State Service of
Special Communications and
Information Protection of
Ukraine

INTERNATIONAL
CYBER ENVIRONMENT
TASK FORCE

WAR AND CYBER: THREE YEARS OF STRUGGLE AND LESSONS FOR GLOBAL SECURITY

Analytical report

KYIV — 2025

CONTENT

INTRODUCTION

Over the past decade, Ukraine has become a key field for analyzing and countering modern cyber operations. The experience of the last three years (since January 2022) is particularly important, as the scale and intensity of cyberattacks have significantly exceeded all previous periods. In the context of the full-scale war, where cyber operations are coordinated with missile strikes and other military actions, Ukraine has proved its cyber resilience.

This report aims to provide a comprehensive overview of the cyber warfare landscape and help policy makers and executives make informed decisions about effective cybersecurity strategies amidst increasing international tensions. Allies in the EU and NATO can adapt these key findings and ideas to prepare for future challenges posed by states such as Russia, its allies and other states with irresponsible behavior in cyberspace. The report also includes practical recommendations for building multi-layered cyber defense at the state level, strengthening the legislative framework, and working with the private sector.

This report pays special attention to targeting, cyber victimology and the strategies behind using cyber components for intelligence gathering, destabilization, and support of military operations. These operations are no longer covert campaigns but a systematic element of military and political aggression. The scale of attacks in cyberspace, their frequency, and strategic focus differs significantly from the experiences of other countries that have experienced cyberattacks in a peaceful context.

The Ukrainian experience provides unique lessons for NATO countries by allowing analysis of the aggressor's actions under extreme stress on IT and cyber infrastructure. It also highlights the need to adopt new cybersecurity approaches to scenarios where cyber operations are integral to warfare.

This report will be valuable because it will enable you to:

1. Analyze how and why specific cyberattack targets are chosen and what is key to forming an effective defense. Ukrainian experience demonstrates that key organizations in energy, telecommunications, finance, logistics, and government administration had become prime targets in the beginning of the full-scale aggression, and how this focus scaled to military over the last three years.

2. Gain a deeper understanding of the motives and tactics of the aggressor. Ukraine's experience enables us not only to assess the enemy's methods but also to understand their long-term strategies. This knowledge allows for the identification of hidden risks, including the presence of hostile groups in the networks of allies, even before their detection.

3. Develop strategies for cooperation and organization of defense. Ukraine has demonstrated effective approaches to coordinating state, private sector, and international resources to identify risks and enhance cyber resilience. These methods combined with deeper analysis of trends highlighted in this report can serve as a foundation for developing EU and NATO member states' initiatives.

Implications for Our Allies

a. Prioritization of key sectors.

Ukraine's experience helps infer potential targets and prioritize which organizations and sectors to protect, considering the aggressor's war strategies.

b. Hunt forward operations.

Ukrainian experience reveals that many attacker groups are present in networks long before they deliver effects. Identifying such threats is key to reducing risks during escalation.

c. Collective response and data exchange.

Lessons from Ukraine demonstrate that effective cyber defense requires coordinated action at the national and international levels, including intelligence sharing and necessity of joint development of defensive solutions.

This document will help allies adapt their approaches to cyber defense according to aggressors' tactics and strategies.

SECTION 1. OVERVIEW OF CYBER OPERATIONS IN 2022–2024

During the full-scale invasion (2022-2024), the number of registered cyber incidents increased compared to 2014-2021, demonstrating a clear escalation in the Russian Federation's use of cyber warfare.

Total number of registered cyber incidents:		**Critical and high-level cyber incidents**	
2021	1350	2021	**403**
2022	2194	2022	**1048**
2023	**2543**	2023	367
2024	**4315**	2024	59
The increase in cyber incidents suggests that Russian intelligence services are prepared to escalate their use of cyber warfare tactics.		On one hand, through cooperation with and support from our partners, we have reduced the destructive impact of cyberattacks on Ukrainian organizations. On the other, aggressor's strategy is shifting from CNA to CNE operations.	

