasis on deploying malicious software suggests an ongoing interest in disruptive and damaging cyber activities. Account Compromise incidents also remained significant, with 207 cases in 2023. This indicates a sustained focus on gaining unauthorized access to user accounts, potentially for espionage or further cyber operations. Malicious Connection incidents saw a notable increase, rising from 105 in 2022 to 278 in 2023. This technique involves establishing unauthorized network connections, potentially indicating a strategic use of infiltration and exploitation. Phishing incidents, however, decreased from 534 in 2022 to 290 in 2023, suggesting evolving tactics or potentially more effective defences against phishing attempts. Undetermined Incidents continued to decline, with 48 incidents reported in 2023. This decrease reinforces the trend towards more identifiable and targeted cyberattacks, where attribution and visibility into tactics have improved.

Our analysis indicates that the rise in cyberattack intensity in 2023, alongside a notable decrease in critical incidents, suggests the Russian cyber units have likely expanded by incorporating less experienced personnel for simpler technical tasks. This expansion may also reflect a shift in their tactical approach. Supporting this theory is the Insikt Group's analysis of nine different wiper malware variants. Their findings show that while these variants share a common destructive purpose, they differ in technical execution and the operating systems they target. It appears each variant was independently created, possibly by various authors. Over time, these wipers have evolved to become technically simpler, featuring fewer stages, reduced obfuscation, and less frequent attempts to simulate ransom demands. Notably, these «simplified» wipers generally lack the capability to self-replicate, with some exceptions like HermeticWiper.

This change in tactics may indicate Russia's intention to minimize collateral damage outside Ukraine, a shift from the widespread impacts seen during the NotPetya incident. It suggests a strategy to appear less aggressive or «cybertoxic» to Western nations, unlike the AcidRain wiper that uncontrollably spread beyond Ukraine's borders. These developments could signify a strategic and tactical shift in cyber operations, potentially due to the inclusion of less experienced cyber personnel. The GRU seems to be adopting a flexible approach, utilizing these "simplified wipers" that are easier to deploy and require fewer resources. This also points to a change in the focus of cyber warfare, prioritizing the volume of attacks with a mass deployment of these "simplified wipers" over more sophisticated, quality-focused attacks.

Cyber Incidents by Targeted Sectors in 2022 and 2023

In 2022, there was a noticeable shift in sector targeting. While Government and Local Authorities continued to be significant targets, with 556 incidents, other sectors also saw increased attention. The Security and Defence sector, in particular, experienced a surge in incidents, with 309 reported cases. Additionally, the Commercial sector became a notable target, with 129 incidents recorded. Specifically, the Financial and Energy sectors saw increased targeting, with 119 and 105 incidents, respectively. This shift indicated a broader targeting strategy, potentially aimed at exerting pressure or causing widespread disruption across various critical sectors.

In 2023, the data on sector targeting revealed some notable changes. Government Organizations and Local Authorities saw an increase in targeting, with 237 incidents. This indicated renewed interest in these sectors, albeit with a more specific strategic focus. The Security and Defence sector remained a target, with 124 incidents, though the intensity of attacks appeared to have decreased compared to 2022. Other sectors, such as Commercial organizations (89 incidents) and the Financial sector (25 incidents), continued to experience cyber incidents but at a reduced level compared to the previous year.

4.3 Physical vs Cyber War

In order to better understand the dynamics and correlation between Russia's physical and cyber-attacks on Ukraine, we first consider high-level monthly data courtesy of STATISTA (statista.com) indicative of the intensity of physical attacks versus the intensity of cyber-attacks. To approximate the intensity of physical attacks, we first correlate the total number of war casualties in Ukraine with the total number of adversarial incidents with alleged Russian origins. Our assumption is that casualties provide a rough indication of physical attacks' intensity (see **Figure 6**).

Figure 6 illustrates the trends in total casualties from physical attacks (in red) and total cyber incidents (in blue) over time. There are peaks and troughs in both physical and cyber incidents, but it is not immediately clear whether there is a strong correlation between the two. Notably, in March 2022, there is a significant peak in physical casualties, which doesn't seem to be mirrored by a corresponding increase in cyber incidents. In contrast, August 2023 shows a high number of cyber incidents without a corresponding peak in physical casualties.

Yet, if we introduce a «lagged» variable for cyber incidents by shifting the total cyber incidents data by one time period (one month in this case) and correlate it with our proxy of the physical attacks' intensity (number of casualties in the current month), we find strong correlation between cyber-attacks preceding physical attacks as depicted on **Figure 7**. The correlation is significant at 5% level.

In order to extend our analysis beyond simple linear regression, we conducted a correlation analysis of the information space using analytical tools based on expert queries to the Attack-Index information system. We analyzed the correlations between cyber

