НКЦК
НАЦІОНАЛЬНИЙ КООРДИНАЦІЙНИЙ
ЦЕНТР КІБЕРБЕЗПЕКИ

# Review of cybersecurity news in Ukraine, tendencies, and world events related to the First World Cyber war

March 2023

USAID
FROM THE AMERICAN PEOPLE

Prepared with the support of the USAID Cybersecurity for Critical Infrastructure in Ukraine Activity.

This publication is made possible by the support of the American people through the United States Agency for International Development (USAID). The authors' views expressed in this publication do not necessarily reflect the views of USAID or the U.S. Government.

# CONTENT

**ACRONYMS** 4

**KEY TENDENCIES** 5

**1. FIRST WORLD CYBER WAR** 8

U.S. Consulate Hacked by "Putin Supporters" 8

Overview of Hacktivists in Russia's War against Ukraine 8

Russia Attempts to Block Starlink Use by Jamming GPS, Says Defense One 8

Russia Bans Foreign Messaging Apps 8

Year of Wipers: How Kremlin-Backed Sandworm Attacked Ukraine During the War 9

Russia Remains a "Very Powerful Cyber Adversary", Says Nakasone 9

Russia-Linked TA499 Stages Attacks Via Video Calls 9

False Air Raid Alarm Causes Panic in Moscow and Other Regions of Russia Once Again 9

Russia Prepares for New Phase of Cyberwarfare, Microsoft Warns 10

Pro-Russian Hackers Step Up Attacks on Hospitals, Researchers Warn 10

Kaspersky Lab Detects New Virus Used in Cyberattacks in Donbas and Crimea 10

Cybersecurity Assistance to Ukraine Provides Crucial Experience for Cybersecurity Companies, Says Cisco Talos 10

New U.S. Cyber Security Strategy Draws on Experience of Russian-Ukrainian War 11

What Can Intelligence Services Learn from a Year of Cyber Warfare? 11

Russia Eases Employment and Residence Permit Process for Foreign IT Specialists 11

Russian "Winter Vivern" Hackers Found Complicit in Attacks against Ukraine, Europe, and India 11

Linux Rejects Patches for Its Driver from Russian Baikal Electronics Company 12

Kremlin-Backed Hackers Accused of Recent Phishing Attempts against EU Agency 12

Russian Rostec Can Allegedly De-anonymize Telegram Users 12

Experts Analyze Media Coverage of the War in Ukraine 12

**2. CYBERSECURITY SITUATION IN UKRAINE** 13

Ukrainian teams won prizes in NATO TIDE Hackathon 2023 13

NCCC Secretary Nataliya Tkachuk at the Phoenix Challenge forum called on Western partners to join forces to counter disinformation 13

In the first month of the Protective DNS system operation, Ukrainians' losses from financial phishing decreased by more than 30% 14

NCCC started cooperation with the international company "Internet 2.0" 14

SBU exposed attempts by Russian special services to collect intelligence in Ukraine "on behalf" of foreign media 14

The SBU exposed fraudsters who "collected" money for the Armed Forces "on behalf" of local authorities 15

The SSSCIP held a workshop on cyber security culture for human resources specialists in the public sector 15

Russia's Cyber Tactics: Lessons Learned 2022 – analytical report of the State Special Communications Service on the year of Russia's full-scale cyber war against Ukraine 15

SSSCIP intensifies cooperation with higher educational institutions of Ukraine 16

Protecting personal data of Ukrainian citizens remains one of the biggest challenges in Russia's cyber war against Ukraine 16

In 2022, Gamaredon carried out 74 cyber attacks against Ukraine 16

Russian hackers distribute infected software via torrents 17

Digital transformation and cyber security: European partners support Ukraine 17

Cybersecurity and digital currencies are new trends in Govtech 17

The Cyber Police became a partner in the project to identify crypto wallets associated with terrorist and sanctioned activities 18

Cyber police exposed a Khmelnytskyi Oblast resident for creating a "virus" to steal user data 18

Cyber police officers improve their skills in detecting crimes committed using virtual assets 18

Cyber police exposed a hacker group member involved in ransomware attacks that caused €40 million in damages to European companies 19

The cyber police team got to the top five at the NATO TIDE Hackathon 2023 19

Cyber police exposed a criminal group that took out loans on behalf of missing and captured servicemen 19

Cyber security and cyber intelligence training for security and defense sector specialists at the NCCC 20

The NCCC is working on improving the regulatory and legal framework in the field of cyber security 20

Ukraine is working on technological solutions together with European partners 21

The Cabinet of Ministers adopted a resolution standardizing the implementation of an independent audit of information security systems at critical infrastructure facilities 21

Cyber attacks on Ukraine: with the help of hackers, Russia tries to get any information that can give it an advantage in its conventional war 22

SBU exposed an enemy botnet in Khmelnytskyi Oblast that amplified fakes about the war in Ukraine 22