CERT-UA Registered Cyber Incidents, 2021-2024 (Quantity)

Over the last three years we observed aggressor's ability to systematically escalate attacks by involving specialized companies, cybercriminals, and "volunteers" within their armed forces and intelligence services. This may result in an increased number of attacks on government institutions, critical infrastructure, and the private sector, along with the adaptation of cyber capabilities to support ground military operations as it was deeply researched within the report "CYBER, ARTILLERY, PROPAGANDA. GENERAL OVERVIEW OF THE DIMENSIONS OF RUSSIAN AGGRESSION".

The significant reduction in critical and high-level attacks during 2023-2024 is partially due to lessons learned and close cooperation with international partners, but also due to changes in aggressor's strategy. Anyway, establishing coordination between state and private entities and the implementation of advanced monitoring and response technologies remain crucial points in ensuring cyber resilience. Its effectiveness depends also on the integration of international experience and the application of best practices in local conditions. This enables rapid response to cyber threats, reduces their criticality, and strengthens infrastructure resilience. The contributions of volunteers from the Ukrainian cybersecurity community and leading cybersecurity experts who joined cybersecurity organizations are also noteworthy.

While Ukraine is demonstrating increasingly effective countermeasures against cyber threats, the pace of vulnerability remediation and implementation of changes to enhance cyber resilience in processes and infrastructure remains insufficient. This is largely due to the scale of the challenges and shortages of resources, licensed software, equipment, and qualified personnel which should be supplementary to a coherent defensive strategy that would take attacker's tactics and priorities into account.

KEY GOALS OF ATTACKERS 2022-2024

ANALYSIS OF CHANGES IN THE LANDSCAPE AND TACTICS OF RUSSIAN HACKERS

This chapter aims to describe the shift of priorities in targeting Ukrainian entities. Initially it was based on a presupposition about the possibility of causing a significant impact to essential services with strong dependencies on power and connectivity.

The following pyramid illustrates the IT ecosystem's dependence on the energy sector (as the foundational level), telecommunications (as the key information transmission environment), and the IT systems and data that support critical civilian and military functions.

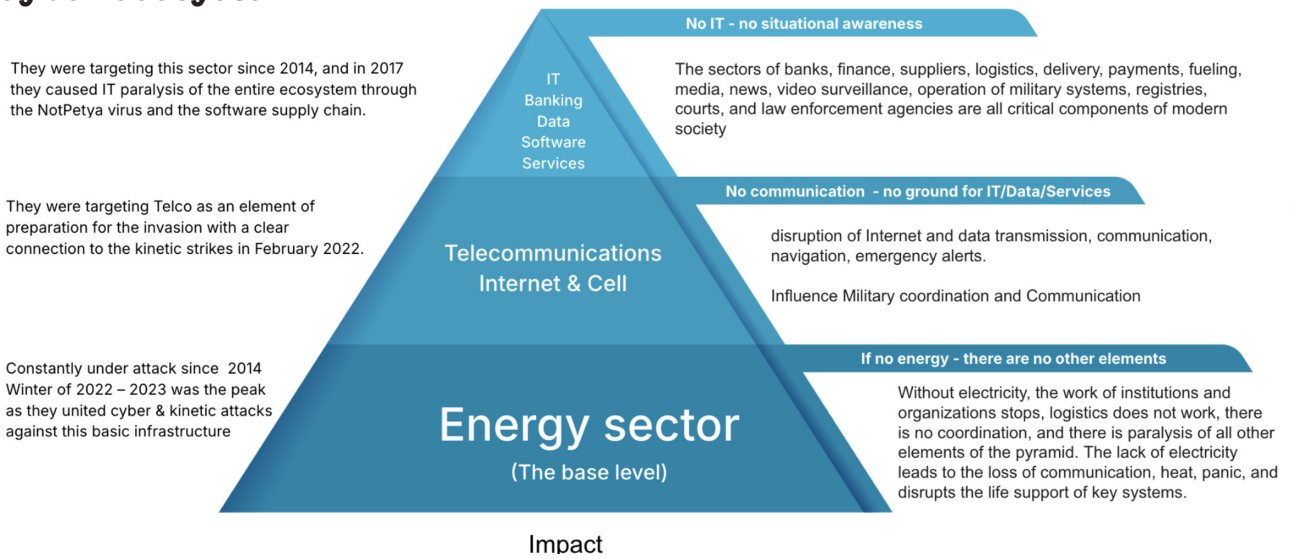
Ukraine is being attacked by:

6

Military Hacking Organizations in Russia that have APT group:

1. GRU
2. MoD
3. FSB
4. MVD
5. FSO
6. SVR

Piramide of targets & dependencies in Cyber ecosystem



Each upper level depends on the lower one, the destruction of which leads to a cascading impact on the higher levels. The cascading impact is manifested as follows:

Energy Sector: Disruptions at this level will cause communications, information and control system outages, as well as interruption of life support systems.

Telecommunications: Loss of communications at this level isolates and disorganizes society. In wartime, this triggers civil panic, limits flow of information, and disrupts social relations, as well as degrades military command and control, thereby degrading national security.

Information technology: Disruption at this level isolates organization from data and automation. This disruption halts information sharing between organizations that support the economy and generates social tensions.

Although the energy sector accounted for only 5% of the total cyberattacks in 2022, its potential impact,

34

The most Active russian threat groups CERT-UA tracking during 2022-2024 (among over 200)

UAC-0002 (SANDWORM)

A GRU unit most active in Energy & Telecom

particularly when combined with kinetic missile strikes, made it a potential source of devastating consequences for the Ukrainian population. However, thanks to a swift response, specialists were able to prevent power outages in most cyberattack incidents.

MOST TARGETED SECTORS, 2021-2024

2021		2022		2023		2024	
1350		2194		2543		**4315**	
Public Sector and Local Governments	20%	Public Sector and Local Governments	26%	Public Sector and Local Governments	25%	Public Sector and Local Governments	58%
Security and Defense Sector	16%	Security and Defense Sector	14%	Security and Defense Sector	7%	Security and Defense Sector	18%
Commercial sector	6%	Commercial sector	6%	Commercial sector	5%	Energy sector	6%
Financial sector	6%	Financial sector	5%	Energy sector	4%	Commercial sector	3%
Energy sector	3%	Energy sector	5%	Telecom sector	4%	Telecom sector	2%

CHANGE OF STRATEGY AND THE ROLE OF THE CYBER COMPONENT IN SUPPORTING MILITARY OPERATIONS

2022

In 2022, the Russian Federation intensified its cyber activities, using cyber operations as an important tool to support its military actions. The main emphasis was on destructive cyber operations aimed at disrupting critical infrastructure, stealing data, and exerting information and psychological influence. Russian hackers planned to launch a cognitive attack by hacking media outlets, significantly overestimating the impact on Ukrainian public opinion.

Between the NotPetya attack in 2017 and 2022, Ukraine did not experience further large-scale destructive cyberattacks. Nevertheless, this allowed government agencies to develop cyber defense infrastructure (e.g., the opening of Cyber Center UA30), improve regulations, and prepare for the escalation of cyber aggression.

Instead, the enemy focused on identifying vulnerabilities in the networks of Ukraine's public and private sectors. Many early 2022 cyberattacks exploited existing vulnerabilities, with a significant number of systems having been compromised as early as 2020-2021. The enemy leveraged pre-installed backdoors to quickly launch cyberattacks against critical systems. This already illustrates aggressor's evolution from probe operations (e.g. BlackEnergy, Industroyer and NotPetya) to a full-scale cyber campaign.