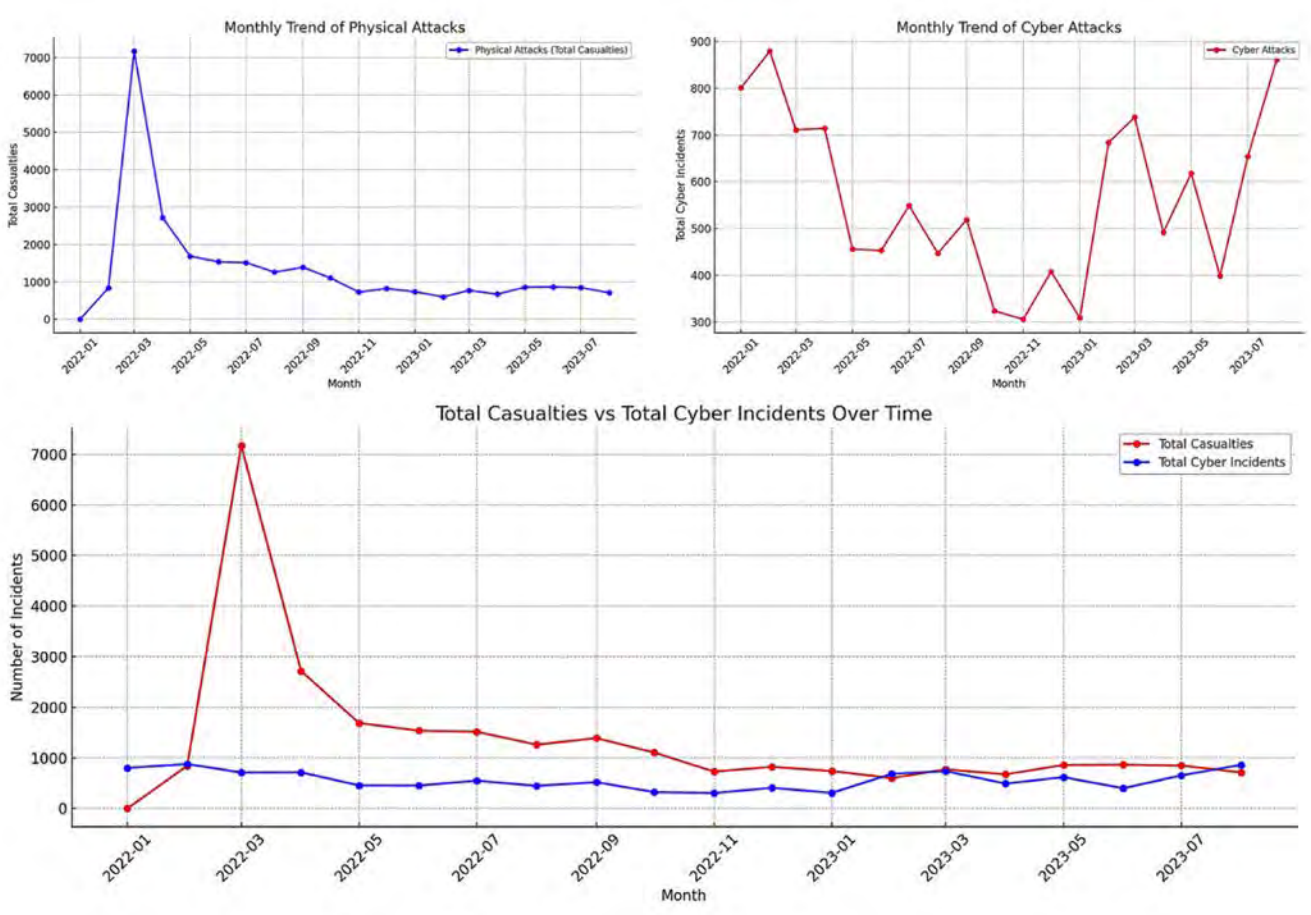


Figure 6 Initial Approximation of Physical vs Cyber Attack

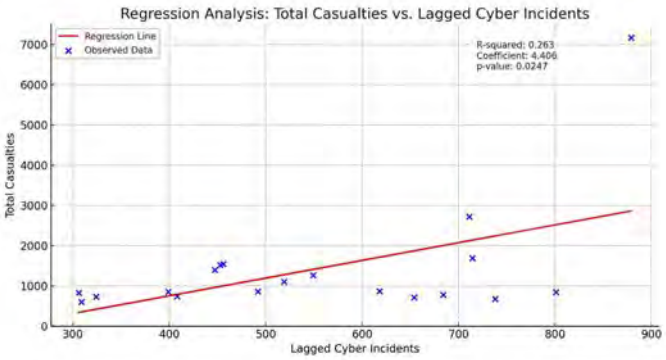


Figure 7 Results of Linear Regression Analysis Demonstrating Correlation between Cyber Attacks in the previous month predicting the magnitude of Physical Attacks in the current month

actions and information operations during the period of Russia's military aggression against Ukraine from 2014 to 2023. Additionally, we separately examined the period of full-scale invasion in 2022-2023. Verified statistical data on cyber incidents and missile strikes were collected for this analysis. The hypothesis of our study posits that the active phase of Russia's overt aggression since 2014 has influenced Ukraine's resilience in at least three spheres: cybersecurity, strategic communications, and defence components. Across all three domains, international support has evolved – methodological, technical, non-lethal, and in the last two years, even with lethal weaponry.

The correlation calculations were conducted over corresponding time intervals (daily, monthly, and weekly) between similarly generalized numerical series, with the results presented in Figure 8. The Figure outlines the correlation results concerning real missile strikes, reports about them, and military aid. It includes a detailed breakdown of correlation coefficients and time lags (daily, weekly, monthly) for different data sets. These sets include correlations between reports of cyberattacks and missile strike statistics, data on missile strikes and reports about them, missile strike data and military aid, and correlations between reports of missile strikes and military aid. The calculated correlation coefficients for missile strikes and reports about them, with a zero-time lag, indicate a strong interrelation. These range from 0.42 for daily data to 0.79 and 0.89 for weekly and monthly data, respectively. This suggests that reporting on missile strikes occurs almost simultaneously with the strikes themselves, with the quantitative characteristics of the reports mirroring the statistics of the missile strikes in both trend and context. **Figure 8** demonstrates the following results:

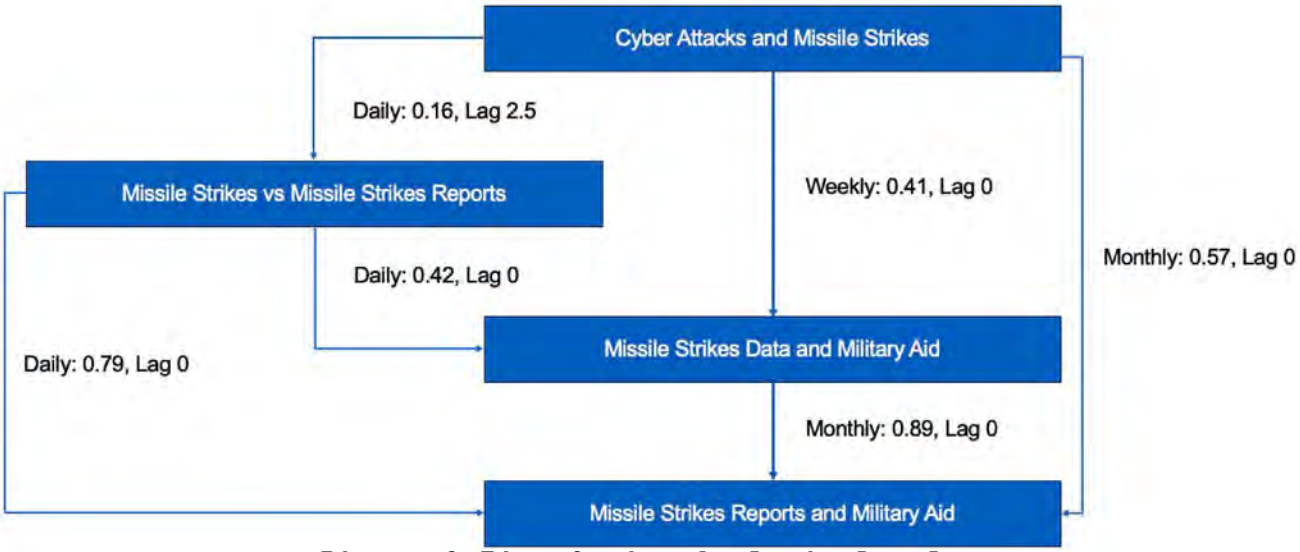


Figure 8 Time Series Analysis Results

(i) Cyberattacks and Missile Strikes:

• Daily: The correlation coefficient of 0.16 suggests a weak positive relationship. It indicates that there is some correlation between reports of cyberattacks and statistics of missile strikes on a daily basis, with a lag of 2.5 days. This means that there is a connection between these two events, with cyberattacks preceding missile strikes by several days.

(ii) Missile Strikes Data and Reports:

• Daily: The correlation coefficient of 0.42 signifies a moderate positive relationship with no lag. Daily data on missile strikes and reports about them are moderately correlated, suggesting that reports closely follow missile strike events in real-time.

• Weekly: The correlation coefficient of 0.79 indicates a strong positive relationship with no lag. Weekly data shows a strong correlation between missile strikes and reports, indicating that reports tend to closely mirror missile strike statistics on a weekly basis.

• Monthly: The correlation coefficient of 0.89 demonstrates a very strong positive relationship with no lag. Monthly data reveals a highly correlated pattern between missile strikes and reports, indicating that monthly reports align closely with the overall missile strike statistics.