Cyber police exposed suspects in financing the occupiers 22

Members of a criminal organization will be tried in Lviv Oblast for fraud under the guise of government benefits 23

# ACRONYMS

| | |
|---|---|
| **AI** | Artificial Intelligence |
| **CERT-UA** | Government Computer Emergency Response Team |
| **CISA** | Cybersecurity & Infrastructure Security Agency |
| **CRDF Global** | Civil Research and Development Fund (U.S.) |
| **CSIRT** | Computer Security Incident Response Team |
| **CWIX** | Coalition Warrior Interoperability eXploration, eXperimentation, eXamination eXercise |
| **CYBERCOM** | United States Cyber Command |
| **DDoS** | Distributed Denial-of-Service |
| **DNS** | Domain Name System |
| **DT4UA** | Digital Transformation for Ukraine |
| **ENISA** | European Union Agency for Cybersecurity |
| **EU** | European Union |
| **EU4PAR** | Support to Comprehensive Reform of the Public Administration in Ukraine |
| **FSB** | Federal Security Service (Russian Federation) |
| **FVEY** | Five Eyes Intelligence Alliance |
| **GPS** | Global Positioning System |
| **HR** | Human Resources |
| **LDNR** | so-called Luhansk and Donetsk People's Republics |
| **MDT** | Ministry of Digital Transformation of Ukraine |
| **NATO** | North Atlantic Treaty Organization |
| **NCCC** | National Coordination Cybersecurity Center |
| **NSDC** | National Security and Defense Council of Ukraine |
| **OT** | Operational Technology |
| **PSYOP** | Psychological Operations |
| **RaaS** | Ransomware as a Service |
| **SBU** | Security Service of Ukraine |
| **SSSCIP** | State Service of Special Communications and Information Protection of Ukraine |
| **TIDE** | Think-Tank Information Decision and Execution |
| **U.S.** | United States |
| **UAH** | Ukrainian Hryvnia |
| **UAV** | Unmanned Aerial Vehicle |
| **UK** | United Kingdom |

# KEY TENDENCIES

In March, the new U.S. National Cyber Security Strategy was released. The document defines five main (strategic) U.S. spheres of interest, including security of critical infrastructure, the fight against ransomware by all possible means, and more attention to the education of cyber professionals. Among the important innovations is the requirement for "safe coding." The expert community is discussing the extent to which this requirement may affect innovation processes in the United States and the competitiveness of U.S. IT companies in the world market. Some experts emphasize that, internationally, the U.S. strategy in cyberspace differs from the more restrained approach that the Biden administration is applying to the Russian-Ukrainian war.

The European Union (EU) continues to modify its cybersecurity legislation to create a safer European cyberspace. Currently, the main line of discussion concerns the norms of the future Law on Cyber Resilience; member states continue a complex debate on the severity of restrictions it can impose on market participants, including on the exchange of information on cyber incidents and the role of the European Union Agency for Cybersecurity (ENISA) and national Computer Security Incident Response Teams (CSIRTs) in this process. However, a draft of a new regulatory document, the Cyber Solidarity Law, will also be presented in April. This document would create a pan-European network of private sector cyber security organizations that can come to the aid of the EU in the event of a large-scale cyber attack (which is one of the lessons of the Russian-Ukrainian cyber war).

Ukrainian specialists from the State Service for Special Communications and Information Protection (SSSCIP) track trends in Russian cyber threats. The report Russia's Cyber Tactics: Lessons Learned 2022 was published, which summarizes Ukraine's experience in countering Russian aggression in cyberspace during 2022. The authors investigated the main groups and their motivations, methods, and tools of attacks. In 2023, Government Computer Emergency Response Team (CERT-UA) specialists note an increase in the number of espionage attacks with an emphasis on maintaining persistent access to the organization, which may mean that the Russian Federation is preparing for a long war.

Ukraine continues to develop international cooperation to jointly counter cyber threats. In March, Ukrainian government agencies began cooperating with several international companies, for example, with the Australian organization Internet 2.0, and there is a dialogue with European analytical centers (Lisbon Council). In addition, in cooperation with the law enforcement officers of Germany, the Netherlands, the Federal Bureau of Investigation and with the support of Europol, a member of the hacker group involved in the DoppelPaymer ransomware was exposed.

The United States continues to pay increasing attention to critical infrastructure and security of its operational technology OT) systems. The Cybersecurity & Infrastructure Security Agency (CISA), in conjunction with both public and private other entities, produces various guidelines for assessing the state of enterprise cyber security in certain sectors (e.g., transportation) and penetration testing individual critical infrastructure facilities (with the help of its own red team), is establishing a process for cyber incident information exchange, and even is launching preventive information programs about cyber security threats. These initiatives not only implement previously adopted documents, but also correspond to the spirit and letter of the new U.S. National Cyber Security Strategy.