80

Breaches attributed to UAC-0002 (Sandworm) during 2022-2024
(2 per month)

Biggest Telco breach impact: 25M users lost cell and internet connection for 1 week

Aha moment:
The attack was temporally linked to massive missile strikes and led to a temporary shutdown of mobile communications

KEY TACTICS AND GOALS

1. Destructive Cyberattacks.

Russia actively employed the tactic of destroying key IT infrastructure and paralyzing services. The primary focus was on energy, telecommunications, government institutions, and transportation/logistics. Malware such as WhisperGate, HermeticWiper, and Industroyer2 caused short-term disruptions, but these efforts failed to cause a global shortage of essential services and achieve a shift in strategic balance.

8
new types of destructive viruses recorded during 2022

2. Cyber Impact on Media and Disinformation.

As a manifestation of a cognitive warfare, media became one of key targets for the Russian Federation. Hacks of television channels, news agencies, and online platforms aimed to spread propaganda and intimidate the population. By disseminating fake news and manipulative materials using the logos of well-known media outlets, the aggressor attempted to create chaos, undermine trust in Ukrainian information sources, promote pro-Russian narratives, and demoralize the population.

More than 200 cyberattacks on Ukrainian media to spread propaganda, manipulate public opinion, and create chaos: Russian hackers targeted news agency websites and state media outlets, such as Ukrinform, to spread fake news or completely erase content. The use of wiper programs and DDoS attacks led to temporary shutdowns of media resources, hindering access to accurate information. A common method involved compromising social networks and journalists' accounts to spread disinformation.

200
Successful attacks on media

With the beginning of the full-scale war, Russia actively used deepfake technologies to spread disinformation and create propaganda materials. A prominent example was the attempt to publish a deepfake video of the President of Ukraine seemingly calling for surrender. Although quickly debunked, the brief circulation of the video on social media and messaging apps aimed to sow panic and undermine confidence in state institutions. Throughout all three years of the full-scale war, propagandists used videos depicting fake meetings of Ukrainian politicians, compromising statements, or alleged corruption to destabilize the political situation and influence international support for Ukraine. These materials were often combined with other forms of disinformation, such as fake news and phishing campaigns. Russia used deepfakes to discredit Ukrainian military commanders, volunteers, and international partners, imitating their speeches or statements.

12
Telecom providers hacked in just 3 months 2023

Also, enemy hackers tried to interfere in the information space and influence public opinion both in Ukraine and abroad, actively using bot networks, fake accounts, and paid posts to create the impression of mass support for pro-Russian narratives among Ukrainians.

These actions became part of the cognitive war, which combines cyberattacks, psychological pressure, and disinformation to achieve the strategic goals of the aggressor, trying to destabilize the situation in Ukraine and cast doubt on its internal unity and international support.

KEY INCIDENTS OF 2022

WhisperGate (January).

Data destruction malware against public systems. This was the first signal of the Russian Federation's preparation for large-scale destructive cyberattacks.

HermeticWiper (February).

A large-scale cyberattack on the eve of the invasion, which disabled systems in the state and private sectors.

IsaacWiper (February).

Cyberattack on government institutions that coincided with the beginning of the full-scale war.

AcidRain (February).

Cyberattack on Viasat satellite communications that disrupted communications in Ukraine and Europe.

Industroyer2 (April).

Cyberattack aimed at the energy sector, which aimed to create power outages.

100

Average number of Ukrainian commercial companies per month where hackers have access and steal money

WHY OFFENSIVE CYBER OPERATIONS OF THE RUSSIAN FEDERATION DIDN'T CAUSE A DRAMATIC IMPACT?

1. Resilience of Ukrainian Society.

Ukrainian society, hardened by a decade of conflict, demonstrated strong psychological resilience against disinformation and information manipulation in the beginning of the full-scale invasion. Attempts to spread fake news and false reports of government surrender failed to achieve the desired effect.

175

incidents related to the Security and Defense Forces were registered in 2023

2. Rapid Response to Incidents.

CERT-UA and its partners swiftly detected and neutralized malware, restored systems functionality, and mitigated the impact of cyberattacks. This minimized the duration and consequences of disruptions.