(iii) Missile Strikes Data and Military Aid:

• Daily: The correlation coefficient of 0.009 suggests a very weak positive relationship with a lag of 2 days. Daily data on missile strikes and military aid shows a minimal and delayed correlation, implying that military aid follows missile strikes with a slight delay.

• Weekly: The correlation coefficient of 0.79 indicates a strong positive relationship with no lag. Weekly data reveals a strong correlation between missile strike statistics and military aid, indicating that military aid closely follows the trends in missile strikes on a weekly basis.

• Monthly: The correlation coefficient of 0.89 demonstrates a very strong positive relationship with no lag. Monthly data shows a highly correlated pattern between missile strikes and military aid, indicating that monthly military aid closely aligns with the overall missile strike statistics.

(iv) Missile Strike Reports and Military Aid:

• Monthly: The graph shows a monthly correlation of 0.62 between reports of missile strikes and military aid, suggesting a strong positive relationship. This indicates that monthly reports about missile strikes are closely tied to the provision of military aid.

Figure 8 highlights the different strengths and temporal aspects of correlations between various aspects of missile strikes, cyberattacks, and military aid. It suggests that reports about missile strikes tend to closely follow the events in real-time, while the relationship between military aid and missile strikes has a lag, with military aid closely associated with trends in missile strikes.

Furthermore, we examined the correlations between actual missile strikes and cyberattacks by looking at the weekly data. The correlation function between the numerical series of missile strike statistics and reports of cyberattacks (see **Figure 9**) shows significant correlation coefficients of 0.41 and 0.57 for zero-time lag in weekly and monthly calculations, respectively.

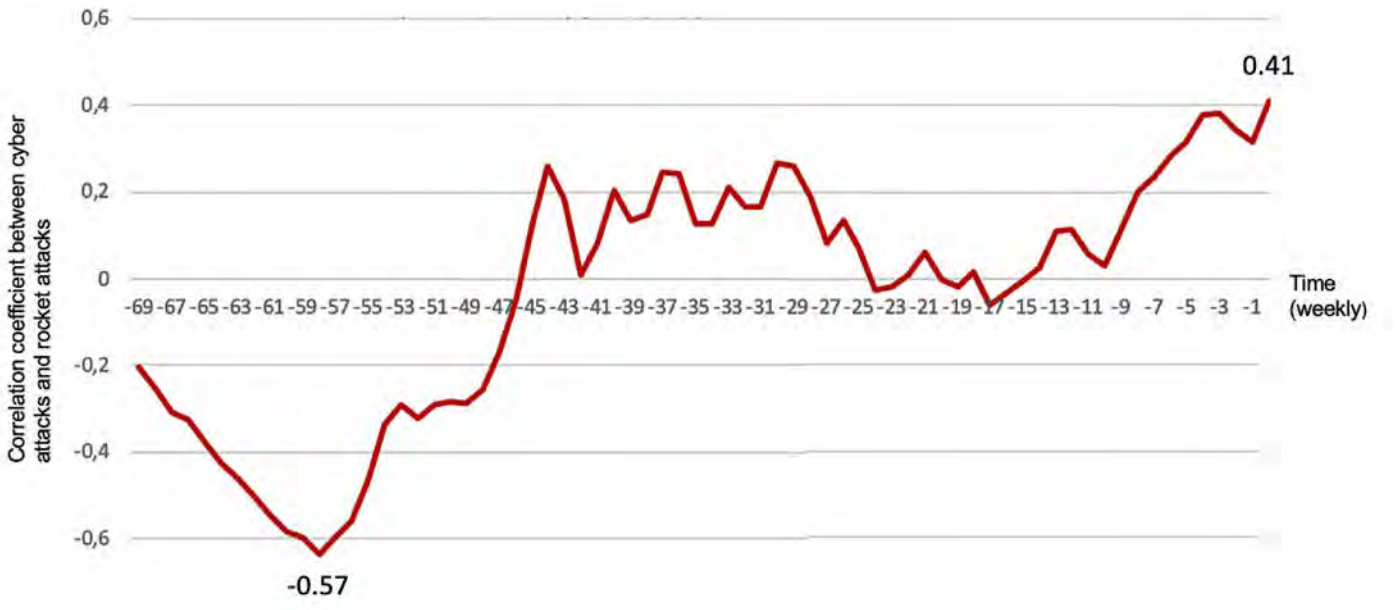


Figure 9 Correlation Function between Cyber Attacks and Missile Attacks

These findings, although with a weaker correlation coefficient of 0.16 and a lag of 25 days, **suggest a nearly month-long time gap between reports of cyberattacks and missile strikes.** This data leads to the inference that Russia, as per its combat plan, tends to employ cyberattacks about a month prior to physical strikes. The purpose of this strategy is presumably to weaken infrastructure resilience and incite panic among the population. It also indicates that these cyberattacks might be aimed at gathering intelligence as a part of planning for subsequent missile strikes.

The analysis of Russian cyberwar tactics from 2021 to 2023 reveals a dynamic and evolving landscape, marked by several overarching trends that provide valuable insights into the strategies, techniques, and targets of Russian cyber operations. These trends highlight the complexity and adaptability of cyberwarfare, as well as the need for robust defences and international cooperation to counter emerging threats effectively. Trend heatmap is presented on **Figure 10**.

Based on the statistical data, reported above in 4.2, we designed a trend strength index ranging from 0 = Very Low to 5= Very High and plotted this index on a heatmap. Deriving the index allows us to make the following conclusions.