Ukraine is strengthening its current and future resilience to cyber threats. Ukrainian specialists successfully participate in international competitions, taking top places in the NATO Think-Tank for Information Decision and Execution (TIDE) Hackathon 2023. The qualification of cyber police officers and cyber defenders is continuously improved. To ensure future cyber resilience, Ukraine is intensifying cooperation with Ukrainian higher educational institutions.

The U.S. Armed Forces continue to increase their cyber potential and capabilities: they launch training programs for their own programmers (on the basis of the Marine Corps), draft manuals for certain zero trust policies, and continue to deploy response teams around the world. As a result, the Pentagon is asking to increase the funding for these activities in 2024 by 21%, up to $13.5 billion.

In March, hacker groups associated with the People's Republic of China became active. They resort to traditional cyber espionage practices, looking for new methods and attack vectors. State institutions, analytical centers, and critical infrastructure facilities in various sectors of the economy fall within their primary sphere of interest. Meanwhile, Chinese telecommunications equipment manufacturers continue to compete in the European market, integrating themselves into large infrastructure projects, for example, as a partnership with Deutsche Bahn. Most likely, this will cause another round of debate about the limits of using Chinese telecom products in various critical infrastructure sectors.

Russian hackers continue their campaign against Ukraine's allies in the global cyber war. CISA has warned about the threat of using Royal ransomware against critical infrastructure facilities in the U.S.A. Russia is testing new attack techniques, increasing cyberattacks against hospitals, attacking European organizations and government officials' social media accounts. At the same time, Russia is looking for opportunities to expand the personnel base in the field of cyber security, in particular, it is simplifying rules for foreign specialists to obtain a permanent residence permit.

Experts assess Russia's cyber activity as its preparation for a new stage of confrontation. They have already tried to block Starlink operation in the war zone through electronic warfare and create new ransomware and vipers. It is also reported that the Russian military can determine the exact location of the terminals, which forces the Ukrainian military to use them only if necessary. Ukraine's partners remind that although Russian cyber capabilities could not show a noticeable effect in the first stages of the war, they should not be underestimated and the parties should be ready for a long confrontation in cyberspace.

The confrontation between the U.S. and China in the sphere of Internet and technology continues. Cooperation between the U.S. private and public sectors in this matter is noted, as well as the intention of U.S. lawmakers to ban the Chinese application TikTok out of U.S. citizen privacy and national security concerns. A report submitted to the special committee of the Australian Senate on Foreign Interference through Social Networks emphasizes the links of Chinese technology companies with the Chinese Communist Party. The struggle between China and the United States is also taking place at the level of physical Internet infrastructure, as laid out in a special Reuters report.

# 1. FIRST WORLD CYBER WAR

## U.S. CONSULATE HACKED BY “PUTIN SUPPORTERS”

On February 28, Newsweek reported that the Twitter account of the U.S. Consulate General in Milan had been taken over by a group of hackers claiming to be Russian-speaking Ukrainians, who spread a series of anti-Ukrainian messages, including a comparison of Ukraine to Nazi Germany. The post, which received at least 149,000 views, was deleted later that morning.

## OVERVIEW OF HACKTIVISTS IN RUSSIA’S WAR AGAINST UKRAINE

GroupSense has identified 42 hacktivist groups that are operating in Ukraine’s interests, compared to 36 groups that act on behalf of Russia. Among the most prominent Ukrainian groups are the IT Army of Ukraine, AgainstTheWest/BlueHornet, Network Battalion ‘65, DoomSec, and GhostSec.

Several Russian ancillary actors have been identified, including Killnet, Zarya, NoName057(16), Beregini, and Nemezida. XakNet is another group that presents ambiguity; while it claims to be an independent patriotic hacktivist organization, many observers suspect it is actually a division of one of Russia’s intelligence services. The attacks perpetrated by these groups tend to target countries that were formerly part of the Warsaw Pact.

## RUSSIA ATTEMPTS TO BLOCK STARLINK USE BY JAMMING GPS, SAYS DEFENSE ONE

On March 1, an article was published describing the current situation with Starlink use by the Ukrainian military in the combat zone. The article highlights that Russian troops, unable to block communication with the satellite group directly, have resorted to other methods of interference. One tactic involves jamming GPS signals, which Starlink uses to select which satellites to transmit its signals from, thereby interrupting its operation.

## RUSSIA BANS FOREIGN MESSAGING APPS

On March 1, Roskomnadzor banned the use of several foreign messaging apps in government agencies. The decision follows the enactment of Parts 8-10 of Article 10 of the Law “On Information, Information Technologies, and Protection of Information.” The affected applications are those that allow direct messaging, do not provide for open posting of information on the network, and are owned by foreign entities. The banned list includes popular apps such as Discord, Microsoft Teams, Skype for Business, Snapchat, Telegram, Threema, Viber, WhatsApp, and WeChat.

According to Computing, other foreign apps such as Zoom remain unaffected by the ban. Roskomnadzor’s statement does not specifically accuse them of subversion or direct complicity in the activities of anti-Russian forces, unlike the case with the ban on Facebook and Instagram.