3. Support from International Partners.

Strong support from Western partners enabled Ukraine to access threat intelligence, monitoring tools, and real-time protection, strengthening its response capabilities.

2023

In 2023, Russian hacker groups shifted their strategy from simple DDOS and wide-range opportunistic attacks to more focused cyber activity. They began experimenting with new tactics, focusing on establishing a presence in key facilities, engaging in covert intelligence gathering, and using cyber capabilities to assess the impact of their kinetic strikes.

Signal

The main messenger used by attackers to attack the military

In the second half of 2023, activity from well-known groups like UAC-0001 (APT28) and UAC-0003 (Turla) decreased significantly. Instead, new and previously unknown hacker groups emerged, employing novel tactics and techniques for their cyberattacks. The increasing number of technically complex attacks

necessitated strengthening Ukraine's cyber resilience, intensifying international cooperation, and engaging IT specialists from the private sector.

KEY TRENDS OF 2023

1. Cyberattacks targeted telecommunication resources to degrade communications in the rear and on the front lines

- One of the most critical areas of cyberattacks was telecommunications providers, such as Kyivstar, Citylan, and others. These attacks aimed to disrupt data transmission, destroy communications, and create strategic advantages on the battlefield.
- Hacks of these networks demonstrated a high technical level of attackers and became a serious challenge for cyber defense.

UAC-0010
(Gamaredon, Primitive Bear)
affiliated to FSB Center 18 — the most active group with 829 registered incidents for 3 years
Team Velocity: 23 incidents per day in average

2. Espionage and Persistence

- Groups associated with the FSB, GRU, and SVR maintained long-term presence in systems and constant collection of intelligence data.
- Attackers created fake versions of software, which they distributed among target users, including military structures.
- Particular attention was paid to attacks on messengers popular among the military for the collection of critical data.

3. Cyberattacks on Media and Disinformation Campaigns

- Starting in April 2023, attackers focused on compromising news agencies, social networks, and messengers to spread provocative information.
- Telegram channels were used to publish stolen documents, technical schemes, and other materials to demoralize and influence public opinion.

4. Financially Motivated Cyberattacks

- In the second half of 2023, 40% of registered incidents were related to extortion and theft of funds.
- The main methods included the use of Remote Access Trojans (RATs), phishing campaigns, and cyberattacks on banking systems.
- Financial attacks targeted both large businesses and government institutions, causing significant economic losses.

801
Financial incidents affiliated with group UAC-0006

5. Information Support for Cyberattacks

- Publication of technical details of attacks and stolen documents in open channels increased significantly, creating information pressure on victims.
- Cyberattacks were synchronized with physical strikes, enhancing their psychological impact.

MAIN CHANGES IN TACTICS

Return to Previous Victims.

APT groups leveraged their knowledge of previous targets' infrastructure to re-attack critical systems.

Scaling offensive cyber capabilities.

New actors strengthened established groups, demonstrating innovative and harder-to-detect cyberattack methods.

Information Influence.

Weaponizing stolen data to spread disinformation became part of their psychological warfare strategy.

2024

In 2024, Russian hacker groups' strategy continued to evolve. The focus of cyberattacks shifted to entities directly related to military operations and service providers supporting the war effort. Attackers sought to remain undetected for as long as possible, establishing persistence within systems and gaining access to sensitive information to support Russian military operations.

Hackers demonstrated a focused approach, targeting strategically important objects to achieve their goals. This included stealing messenger accounts to spread malware and orchestrate phishing campaigns.

MAIN TRENDS OF THE YEAR

1. Shift From Critical Attacks And Incidents To Data Collection

While the number of cyber incidents continued to increase in 2024, the proportion of critical and highly serious incidents decreased.

Concurrently, cyberattacks on government organizations and local authorities significantly increased, accounting for up to 60% of all incidents which may be related to initial access attempts through phishing and malware distribution.

15

key government registries affected by attacks that paralyzed the work of approximately 15 million people (half the population) for 3 weeks

2. Fewer Direct Attacks on Critical Infrastructure

Instead of directly attacking critical infrastructure objects (CIOs), attackers increasingly targeted the supply chain, compromising suppliers and developers of specialized software.