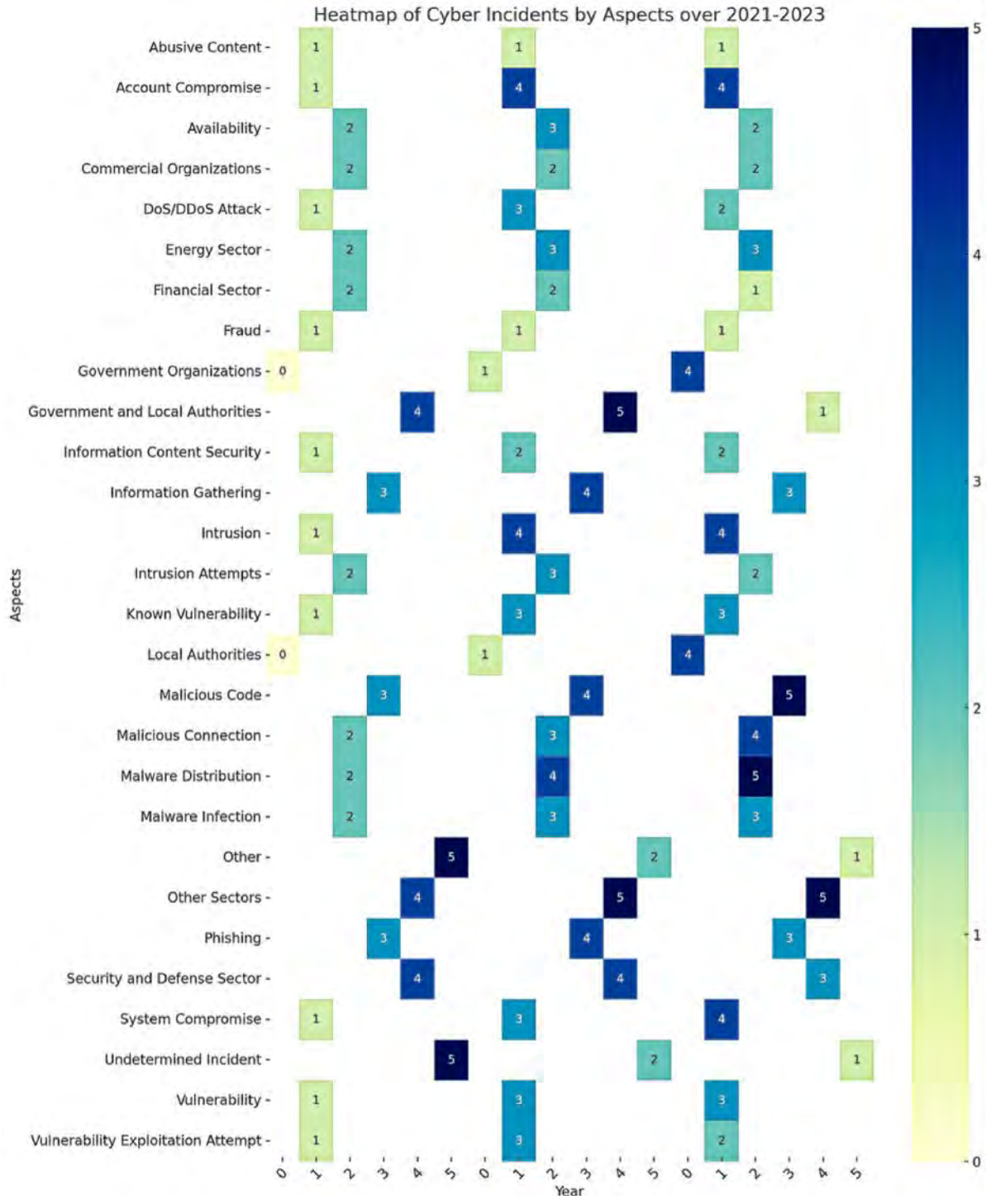


Figure 10 Overall Cyberwarfare Trends

PART V

Conclusion

Russian cyberwar tactics have undergone significant changes and refinements from 2013 to 2021 and then from 2021 through 2023. This evolution indicates a maturation of strategies, techniques, and targeting preferences. While 2021 saw a more exploratory and diverse approach, subsequent years showed a shift towards more specific, identifiable, and impactful tactics. As cyber threats continue to evolve, it is crucial for cybersecurity professionals, organizations, and governments to stay vigilant, adapt their defences, and collaborate internationally to mitigate the risks posed by sophisticated nation-state cyber actors like Russia. The lessons learned from the analysis of these trends (summarized in Table 1) can help inform future cybersecurity strategies and policies to protect critical infrastructure, data, and national security.

The conclusions drawn from the comprehensive analysis of Russian cyberwarfare tactics paint a vivid picture of a nation-state actor that has not only evolved but also refined its adversarial cyber operations significantly. This evolution is marked by a strategic shift from experimental and diverse tactics to more specific, sophisticated, and impactful methods, reflecting a maturation process in their cyberwarfare approach. Up to 2021, Russian cyber tactics were characterized by a diverse and exploratory approach, as evidenced by the high incidence of various cyber incidents and techniques. This period saw a significant reliance on malicious code, phishing, and malware distribution, indicating a broad-based strategy to probe and exploit vulnerabilities across multiple fronts. However, as we moved into 2022 and 2023, there was a noticeable shift towards more targeted and defined cyber operations.

This transition is particularly evident in the reduction of undetermined incidents and the increased focus on specific techniques like account compromise, system compromise, and establishing malicious network connections. The refinement in techniques underscores the adaptability and resourcefulness of Russian cyber actors. They demonstrated a keen ability to exploit human vulnerabilities, deploy sophisticated malicious software, and infiltrate digital identities and systems. This adaptability is further highlighted by the evolving sector targeting trends. Initially, the focus was broad, encompassing various sectors. However, over time, there was a strategic shift towards more specific targeting, particularly in government organizations and local authorities by 2023, indicating a nuanced understanding of geopolitical dynamics and tactical considerations. The data summarized in Table 1 provides a clear trajectory of these evolving tactics.

The increasing reliance on sophisticated malicious code, the spike and subsequent decrease in information gathering efforts, and the marked increase in direct system intrusions reflect a strategic refinement in cyber operations. The growing exploitation of known vulnerabilities and the variation in intrusion attempts also indicate a dynamic approach in response to evolving cyber defences. As the cyber threat landscape continues to evolve, the insights gained from this analysis are crucial for enhancing cyber defences, mitigating risks, and developing comprehensive policies to safeguard critical infrastructure, data, and national security in an increasingly interconnected digital world.

The increasing reliance on sophisticated malicious code, the spike and subsequent decrease in information gathering efforts, and the marked increase in direct system intrusions reflect a strategic refinement in cyber operations. The growing exploitation of known vulnerabilities and the variation in intrusion attempts also indicate a dynamic approach in response to evolving cyber defences. As the cyber threat landscape continues to evolve, the insights gained from this analysis are crucial for enhancing cyber defences, mitigating risks, and developing comprehensive policies to safeguard critical infrastructure, data, and national security in an increasingly interconnected digital world.

Table 1 Trends in Russian Cyberwarfare

Aspect	2021	2022	2023	Trend and Interpretation
Cyber Incidents by Tactics				
Malicious Code	Moderate	High	Very High	Increasing reliance on sophisticated malicious code.
Other	Very High	Low	Very Low	Major shift away from diverse, less-defined tactics.
Information Gathering	Moderate	High	Moderate	Spike in 2022 suggests intensified intelligence efforts, with a slight decrease in 2023.
Intrusion	Very Low	High	High	Marked increase in direct system intrusions, maintaining high levels over time.
Known Vulnerability	Very Low	Moderate	Moderate	Growing exploitation of known vulnerabilities.
Intrusion Attempts	Low	Moderate	Low	Variation indicates fluctuating levels of attempted breaches.
Availability	Low	Moderate	Low	Indicates targeted attacks on system availability, but not a primary focus.
Information Content Security	Very Low	Low	Low	Gradual increase in attacks targeting content security.
Abusive Content	Very Low	Very Low	Very Low	Minimal focus on abusive content.
Fraud	Very Low	Very Low	Very Low	Limited use of fraud in cyber tactics.
Cyber Incidents by Techniques and Procedures				
Undetermined Incident	Very High	Low	Very Low	Major decrease in incidents with unclear techniques, indicating a shift to more specific, targeted methods.
Phishing	Moderate	High	Moderate	Consistent use of phishing with a peak in 2022, suggesting a strategic reliance on this technique.
Malware Distribution	Low	High	Very High	Significant increase in malware use, becoming a primary technique.
Account Compromise	Very Low	High	High	Marked increase, indicating a focus on compromising individual accounts.
Malicious Connection	Low	Moderate	High	Increasing efforts in establishing malicious network connections.
System Compromise	Very Low	Moderate	High	Rising trend in compromising entire systems.
Vulnerability	Very Low	Moderate	Moderate	Consistent focus on exploiting vulnerabilities.
DoS/DDoS Attack	Very Low	Moderate	Low	Fluctuating focus on denial-of-service attacks.
Malware Infection	Low	Moderate	Moderate	Increased use of malware infections, stabilizing in recent years.
Vulnerability Exploitation Attempt	Very Low	Moderate	Low	Indicative of opportunistic targeting of vulnerabilities.
Cyber Incidents by Targeted Sectors				
Other	High	Very High	Very High	Persistent, broad targeting outside of specific sectors.
Government and Local Authorities	High	Very High	Very Low	Major shift away from targeting government sectors in 2023.
Security and Defence Sector	High	High	Moderate	Decreasing focus on security and defence sectors.
Commercial Organizations	Low	Low	Low	Consistent but limited targeting of commercial entities.
Government Organizations	-	Very Low	High	Emergence and significant increase in targeting government organizations in 2023.
Financial Sector	Low	Low	Very Low	Decreased interest in targeting the financial sector.
Energy Sector	Low	Moderate	Moderate	Growing interest in targeting the energy sector.
Local Authorities	-	Very Low	High	Sudden increase in targeting local authorities in 2023.