## YEAR OF WIPERS: HOW KREMLIN-BACKED SANDWORM ATTACKED UKRAINE DURING THE WAR

On March 1, The Record published an analysis of the Sandworm group's activities, an organization affiliated with the Russian Central Intelligence Directorate. According to the report, Sandworm's most significant contribution to the cyber aspect of Russia's war against Ukraine was the deployment of the Wiper malware. Although the malware attempted to bypass Ukrainian defenses, it ultimately failed to meet expectations.

Sandworm failed to mount attacks against Ukraine's infrastructure, including the energy grid. Instead, the group deployed ransomware against targets of interest to Russia, particularly to retaliate against organizations that provided material aid to Ukraine.

"Sandworm hackers also contribute to PSYOPs," the report notes. "For example, they spread conspiracies about Western biological weapons labs in Ukraine on their own blog, Substack, and through the Central Intelligence Directorate-controlled Telegram channel." But it is clear that tactical coordination with conventional kinetic military operations may be either beyond Sandworm's purview or beyond its capabilities. "It is not yet clear whether Sandworm hackers coordinate their cyberattacks with Russian military operations."

On March 15, Wired published a portrait of the new Sandworm leader, Evgeny Serebryakov.

## RUSSIA REMAINS A "VERY POWERFUL CYBER ADVERSARY", SAYS NAKASONE

During a Senate Armed Services Committee hearing on March 7, both General Nakasone, who leads U.S. Cyber Command (CYBERCOM), and the National Security Agency stated that their teams are closely monitoring the situation in Ukraine, highlighting that Russia remains a "very powerful adversary." Nakasone warned that Russia may launch a wave of cyberattacks against Ukraine and the West in retaliation for a Ukrainian counteroffensive or as part of a military advance deeper into Ukraine during the spring offensive. He underscored that the war in Ukraine is far from over.

## RUSSIA-LINKED TA499 STAGES ATTACKS VIA VIDEO CALLS

On March 7, Proofpoint published a report outlining the activities of the Russian pranksters Vovan and Lexus. The report highlighted that the TA499 threat group uses a tactic of sending emails to Western politicians who support Ukraine, inviting them to join a video call on behalf of Ukrainian embassies. During these calls, the victim is made to say something that could potentially embarrass them, and deepfakes of a trusted caller are used to establish trust. These conversations are then recorded and potentially used for Russian propaganda. "TA499 is a serious threat that should not be underestimated due to the potential harm to the reputation and public perception of those targeted," warned the company.

## FALSE AIR RAID ALARM CAUSES PANIC IN MOSCOW AND OTHER REGIONS OF RUSSIA ONCE AGAIN

On March 9, false information about an air raid was broadcast on radio stations and TV channels in Moscow after hackers gained access to their servers, as reported by the Moscow office of the Ministry of Emergency Situations. Similar incidents were also reported in Tula and Sverdlovsk oblasts by their respective departments of the Ministry of Emergency Situations. Such occurrences have previously been observed in Russia, particularly at the end of February this year.

## RUSSIA PREPARES FOR NEW PHASE OF CYBERWARFARE, MICROSOFT WARNS

On March 15, Microsoft published a report analyzing the first year of the cyber war between Russia and Ukraine, providing a detailed analysis of the actions of both parties as well as the methods and means Russian attackers used to target Ukraine. According to the report, the current phase of the confrontation is the third one, which began in September 2022.

The predictive assessment of the actions of Russian malicious actors indicates that they are constantly adjusting their targets and attack methods. Furthermore, Russia seeks to expand its access to intelligence about Ukraine and the support provided to both its civilian and military components.

Another tactic being pursued is creating conditions for destructive attacks against Ukraine and potentially other targets outside Ukraine, including developing new types of ransomware and using social media to promote pirated software with backdoors to Ukrainian users.

## PRO-RUSSIAN HACKERS STEP UP ATTACKS ON HOSPITALS, RESEARCHERS WARN

On March 19, cybersecurity researchers reported that a pro-Russian hacker group known as Killnet has significantly stepped up its Distributed Denial-of-Service (DDoS) attacks on healthcare organizations since November.

In recent months, the group has directed its attention towards the websites of healthcare organizations and launched a campaign in February that targeted hospitals in more than 25 U.S. states. Although the group has not caused significant damage to the targeted organizations, most of the attacks have successfully disconnected hospital websites from the network for a temporary period.

## KASPERSKY LAB DETECTS NEW VIRUS USED IN CYBERATTACKS IN DONBAS AND CRIMEA

On March 21, Kaspersky Lab announced the discovery of a large-scale cyber espionage campaign that has been targeting the occupied parts of Donbas and Crimea since 2021. The campaign has focused on occupation administrations, transportation, logistics, and agricultural organizations. The company highlighted that a new malware called Common Magic is being used to carry out these cyberattacks.