This approach allowed them to remain undetected while gaining access to critical systems through less secure supply chains.

3. Phishing and Social Engineering

Phishing campaigns remain a primary tool for hackers. In 2024, these campaigns became more sophisticated, employing multi-stage schemes and exploiting linguistic and cultural nuances to enhance their effectiveness.

For example, UAC-0010 (Gamaredon) actively used social engineering to steal military and personal data, as well as gain access to government systems. Other campaigns focused on distributing malware through attachments disguised as documents related to state or humanitarian aid.

4. Evolving Cyberattack Techniques

Exploitation of Border Gateways: Attackers create SSH tunnel chains using TOR to hide their location and spoof Ukrainian IP addresses.

Instant Data Theft: Malware rapidly exfiltrates data without long-term presence in systems.

Cyberattacks on Messengers: Messenger applications such as Telegram, WhatsApp, Signal, Element, and Discord spread malware and conduct phishing scams.

Penetration Through Web Resources: Publicly available web resources remain the main target of attackers. They actively exploit vulnerabilities, looking for new entry points and returning to previously attacked systems.

SECTION 2. UKRAINIAN CYBER DEFENSE STRATEGY: FROM RESILIENCE TO ACTIVE DEFENSE

KEY CHALLENGES

- Limited resources (finance, licensed products, highly qualified personnel on the ground) prevent technological upgrades to IT systems, which limits overall protection of Ukrainian cyber infrastructure. This hinders the correct configuration and safe use of such systems. This problem is inherent not only in Ukraine and is common in the world. Underfunding of cybersecurity can usually be associated with a low level of awareness, a lack of regulatory requirements, or a weak economy. Ukraine, on the other hand, is the object of targeted aggression by a country that is considered a cyber power in the world, which means that the task of Ukrainian cyber defenders is even more difficult.
- Cyber security relies on trust and information sharing and can be significantly degraded when those practices are undermined. As in many countries, Ukraine lacks a hierarchy in the national cybersecurity system, which sometimes leads to a lack of coordination. The trust of businesses and citizens in the main cybersecurity organizations increased during the full-scale aggression, but still remains at an insufficient level.
- Lack of responsibility for non-compliance with regulatory acts, requirements, and recommendations. If we are talking about state organizations, the indifferent attitude of management and the lack of focus on cybersecurity often replace insufficient funding, which complicates holding accountable in the event of cyber incidents. The lack of adequate cyber defense measures in the private sector is primarily due to insufficient regulation. Even despite the presence of a state MSSP in the form of the State Cyber Defense Center and a number of private MSSPs, the demand for their services is extremely low.
- Outdated regulatory framework in the field of cybersecurity that does not correspond to the realities of the full-scale war. Although since 2020 the State Service of Special Communications and Information Protection has ensured the implementation of advanced approaches in the field of cyber defense at the level of bylaws, the overall situation with the legislative support of strengthening cyber defense and responsibility for its absence requires significant changes. During 2023-2024, several unsuccessful attempts were made to adopt laws that would not only update the requirements in the field of cybersecurity and information protection but also implement the norms of the NIS2 directive into Ukrainian legislation.
- Cyber security expertise is critical to reducing cyber risk. Qualified information system security officers are desperately needed to lead protection activities. This is explained by both gaps in legislation and a low level of awareness of the issues by the owners and managers of these organizations, leads to an increase in cyber security risks, non-compliance of processes with the requirements of standards, and a lack of responsibility in the event of cyber attacks on critical service providers.
- The lack of cyber forces and cyber command leads to a lack of strategy and dispersion of resources that could be used for military response in cyberspace during a full-scale war. Despite the presence of a Presidential Decree valid since August 2021, the law on the creation of cyber forces has not yet been voted on by parliament.