PART VI

Recommendations

Considering the evolution and refinement of Russian cyberwar tactics from 2013 to 2023, the following recommendations are adjusted to address the dynamic and sophisticated nature of contemporary cyber threats:

1. Develop and Implement Proactive Cyber Defense and Information Countermeasures:

Formulate and implement dynamic guidelines for tactics in cyber operations and proactive information operations, incorporating the latest trends and tactics identified in the evolution of cyber warfare.
Recognize and categorize cyber/informational operations as distinct forms of warfare, with unique phases and classifications, emphasizing their strategic importance alongside kinetic actions.
Integrate these adaptive guidelines into military strategic documents for operational and tactical use, ensuring the effective planning and execution of cyberattacks and informational operations. Involve cyber reservists from Ukraine's private and public sectors, harnessing their expertise in the face of evolving cyber threats.

2. Establish a Notification Mechanism for Potential Cyber Threats to Critical Infrastructure:

Develop an advanced notification system to alert operators of critical infrastructures about potential cyber threats promptly. This system should incorporate real-time data and predictive analytics based on a comprehensive vulnerability analysis of critical information infrastructure.
Provide continuous and adaptive organizational and methodological support to these operators, facilitating the development and implementation of flexible strategies to mitigate identified vulnerabilities, manage emerging risks, and handle information security events and cyber incidents effectively.

3. Adapt to the Evolving Tactics, Technologies, and Procedures of Russian Cyber Threat Actors:

Stay abreast of and adapt to the changing tactics, technologies, and procedures of Russian cyber adversaries, with a particular focus on the sophisticated use of malicious software like wipers.
Develop agile preventive strategies, enhance timely detection capabilities, and formulate robust cyber defense measures to mitigate adverse effects. Involve entities from national cyber security systems, the private sector, and civil society, fostering a holistic cyber defense mechanism.
Recognize and respond to the expanding landscape of cyberattacks, particularly those targeting private and public sector organizations. Foster collaboration among relevant stakeholders in these sectors to develop effective public-private cyber interaction mechanisms, leveraging the expertise of cyber professionals.

4. Conduct Systematic Analysis of Cyber and Informational Operations:

Implement a systematic and continuous analysis of cyber and informational operations, considering the broader military context and their integration into armed conflict. Utilize verified statistical and operational-tactical data for effective planning and implementation of combat tasks.
Employ artificial intelligence and machine learning technologies to predict cyber and informational operations, aiming to proactively prevent or mitigate the impact of cyberattacks.
Ensure the responsible deployment of cyber offensive tactics by developing and training military personnel in the rules of cyber weapon usage, in strict alignment with international legal norms for responsible conduct and protocols for cyber operations.

5. Promote Ukraine's Stance Internationally on Recognizing Cyberattacks as War Crimes and Strengthen International Collaboration:

Vigorously advocate for the international recognition of cyberattacks on critical civilian infrastructure, particularly during armed conflicts, as war crimes and terrorist acts, especially those perpetrated by Russia, a state sponsor of terrorism.
Intensify collaboration with international partners to investigate and attribute cybercrimes, aiming for criminal prosecution in national courts and the submission of evidence regarding war and terrorist cybercrimes to the International Criminal Court.
Actively engage in information sharing and participate in joint initiatives under the international initiative to combat ransomware, emphasizing the development of a united global front against evolving cyber threats.

References

1. Guchua, A., Zedelashvili, T., & Giorgadze, G. (2022). Geopolitics of the Russia-Ukraine war and Russian cyber attacks on Ukraine-Georgia and expected threats. Ukrainian Policymaker, 10(1), 26-36.

2. Maliukevičius, N. (2006). Geopolitics and information warfare: Russia's approach. Lithuanian annual strategic review, 2006, 121-47

3. NATO. (2023, December). Russian War Against Ukraine Lessons Learned Curriculum Guide. Retrieved from https://www.nato.int/cps/en/natohq/topics_221175.htm

4. President of Russia. (2010, February 5). Военная доктрина рф, утверждена указом президента рф [Military Doctrine of the Russian Federation, approved by presidential decree]. Retrieved from https://web.archive.org/web/20110722191323/http://news.kremlin.ru/ref_notes/461/print

5. President of Russia. (2014, December 26). Военная доктрина рф, утверждена указом президента рф с изменениями 2018 года. (2018) [Military Doctrine of the Russian Federation, approved by presidential decree]. Retrieved from http://static.kremlin.ru/media/events/files/41d527556bec8deb3530.pdf

6. Supreme State Council of the Union State. (2021, November 4). Военная доктрина Союзного Государства [Military Doctrine of the Union State]. Retrieved from https://xn--c1anggbdpdf.xn--p1ai/documentation/document/1899/

7. Buchanan, B. (2020). The hacker and

the state: Cyber attacks and the new normal of geopolitics. Harvard University Press.

8. Grossman, T., Kaminska, M., Shires, J., & Smeets, M. (2023, April). The Cyber Dimensions of the Russia-Ukraine War. ECCRI Tallinn Workshop Report. Retrieved from https://policycommons.net/artifacts/4397494/eccri_report_the-cyber-dimensions-of-the-russia-ukraine-war-19042023/5194113/

9. Khac Quoc Nguyen, B., & Hoang, K. (2023). From Geopolitical Threats to Cyberwarfare: The Effect of Russia's Threats on Corporate Cybersecurity in the United States. Khanh, From Geopolitical Threats to Cyberwarfare: The Effect of Russia's Threats on Corporate Cybersecurity in the United States (January 15, 2023).