## CYBERSECURITY ASSISTANCE TO UKRAINE PROVIDES CRUCIAL EXPERIENCE FOR CYBERSECURITY COMPANIES, SAYS CISCO TALOS

On March 23, cybersecurity company Cisco Talos released a short documentary highlighting its role in providing cyber assistance to Ukraine during the ongoing cyber war. One of the key takeaways from the documentary is that rapidly mobilizing a large number of cybersecurity experts into special Threats Hunting teams and establishing strong working relationships with government agencies can serve as a blueprint for creating similar groups in the event of future conflicts or large-scale cyber incidents.

## NEW U.S. CYBER SECURITY STRATEGY DRAWS ON EXPERIENCE OF RUSSIAN-UKRAINIAN WAR

An article by Colin Demarest, published on March 2 in Defense One, outlines the main components and approaches of the new U.S. Cyber Security Strategy, with comments from key U.S. officials responsible for cybersecurity. The officials argue that the document is heavily influenced by the experience of countering Russian aggression against Ukraine.

## WHAT CAN INTELLIGENCE SERVICES LEARN FROM A YEAR OF CYBER WARFARE?

The article in Computer Weekly summarized the year-long cyber war between Russia and Ukraine and quoted experts who drew the following conclusions:

- Russia's failures in the cyberwar against Ukraine were not due to the absence or weakness of attacks, but rather the fact that Ukraine and its allies, who came to its rescue, had learned to repel them over the course of more than a decade of Russian attacks.
- Clients who initiated a large-scale digital transformation project 2-5 years ago are now realizing the need to pause and reevaluate the risks posed by the ongoing conflict in Ukraine.
- To mitigate the risk of being targeted by Russian intrusion, chief information security officers and security teams of organizations with higher vulnerability should prioritize monitoring and analyzing new threat intelligence as it becomes available. The conflict led to a significant shift in the nature of the financially motivated Russian cybercrime ecosystem.

## RUSSIA EASES EMPLOYMENT AND RESIDENCE PERMIT PROCESS FOR FOREIGN IT SPECIALISTS

On March 15, the official representative of the Russian Ministry of Internal Affairs, Irina Volk, announced that foreign IT specialists are now able to enter into employment contracts or independent contractor agreements with organizations operating in the IT sector without obtaining a work permit or patent. Accredited IT companies may also hire foreign workers without obtaining a work permit.

## RUSSIAN "WINTER VIVERN" HACKERS FOUND COMPLICIT IN ATTACKS AGAINST UKRAINE, EUROPE, AND INDIA

On March 16, researchers reported a new espionage campaign that targeted government agencies and telecom operators in Ukraine, India, and Europe. The hacker group responsible for the attacks is suspected to have ties to Moscow.

SentinelOne's analysis suggests that the group, Winter Vivern, is "highly creative" and operates with limited resources, carefully choosing targets for its attacks. The group's activities appear to align with the interests of the Russian and Belarusian governments, particularly with regard to the ongoing conflict in Ukraine. The tactics used by the group include:

- Attempts to infect Ukrainian state computer systems by imitating legitimate government services on fake websites hosting malware;
- Creating a phishing web page in an attempt to steal login credentials from users of an email service that the Indian government uses;
- Downloading malicious payloads onto victims' devices by disguising Windows batch files, which are commonly used to automate routine tasks or execute a series of commands, as anti-virus scanners.

## LINUX REJECTS PATCHES FOR ITS DRIVER FROM RUSSIAN BAIKAL ELECTRONICS COMPANY

According to the Russian cybersecurity website Securitylab, Jakub Kicinski, a Linux kernel network subsystem maintainer, rejected patches for the STMMAC network driver from Sergey Semin, an employee of the Russian company Baikal Electronics. Kicinski stated the reason for his refusal as, "We are uncomfortable accepting patches from your organization or related to the equipment it manufactures." Moreover, Kicinski advised Semin to abstain from contributing to the development of the Linux kernel network subsystem until further notice.

## KREMLIN-BACKED HACKERS ACCUSED OF RECENT PHISHING ATTEMPTS AGAINST EU AGENCY

On March 15, cybersecurity researchers from BlackBerry reported that recent attempts to cyberattack diplomatic and governmental institutions in the EU were attributed to Nobelium, a Russian state-owned hacking group. The researchers highlighted that the group specifically targeted organizations that "provided aid to Ukrainian citizens who fled the country and assisted the Ukrainian government."

Nobelium, also known as APT29 or Cozy Bear, sent phishing emails containing EnvyScout malware, which enables attackers to drop malicious files on a computer, to several diplomatic and governmental institutions in the EU, BlackBerry reports.

According to the researchers, "Threat actors closely monitor geopolitical events and leverage them to increase the likelihood of successful infection."

## RUSSIAN ROSTEC CAN ALLEGEDLY DE-ANONYMIZE TELEGRAM USERS

Bleeping Computer reported on March 25, citing Russian media outlets The Bell and Medusa, that Russian Rostec has acquired a platform capable of revealing the identities of anonymous users on Telegram. The corporation, which is actively involved in monitoring the circulation of information within the country, is particularly interested in identifying the administrators of Telegram channels. This capability is expected to be used to suppress any unfavorable news from the country.