HOW UKRAINE MANAGED TO WITHSTAND

1. Ukraine built its cyber defense program during an active cyber campaign.

2021 can be characterized as the beginning of structural reforms in the field of cyber defense, which became a key factor in the state's readiness to resist cyber aggression. Following the Russian invasion, Ukraine significantly strengthened its cyber defense personnel by recruiting leading IT and cybersecurity experts from the commercial sector. Our cyber defense works in conditions of war, energy crises, and daily DDoS attacks.

Ukraine's experience is unique globally: the digital resilience model, implemented by the government in partnership with private companies and international technology partners, has demonstrated how decisive action can protect critical government data.

Ukrainian cybersecurity is a collaborative effort between the government, the private sector, and civil society. Cooperation with partners and effective interaction among government structures, the IT community, and volunteers has formed the foundation of our cyber resilience.

2. Ukrainian specialists have become some of the most experienced cyberattack defenders globally.

Daily engagements with advanced persistent threat (APT) groups have elevated our expertise to an unprecedented level.

Ukraine has learned to transform every attack into an improvement of its systems.

Every attack is a lesson, and every incident presents an opportunity for improvements. Ukraine shares its experience with partners and allies, thereby contributing to the global security ecosystem, and is ready to become an active participant in the global cyber police.

3. The future of global cyber security may depend on the efforts in Ukraine.

Joint exercises, data exchange, and technical support are a contribution to the world of safer digital borders.

Our approaches to protection and interaction, which by trial and error have been crystallized on a national scale, can be used globally.

Due to strategic communications and proven professionalism, CERT-UA purposefully builds trusting relationships with the ecosystem and establishes contact with all victim organizations. This allows not only to prevent cyber incidents but also to speed up investigations, respond, and share the acquired experience with the community.

4. Rapid Cyber Restoration

Cyber Resilience is the ability to timely detect and prevent cyberattacks, as well as the ability to quickly restore data, services, and infrastructures after cyber incidents. Ukrainian government teams of IT specialists, under the coordination and methodological and practical assistance of the State Service of Special Communications, together with international partners, ensured:

- Migration to Cloud Environments: Key government data has been moved to secure data centers in the EU and the USA, which has reduced the risks of physical destruction or capture of data centers, power outages, and damage to communication systems.

- Ensuring the Availability of Critical Information Resources: Back-up copies and access channels to important resources and applications have been created to reduce the likelihood of their loss during enemy attacks or technical failures.
- The development of the capacities of the National Center for Reserving Government Information Resources allowed the launch of new registers and digital services aimed at helping the population during the war, as well as: ensuring the smooth operation of government bodies during crisis situations.

These measures made it possible to preserve the functioning of key government institutions and services, ensuring data security and infrastructure stability in conditions of constant cyber threat.

5. Building international collaboration and interoperability

International cooperation in cyber security has become one of the key elements of Ukraine's resilience in resisting Russian aggression in cyberspace. Ukraine actively cooperated with government agencies and cyber defense teams of partner countries (CERTs/CSIRTs and similar structures), as well as leading cyber security companies to:

- Detect and neutralize cyber attacks on critical infrastructure and government information systems;
- Exchange operational information about new types of malware, tactics, and techniques used by Russian hacker groups;
- Conduct joint exercises and training to increase the speed of response to incidents;
- Strengthen early warning systems about threats in cyberspace.

Close cooperation with countries such as the USA, Great Britain, partners from the EU and NATO countries made it possible to quickly localize the consequences of cyber attacks and improve Ukraine's overall cyber resilience. A significant role in this process was played by both state institutions and international private companies in the field of cyber security, which provided technological and expert support.

The Ukrainian experience has become valuable for the global community, demonstrating the need for consolidated efforts to counter cyber threats in the modern world.

SECTION 3.
CONCLUSIONS AND RECOMMENDATIONS

Understanding adversary's strategy

- It is important to understand the adversary's key objectives, their initial strategy, and how it changes over time. This can be understood by analyzing cyber incidents and trends, what information the enemy is interested in, and by sharing intelligence with partners about the aggressor's strategic targets.