10. Zvezda. (2016, September 14). Армия России впервые отработала информационное противоборство на учениях «Кавказ-2016» [The Russian Army for the first time practiced information warfare during the «Caucasus-2016» exercises]. Retrieved from https://tvzvezda.ru/news/201609141221-va0s.htm

11. RIA Novosti. (2017, February 22). Шойгу рассказал о задачах войск информационных операций [Shoigu talks about the tasks of information operations forces]. Retrieved from https://ria.ru/20170222/1488617708.html

12. InformNapalm. (2023, April 10). Злам офіцера ГРУ рф, куратора хакерського угруповання APT 28 [The exposure of the Russian GRU officer, curator of the APT 28 hacker group]. Retrieved from https://informnapalm.org

13. Congressional Research Service. (2022). U.S. Sanctions on Russia (R45415). Retrieved from https://crsreports.congress.gov/product/pdf/R/R45415

14. The Economist. (2023, December 31). How ransomware could cripple countries, not just companies. The Economist Group Limited. https://www.economist.com/international/2023/12/31/how-ransomware-could-cripple-countries-not-just-companies

15. U.S. Department of the Treasury. (2021, April 15). Treasury sanctions Russia with sweeping new sanctions authority [Press release]. https://home.treasury.gov/news/press-releases/jy0127

16. CNN. (2023, February 14). Wagner chief admits to founding Russian troll farm sanctioned for meddling in US elections. Retrieved from https://edition.cnn.com/2023/02/14/europe/russia-yevgeny-prigozhin-internet-research-agency-intl/index.html

17. Security Service of Ukraine. (2021, February 1). СБУ викрила мережу російських агентів. Retrieved from https://ssu.gov.ua/en/novyny/sbu-vykryla-ahenturnu-merezhu-spetssluzhb-rf-yakadestabilizuvala-sytuatsiiu-v-ukraini-cherez-telegramkanaly.

18. House of Commons Library (2024) Conflict in Ukraine: A timeline (2014 – eve of 2022 invasion) https://commonslibrary.parliament.uk/research-briefings/cbp-9476/

19. Ukrinform. (n.d.). Революція Гідності. Згадаймо головне [Maidan Revolution. Let's remember the main points]. Retrieved from https://www.ukrinform.ua/rubric-polytics/2122489-revolucia-gidnosti-zgadajmo-golovne.html

20. Silicon UK. (n.d.). Retrieved from https://www.silicon.co.uk/security/notpetya-ransomware-wannacry-215985

21. Верховна Рада України. (2017). Про основні засади забезпечення кібербезпеки України. Законодавство України. https://zakon.rada.gov.ua/laws/show/2163-19#Text

22. BBC News Україна. (2020, July 26). Зеленський поговорив із Путіним. У Москви і Києва дещо різні версії розмови [Zelensky talked to Putin. Moscow and Kyiv have slightly different versions of the conversation]. Retrieved from https://www.bbc.com/ukrainian/news-53546908

23. Easterly, J., & Fanning, T. (2023, May 7). The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years. Cybersecurity and Infrastructure Security Agency. Retrieved from https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years

24. Operational Center for Cyber Incident Response, State Cyber Protection Center, State Service of Special Communications and Information Protection of Ukraine. (2021). Звіт роботи системи виявлення вразливостей і реагування на кіберінциденти та кібератаки за 2021 рік [Annual report on the vulnerability detection system and response to cyber incidents and cyberattacks for 2021]. Retrieved from https://cert.gov.ua/files/pdf/SOC_Annual_Report_2022.pdf

25. ESET. (2022). ESET Threat Report T1 2022. Retrieved from https://www.eset.com/int/business/resource-center/reports/eset-threat-report-t1-2022/

26. Reuters. (2022, February 28). Satellite outage knocks out control of Enercon wind turbines. Retrieved from https://www.reuters.com/business/energy/satellite-outage-knocks-out-control-enercon-wind-turbines-2022-02-28/

27. Vasquez, C., & Groll, E. (August 10, 2023). Satellite hack on eve of Ukraine war was a coordinated, multi-pronged assault. CyberScoop. Retrieved from https://cyberscoop.com/viasat-ka-sat-hack-black-hat/

28. Microsoft Threat Intelligence. (March 15, 2023). A year of Russian hybrid warfare in Ukraine: What we have learned about nation-state tactics so far and what may be on the horizon. Retrieved from https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW10mGC

29. Office of the Director of National Intelligence. (2023, February 6). Annual Threat Assessment of the U.S. Intelligence Community. Retrieved from https://www.odni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf

30. Komarov. (December 12, 2023). Pro kiberataku na Kyivstar: Vidnovlennya zvyazku ta dopomogu Microsoft, Cisco, Ericsson, BLITS [Interview with the President of the Company Komarov]. Forbes Ukraine. Retrieved from https://forbes.ua/innovations/pro-kiberataku-na-kiivstar-vidnovlennya-zvyazku-ta-dopomogu-microsoft-cisco-ericsson-blits-intervyu-prezidenta-kompanii-komarov-12122023-17855

31. Мельник, Т. (2023, December 12). «Це найбільша у світі хакерська атака на телеком-інфраструктуру». Перше інтерв'ю президента «Київстару» після кібератаки, яка паралізувала оператора [«This is the world's largest hacker attack on telecom infrastructure.» First interview with the president of «Kyivstar» after the cyberattack that paralyzed the operator]. Forbes. https://forbes.ua/innovations/pro-kiberataku-na-kiivstar-vidnovlennya-zvyazku-ta-dopomogu-microsoft-cisco-ericsson-blits-intervyu-prezidenta-kompanii-komarov-12122023-17855

32. У «Київстарі» розповіли про відновлення після атаки: які послуги доступні і над чим ще працюють [«Kyivstar Reveals Recovery After Attack: What Services Are Available and What They Are Still Working On»]. Retrieved from https://tsn.ua/ukrayina/u-kiyivstari-rozpovili-pro-vidnovlennya-pislya-ataki-yaki-poslugi-dostupni-i-nad-chim-sche-pracyuyut-2474803.html

33. BBC Ukrainian. (2023, December 13). Хто стоїть за атакою на «Київстар» і коли відновлять зв'язок [«Who Is Behind the Attack on 'Kyivstar' and When Will Communication Be Restored»]. Retrieved from https://www.bbc.com/ukrainian/articles/c51z82rdppxo

34. VEON вітає колишнього держсекретаря США у Раді директорів Київстар» [VEON Welcomes Former U.S. Secretary of State to the Board of Directors of Kyivstar]. (November 24, 2023). Biz. Retrieved from https://biz.nv.ua/ukr/markets/sekretar-pompeo-priyednuyetsya-do-impact-investments-ta-veon-zminyuye-kerivnictvo-kijivstar-50368239.html

35. «Стратегічна помилка»: Майк Помпео прокоментував чутки про можливу націоналізацію Київстару [Strategic Mistake: Mike Pompeo Comments on Rumors of Possible Nationalization of Kyivstar]. (November 29, 2023). UNIAN. Retrieved from https://www.unian.ua/economics/other/strategichna-pomilka-mayk-pompeo-prokomentuvav-chutki-pro-mozhlivu-nacionalizaciyu-kijivstaru-12469461.html

36. Burt, T. (2022, April 27). The hybrid war in Ukraine. Microsoft On the Issues. https://blogs.microsoft.com/on-the-issues/2022/04/27/hybrid-war-ukraine-russia-cyberattacks/

37. Insikt Group. (2022, May 12). Overview of the 9 distinct data wipers used in the Ukraine war. Recorded Future. https://www.recordedfuture.com/blog/overview-9-district-data-wipers-ukraine-war

38. Lande, D., Soboliev, A., & Dmytrenko, O. (2022). Intelligent technologies in information retrieval systems. Artificial Intelligence, 27(1), 260-268. DOI: https://doi.org/10.15407/jai2022.01.260

Web Pages and Statistical Sources:

- **Attack-Index information system**

https://attackindex.com

- **Cybersecurity and Infrastructure Security Agency (CISA)**

https://www.cisa.gov/news-events/alerts/2022/04/07/guidance-sharing-cyber-incident-information
https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/russia

- **Cyber Peace Institute**

https://cpi.link/CATC-2022-Q4-report
https://cpi.link/CATC-2023-Q2-report
https://cyberconflicts.cyberpeaceinstitute.org/report/2023-q1
https://cyberpeaceinstitute.org/news/publications/cyber-dimensions-of-the-armed-conflict-in-ukraine-q2-2023/

- **ECCRI**

https://eccri.eu/wp-content/uploads/2022/07/ECCRI_WorkshopReport_Version-Online.pdf
https://policycommons.net/artifacts/4397494/eccri_report_the-cyber-dimensions-of-the-russia-ukraine-war-19042023/5194113/

- **ESET**

https://www.eset.com/int/business/resource-center/reports/eset-threat-report-t1-2022/
https://www.eset.com/ca/about/newsroom/press-releases/eset-announces-new-eset-threat-report-q1-2020/

- **European Union**

https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf

- **Google**

https://blog.google/threat-analysis-group/fog-of-war-how-the-ukraine-conflict-transformed-the-cyber-threat-landscape/

- **Microsoft**

https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/
https://blogs.microsoft.com/on-the-issues/2022/04/27/hybrid-war-ukraine-russia-cyberattacks/
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd
https://www.microsoft.com/en-us/security/business/security-intelligence-report
https://www.microsoft.com/security/blog/2020/09/29/microsoft-digital-defense-report-2020-cyber-threats/
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW10mGC

- **MSSP Alert**

https://www.msspalert.com/news/ukraine-russia-cyberattack-timeline-updates-amid-russia-invasion

- **NATO**

https://www.nato.int/cps/en/natohq/topics_221175.htm

- **NATO CCDCOE**

https://ccdcoe.org/uploads/2018/10/Ch01_CyberWarinPerspective_Geers.pdf
https://ccdcoe.org/uploads/2018/10/Ch15_CyberWarinPerspective_Roigas.pdf
https://www.ccdcoe.org/uploads/doc/CyCon_2023_book_print.pdf

- **Recorded Future**

https://therecord.media/russian-hackers-target-ukraine-gov-systems-war-crime-espionage
https://www.recordedfuture.com/blog/overview-9-district-data-wipers-ukraine-war

- **State Service of Special Communications and Information Protection of Ukraine (CERT-UA, SOC)**

https://cert.gov.ua/files/pdf/SOC_Annual_Report_2022.pdf
https://dciber.org/wp-content/uploads/2022/04/SSSCIP-Weekly-Digest-2022-04-11-ENG.pdf.
https://cip.gov.ua/services/cm/api/attachment/download?id=53466
https://cip.gov.ua/services/cm/api/attachment/download?id=60068

- **STATISTA**

https://statista.com/

- **Unit42**

https://www.paloaltonetworks.com/resources/research/2023-unit42-ransomware-extortion-report

Research Team

Research Project Lead: **Andrii Paziuk, Dr.jur.**

Analytics: **Ellina Shnurko-Tabakova, Oles Osadchyi**

Contributors: A**ndrii Davydiuk, NataliyaTkachuk, Sergii Prokopenko, Olexandr Bakalynskyi, Mykola Kuleshov, Roman Proskurovskyi, Maryna Yevdokymenko**

Global Analytical Partner: **Prof. Ganna Pogrebna, PhD, AI and Cyber Futures Institute**

Photos:
cover **Artem Kniaz,** https://unsplash.com/de/fotos/eine-person-die-einen-helm-tragt-Uv6u_0xVUp8
p.4 **National Cybersecurity Coordination Centre (NSCCC NSDC)**
p.7 **Pavel Neznanov,** https://unsplash.com/photos/white-and-black-round-ceramic-plate-Dd627ieukZU
p.12 **Markus Spiske,** https://unsplash.com/photos/matrix-movie-still-iar-afB0QQw
p.15 **Locked Shields 2023 Day 1, NATO CCDCOE**
p.14 **Bermix Studio,** https://unsplash.com/photos/a-person-wearing-a-mask-using-a-laptop-56CjIvG10lo
p.16 **Lewis Kang'ethe Ngugi,** https://unsplash.com/photos/black-laptop-computer-turned-on-f5pTwLHCsAg
p.17 **Dan Nelson,** https://unsplash.com/photos/person-using-macbook-pro-on-white-table-AvSFPw5Tp68
p.24 **Vi Ko,** https://commons.wikimedia.org/wiki/File:The_silhouette_of_the_Russian_invasion.jpg
p.33-34 **CRDF Global**

The responsibility for the views expressed ultimately rests with the authors.

About Cyber Diia

Cyber Diia Platform is a non-profit public association that combines the expertise and resources of various civil organizations, research and academic institutions, companies, and international partners. This collaboration aims to foster development.

Cyber Diia has effectively utilized the extensive knowledge and experience of its staff and members. It features an Expert Advisory Board composed of renowned scholars and professionals specializing in cybersecurity, digital resilience, and innovation. The organization's management system is recognized for its excellence, having achieved the ISO 9001:2015 certification from the BVCH SAS UK Branch. This certification acknowledges Cyber Diia's proficiency in managing educational, scientific, and technical projects in areas like cybersecurity, digital transformation, and emerging technologies.

Cyber Diia also plays a crucial role in establishing an R&D network. It has set up Centers of Innovations and Competences "Cyber Diia" at four leading universities: National Aviation University, Kharkiv National University of Radio Electronics, National Technical University «Dnipro Polytechnic», and National University «Lviv Polytechnic». The team facilitates development of European Digital Innovations Hub network focusing on cybersecurity and digital resilience by uniting skills and experiences of its members and partners to enhance Ukraine's scientific and technical capabilities, fortify national resilience, assist in infrastructure rebuilding, and promote the digitization of the national economy.

Cyber Diia is playing a pivotal role in an R&D consortium tasked with developing a comprehensive digital resilience strategy for Ukraine. This project entails an in-depth analysis of the architecture and operational aspects of Ukraine's national digital services. The valuable insights derived from this examination will be instrumental in shaping a robust digital resilience strategy, focusing particularly on enhancing the resilience of the supply chain.

Furthermore, Cyber Diia actively strengthens partnerships with government bodies to boost their operational capabilities. It offers specialized support for the implementation of initiatives, focusing on adaptability and efficiency. These collaborations aim to advance digital development, scientific and technological progress, enhance national digital resilience, and support infrastructure reconstruction.
Get in touch for more info and collaboration opportunities!