## EXPERTS ANALYZE MEDIA COVERAGE OF THE WAR IN UKRAINE

The Atlantic Council convened a panel of experts to shed light on the ongoing war for control of Ukraine's information environment, which is largely comprised of private companies. The panel's objective was to draw lessons for the future, both for the United States and its allies. On March 22, the Atlantic Council published a report containing the experts' analysis.

# 2. CYBERSECURITY SITUATION IN UKRAINE

## UKRAINIAN TEAMS WON PRIZES IN NATO TIDE HACKATHON 2023

More than 100 cyber professionals from 26 teams representing 13 NATO member and partner states participated in TIDE Hackathon 2023. Ukraine was represented by the winners of the National Defense Hackathon 2022, two teams each from the Cyber Police Department of the National Police of Ukraine (First-C.O.P and NEXT-C.O.P) and from the SoftServe company (Valkyria-1 and Valkyria-2). Two teams of the State Service of Special Communications and Information Protection of Ukraine (KRAB and SSSCIP LAB) and a team of the Military Institute of Telecommunications and Informatization named after Kruty Heroes also took part in the competition.

The Valkyrie-1 team won first place in creating a dashboard to analyze the performance indicators of Coalition Warrior Interoperability eXploration, eXperimentation, eXamination eXercise (CWIX) training participants regarding their progress in achieving interoperability. The SSSCIP team KRAB won second place in this discipline, and the team from the Military Institute of Telecommunications won the prize for the most innovative solution for building a visual navigation concept for small unmanned aerial vehicles (UAVs).

## NCCC SECRETARY NATALIYA TKACHUK AT THE PHOENIX CHALLENGE FORUM CALLED ON WESTERN PARTNERS TO JOIN FORCES TO COUNTER DISINFORMATION

Natalia Tkachuk, Head of the Information Security and Cyber Security Service of the National Security and Defense Council of Ukraine and National Coordination Cybersecurity Center (NCCC) Secretary, took part in the Phoenix Challenge 2023 forum in London on February 27-March 3. The event was organized by the U.S. Office of the Under Secretary of Defense for Policy and the United Kingdom (UK) Ministry of Defense, and was titled "Orientation for the Future of Competition in the Information Environment."

In her speech, Natalia Tkachuk shared Ukraine's experience in building information resilience in wartime conditions. "It is important for us to ensure the realization of citizens' rights to have access to true and objective information, in particular, in the occupied territories. The state takes systematic steps not only to counter disinformation and Russian propaganda fakes, but also ensures the stability of the technological component of information security, the functioning of communications, telecommunications facilities, and broadcasting, in particular, during blackouts and in conditions of hostilities," she said.

Tkachuk emphasized that Ukrainians differ from Russians in an extremely high level of critical thinking, and have already developed a certain immunity to Russian propaganda. "The Western world must finally realize that for the terrorist country, human rights, universal and democratic values have no meaning, so we must be ready to counter the information war in these conditions."

## IN THE FIRST MONTH OF THE PROTECTIVE DNS SYSTEM OPERATION, UKRAINIANS' LOSSES FROM FINANCIAL PHISHING DECREASED BY MORE THAN 30%

On March 14, a working meeting was held at the NCCC on the functioning of the Protective DNS system, designed to combat financial phishing. Participants discussed issues related to intermediate results and possibly improving the system. Representatives of the legislative and executive branches, the banking sector, telecom businesses, and professional associations took part in the discussion.

In February, the Protective DNS system was implemented in Ukraine. It filters phishing sites, thus hindering cybercriminals' activities so Ukrainians have received additional protection from fraudsters on the Internet. More than 320 Ukrainian providers who are responsible for their customers' security have already joined the system, including the largest market players: Kyivstar, lifecell, Vodafone, Ukrtelecom, Datagrup, and Volya.

"In the first month of the system's operation, we already have significant results - the volume of phishing fraud in monetary terms has dropped by approximately 40-50%, and the number of complaints from defrauded citizens by 30-40%. In general, these are tens or even hundreds of millions of hryvnias every month, which Ukrainians will not lose thanks to the operation of the system," said Serhiy Prokopenko, Head of the Department for Ensuring the Functioning of the NCCC of the Specialized Service of the NSDC.

## NCCC STARTED COOPERATION WITH THE INTERNATIONAL COMPANY "INTERNET 2.0"

The NCCC signed a memorandum of cooperation with Internet 2.0, a leading U.S. and Australian cyber security organization. The parties agreed on cooperation in the field of cyber security and joint educational training.

With the assistance of the Ministry of Digital Transformation (MDT), Ukraine became the world's first Internet 2.0 partner outside of the Five Eyes intelligence alliance (FVEY), which includes Australia, Canada, New Zealand, the UK, and the U.S. The company will provide its technologies and share advanced experience for Ukraine's cyber defense needs. Internet 2.0 also opened an office in Ukraine.