Strengthening International Cooperation

- **Conduct Large-Scale Cyber Exercises:** In crisis situations, both the personal experience of specialists and the skills of teamwork and practiced action scenarios become critical. It is advisable to intensify joint cyber exercises for operational teams (CERTs/CSIRTs) at the national, sectoral, and object levels, aimed at detecting, deterring, and neutralizing threats in real-time. This will give partner countries the opportunity to adapt to new tactics and techniques of Russian hacker groups and increase the overall speed and effectiveness of response to incidents.
- **Global Security requires shared data and analysis:** Established channels of information exchange about threats, a high level of trust between participants of the ecosystem, automatic procedures for enriching knowledge of cyberattack countermeasures systems, and consideration of experience in responding to specific cyber incidents are key to forming collective security systems in cyberspace. Integrated platforms for prompt exchange of information about cyber threats, malware, indicators of compromise (IoC), and attack methods can be the key to this. Such cooperation will help partners quickly respond to common threats and prevent their spread.
- **Investments in Joint Cyber Platforms:** Technologies and means of cyber defense require not only scaling from government organizations and the corporate segment to small and medium-sized businesses but also constant updating and improvement. Today's challenges require expanding financial and technical support for the development and modernization of cyber defense infrastructure, in particular through joint platforms for monitoring, threat analysis, and coordination of actions. This will ensure the resilience of partner countries to future large-scale attacks.

Strengthening Sanctions Against the Russian Federation

- Through deanonymization and OSINT, it is necessary to intensify work on identifying persons and imposing sanctions against specific members of Russian hacker groups who carry out attacks on the critical infrastructure of Ukraine and other countries. Groups such as **UAC-0004 (APT29)**, **UAC-0002 (Sandworm)**, and **UAC-0108 (Killnet[t])** should be recognized as a threat to international security. Technological sanctions against the Russian Federation, personal sanctions against the leadership of special services and their cyber units, as well as cyber security companies affiliated with the Kremlin and Russian special services must be maintained and strengthened.
- A feature of modern cyber aggression is the widespread use of tools for hacking IT infrastructures that provide services to the civilian population. Cyber crimes intentionally committed against civilian infrastructure during martial law by state or affiliated units of the aggressor must be qualified by the international community as war crimes.

Supporting the Development of National Cyber Capabilities

- **Technological Assistance.**

  Countries that are objects of Russian cyber aggression should be given access to advanced cyber defense technologies, in particular, early warning systems, threat analysis based on artificial intelligence, and platforms for automating response to cyber threats.

- **Educational Initiatives.**

  The personnel reserve can serve as a significant mobilization resource in the event of full-scale cyber aggression. It is necessary to expand training programs for specialists in the field of cyber security, including scholarships, exchange of experience, and the involvement of international trainers.

Engaging Businesses to the Protection of States

Cooperation with the private sector in IT and cybersecurity should maximize the existing potential for preventing cybercrime, cognitive influence, and infiltration of the aggressor's special services into critical infrastructures. It is necessary to more actively businesses in cooperation in detecting attacks, neutralizing malware, and blocking the infrastructures of hacker groups.

These measures will contribute to strengthening global cyber resilience, ensure effective protection of digital infrastructures from destructive attacks, and make it impossible for cyber criminals to go unpunished in the modern world.

For comments and explanations, please contact: press@cip.gov.ua

We are in social networks:

https://twitter.com/SSSCIP

https://twitter.com/_CERT_UA

https://www.facebook.com/dsszzi

https://www.whatsapp.com/channel/0029Vab3J3Q8vd1NmUckuj3n

https://www.instagram.com/dsszzi

State Service of
Special Communications and
Information Protection of
Ukraine

INTERNATIONAL
CYBER ENVIRONMENT
TASK FORCE

WAR AND CYBER:
THREE YEARS OF STRUGGLE AND LESSONS FOR GLOBAL SECURITY

Analytical report

KYIV — 2025