Cyber Diia Platform
Email: info@cyberdiia.org | www.cyberdiia.org

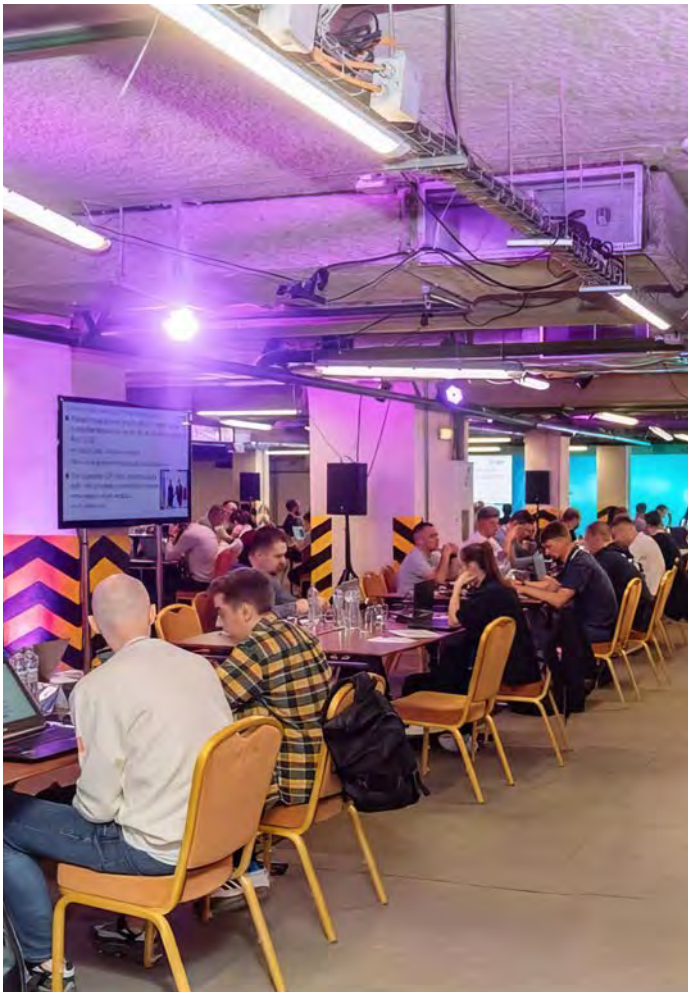
CYBER DIIA


НКЦК
CRDF GLOBAL
NATIONAL CYBERSECURITY CLUSTER
Public-Private Partnership at the International Level


NATIONAL CYBERSECURITY


NATIONAL CYBERSECURITY CLUSTER


«МАСШТАБУВАННЯ УКРАЇНСЬКИХ
РОЗРОБОК БПЛА ТА МАКСИМАЛЬНЕ
ЕФЕКТИВНЕ ЗАСТОСУВАННЯ ЇХ
НА ФРОНТІ



KYÏV
INTERNATIONAL
CYBER RESILIENCE
FORUM 2024

RESILIENCE AT THE CYBER WAR

7-8 FEBRUARY/KYIV/UKRAINE

KYIV INTERNATIONAL CYBER RESILIENCE FORUM 2024
Kyiv, Ukraine, February 7-8, 2024

Kyiv International Cyber Resilience Forum 2024 (KICRF 2024) is the main event on the Ukrainian cybersecurity landscape aimed to highlight existing challenges and tailor strategies to strengthen cyber resilience of Ukraine and its allies during the first world cyber war. The Forum will unite representatives of the public sector, tech companies, cyber community and leading experts in the field.

GOALS: Key goal of the event lies in top-level discussion of such vital issues as cyber resilience, cyber diplomacy, cyber defense and application of international law in the sector. Another important objective is to share Ukraine`s experience of cyber resistance during the first world cyber war and overview key challenges that Ukraine and leading countries` governments faced. The event will also facilitate the increase of cybersecurity level domestically and globally.

FORMAT: hybrid (0ffline/online).
The Forum will cover a plethora of sectoral events i.e. discussions focused on the national and foreign policies in the cybersecurity sector, role of cyber diplomacy, development of innovative products and startup ecosystem, National Cybersecurity Cluster, National Information Resilience Cluster, CTF, exhibition of innovative products and solutions, workshops and press-conferences.

AUDIENCE: 400-500 attendees from Ukraine and abroad.

LOCATION: Kyiv, Ukraine. The exact location will be announced the day before the event to approved participants only.

ACCESS: via registration and upon organizers` approval. Online broadcasting will be available for approximately 1000 participants via registration and upon organizers` approval.

EXPECTED KICRF 2024 RESULTS: the establishment of the platform for best practices and experiences exchange in the cybersecurity sector; identification of common strategies and coordination of efforts in countering cyber threats; strengthening of international cooperation and synergy to enhance global cyber resilience.

KEY OBJECTIVES:
Political component: facilitate mobilization of international players in the public and private sectors in terms of security and resilience issues in cyberspace.
Operational component: share experiences gained during the war in Ukraine with partner countries and shape potential fields to facilitate cybersecurity and resilience in the digital space.
Industrial component: demonstrate capabilities of the Ukraine`s national cybersecurity system and potential for the development of innovative projects in the sector.

Kyiv International Cyber Resilience Forum 2024 is organized by the National Cyber Security Coordination Center (NCSCC) under the National Security and Defense Council of Ukraine (NSDC) and the U.S. Civilian Research and Development Foundation Representation in Ukraine (CRDF Global) together with the Ministry of Defense of Ukraine, the Security Service of Ukraine, the Ministry of Digital Transformation of Ukraine and the Ministry of Foreign Affairs of Ukraine. The Forum is conducted with the support of the U.S. Department of State. Technological partners of the event are the Institute of Cyber Warfare Research (ICWR) and Cyber Unit Technologies.

The global role of cybersecurity in current wars and Ukraine`s unique experience in the first world cyber war will be among key focuses of the Forum. Another emphasis of the event will be on the overview of the international law application in the cybercrime cases and the role of cyber diplomacy for the promotion and protection of national interests abroad. The Forum will provide for multi-dimensional review of the cyber resistance facilitation through the prism of mil-tech innovations, critical infrastructure protection, public-private partnership, and counter disinformation by means of OSINT tools.

The KICRF 2024 participants will have an opportunity to participate in discussions, experts` presentations, communicate with government officials and representatives of international and Ukrainian tech companies. In addition, the attendees will have a chance to visit exhibition of Ukrainian technology products, workshops, and find out more about opportunities for donor support in the field of cybersecurity. The Forum will also include a two-day CTF for cybersecurity professionals from the public and private sectors. The competition is aimed to improve skills of the relevant specialists and master their qualifications by performing tasks developed based on the real cybersecurity incidents considering the challenges Ukraine faced in 2023.

Ukrainian and foreign representatives of relevant cybersecurity bodies, tech companies, cyber community, government officials, cyber diplomats, cybersecurity experts (CxO level non-technical and technical) and journalists will join the event.

KEY SPEAKERS:

- Oleksiy Danilov, Secretary of the National Security and Defense Council of Ukraine
- Mykhailo Fedorov, Deputy Prime Minister of Ukraine for Innovations, Education, Science, and Technology - Minister of Digital Transformation of Ukraine
- Rustem Umerov, Minister of Defence of Ukraine
- Dmytro Kuleba, Minister of Foreign Affairs of Ukraine
- Nathaniel Fick, Ambassador at Large for Cyberspace and Digital Policy, U.S. Department of State
- Mart Noorma, Director of the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)
- Jen Easterly, Director of the Cybersecurity and Infrastructure Security Agency (CISA)
- Juhan Lepassaar, The Executive Director of the European Union Agency for Cybersecurity (ENISA)

PLEASE JOIN THE FORUM VIA THE REGISTRATION

Content:

With the assistance of CRDF Global and financial support of the U.S. Department of State