## SBU EXPOSED ATTEMPTS BY RUSSIAN SPECIAL SERVICES TO COLLECT INTELLIGENCE IN UKRAINE "ON BEHALF" OF FOREIGN MEDIA

Cyber specialists from the Security Service of Ukraine (SBU) record numerous attempts by Russian special services to obtain intelligence information in Ukraine under the guise of foreign media representatives. To collect classified information, the enemy uses specialized Internet platforms and Ukrainian journalists' professional online forums. The occupiers post information requests on these resources allegedly from employees of well-known foreign media.

In their messages, they ask the media and other members of professional groups to obtain materials, supposedly for the preparation of "stories" or "documentaries" about the war in Ukraine. First of all, the enemy is interested in information about the results of Russian missile attacks on Ukrainian cities, including the locations of hits and their consequences. The authors of the "ads" promise a "fee" for providing relevant media files or text messages. The aggressor needs the information obtained in this way to adjust repeated air attacks on Ukrainian objects.

## THE SBU EXPOSED FRAUDSTERS WHO “COLLECTED” MONEY FOR THE ARMED FORCES “ON BEHALF” OF LOCAL AUTHORITIES

SBU cyber specialists exposed a criminal organization that was extorting money from Ukrainian businessmen. The fraudsters presented themselves as local government officials and asked entrepreneurs to “help the Armed Forces.” According to available information, they managed to appropriate more than 3 million UAH.

As the investigation established, a citizen of a Central Asian country who is currently in the temporarily occupied part of Luhansk Oblast organized the criminal scheme. He drew nine more accomplices from Kyiv Oblast and the south of Ukraine into the illegal activities.

Through their own contacts they sought out representatives of companies operating under martial law and found the contact details of their managers. After that, fake letters were sent to them on behalf of the heads of regional, city, and rayon military administrations. They were asked to transfer between 20,000 and 100,000 UAH to the Armed Forces. The amount depended on the company’s turnover.

## THE SSSCIP HELD A WORKSHOP ON CYBER SECURITY CULTURE FOR HUMAN RESOURCES SPECIALISTS IN THE PUBLIC SECTOR

With the support of the National Agency for Civil Service, the Higher School of Public Administration, and the Support to Comprehensive Reform of Public Administration in Ukraine (EU4PAR) project, the SSSCIP held a workshop on cyber security culture for HR specialists in the public service to help Ukraine’s public sector strengthen cyber resilience and promote the development of civil servants’ awareness of cyber protection issues. About 50 specialists took part.

“Human resources professionals play one of the key roles in establishing a cyber security culture in the institution, along with information security and communications professionals. These people have the right skills to spread the culture in the institution, and have the authority and tools to help them do it. That’s why I call on all institutions, both the public sector, critical infrastructure, and all other companies, to attract relevant specialists in order to strengthen their own cyber protection,” said Oleksandr Potiy, SSSCIP Deputy Head.

## RUSSIA’S CYBER TACTICS: LESSONS LEARNED 2022 – ANALYTICAL REPORT OF THE STATE SPECIAL COMMUNICATIONS SERVICE ON THE YEAR OF RUSSIA’S FULL-SCALE CYBER WAR AGAINST UKRAINE

The SSSCIP prepared an analytical report on Russia’s cyber aggression against Ukraine in 2022, Russia’s Cyber Tactics: Lessons Learned 2022. The report examines the main groups and their motivation, methods, and tools of attacks. This knowledge will help in building effective protection systems both in Ukrainian institutions and in organizations around the world.

This report’s target audience is everyone whose activities are related to cyber security in one way or another:

- Top Ukrainian government officials;
- Information security specialists of critical and critical information infrastructure operators and companies that provide services to them;
- Vendors that create cybersecurity products;
- Ukraine’s partners around the world.

On the basis of the research, it is possible to talk about the main trends of the Russian cyber threat.

## SSSCIP INTENSIFIES COOPERATION WITH HIGHER EDUCATIONAL INSTITUTIONS OF UKRAINE

The SSSCIP signed memorandums of cooperation with the Western Ukrainian National University and the Ivan Puliuy Ternopil National Technical University. The memoranda provide for involving SSSCIP specialists in conducting lectures, cyber studies, training sessions, and other events for university students and professors and interaction in the field of information protection and cyber defense.

"Ukraine will increasingly need highly qualified specialists in the fields of information and cyber security, able to effectively and quickly respond to cyber threats and counter them, and strengthen the cyber resilience of government agencies, critical infrastructure facilities, and other institutions. Therefore, strengthening the personnel potential in the field of cyber security is one of the priorities of the SSSCIP. It is extremely important that students acquire the necessary and relevant knowledge for their future work and acquire relevant skills already during their studies," says Oleksandr Potii, SSSCIP Deputy Head.

## PROTECTING PERSONAL DATA OF UKRAINIAN CITIZENS REMAINS ONE OF THE BIGGEST CHALLENGES IN RUSSIA'S CYBER WAR AGAINST UKRAINE

During the war, Russian hackers tried to steal any information about persons who served or are serving in Ukraine's security and defense sector, the SSSCIP states in its report Russia's Cyber Tactics: Lessons Learned 2022. Intruders hunted for information about mobilization plans, rotations, promotions, etc. The data could be used by the Russian special services in the temporarily occupied territories to repress the Ukrainians remaining there.

An example of this is the Armageddon/Gamaredon group (tracked by CERT-UA under the UAC-0010 identifier), whose hackers hunt for privileged/unlimited access to the databases, directories, and social registers of the National Police, since the police store and process information about cars, traffic, cameras, traffic situations, arrests, etc. The data can also be used by the Russian Federation special services for hunting specific individuals, provocations, and sabotage.

## IN 2022, GAMAREDON CARRIED OUT 74 CYBER ATTACKS AGAINST UKRAINE

Gamaredon includes hackers from the Yalta (occupied Crimea) branch of the Russian Federal Security Service (FSB), former employees of the Ukrainian SBU who betrayed their Motherland and went over to the enemy side. Last year, there was not a single week when CERT-UA did not register this group's activities. Gamaredon's main purpose is espionage. A distinctive feature of the group's phishing mails is their high level of preparation: knowledge of the Ukrainian context and understanding of the details of how certain organizations work.

The group attacks the public sector, state-owned enterprises, and the security and defense sector. One of the main targets in the security and defense sector is the National Police. Gamaredon hackers try to gain access to all possible databases and extract maximum information about cars, their movement, surveillance cameras, traffic, arrests, etc.

In addition, Gamaredon's main targets in the second half of 2022 included:

- Credentials of SBU employees in the messenger app Signal in order to gain access to accounts for data theft and user deanonymization;
- Attacks on the communication system of Ukraine's State Border Guard Service and the Shlyakh system used by border guards to check persons crossing the state border of Ukraine;
- Phishing of the Ministry of Defense of Ukraine;
- Defense contractors and manufacturers.

Gamaredon actively uses the infrastructure of the Crimean telecom hosting provider CrymCom for attacks.

## RUSSIAN HACKERS DISTRIBUTE INFECTED SOFTWARE VIA TORRENTS

The SSSCIP warns that downloading hacked software is dangerous. Usually, this kind of software is distributed via torrent trackers actively used by criminals, including Russian special services, which add malicious code to the hacked software.

Hackers trojanize ISOs and installation files and make them available for free on torrent trackers. If a victim downloads and installs the files on their computer, hackers gain access to the contents and can remain undetected for a long time.

In many post-Soviet countries, system administrators still use unlicensed software  distributed via torrent trackers (including operating systems) in institutions and companies with various forms of ownership. By installing hacked software from torrents, they actually give Russian intelligence services access to the contents of working machines. Using hacked operating system is especially dangerous, because attackers have full administrative access to the computer on which it is installed.

Average Ukrainian users are also at risk by installing unlicensed software from unofficial sources, from torrents in particular.

## DIGITAL TRANSFORMATION AND CYBER SECURITY: EUROPEAN PARTNERS SUPPORT UKRAINE

The team of the Estonian Academy of e-Government, the EU Delegation to Ukraine, the MDT, and the SSSCIP took part in the "Let's save digital Ukraine" event on March 16 in Kyiv.

The large-scale European program Digital Transformation for Ukraine (DT4UA) was presented in the meeting. Its tasks include developing electronic public services in Ukraine, improving data exchange between registers and state institutions, etc. The issues of the EU's support in strengthening cyber security in Ukraine were also a focus of the meeting.

During the event, SSSCIP Deputy Head Oleksandr Potii emphasized the importance of the international community's cooperation, in particular to strengthen protection against cyber threats, and thanked the European partners for their help.

## CYBERSECURITY AND DIGITAL CURRENCIES ARE NEW TRENDS IN GOVTECH

With the support of the MDT, the Ministry of Economy of Ukraine, the Office of Reforms of the Cabinet of Ministers of Ukraine, and ISE Corporate Accelerator, Kreston Ukraine presented the results of the study "The global market of Govtech solutions as of February 2023."

The study contains general information about the Govtech industry, key companies, investors, regional features of the industry, and Ukraine's achievements. According to the study, the main trends in Govtech for 2023 are:

- Hyperautomation. According to Gartner, 75% of governments will have at least three hyperautomation initiatives in the next three years;
- Modernization of the state IT infrastructure to improve work efficiency;
- Cyber security. Government institutions must maintain the security and trust of citizens in the digital space;
- Digital currencies. The use of cryptocurrencies will increase operational efficiency and help fight corruption;
- Digital identification. Some countries already have a simple identification process and have implemented digital ID cards that sometimes include biometric verification;
- Artificial intelligence (AI) technologies for interacting with citizens. Governments will increasingly use AI-based applications to automate public services.

## THE CYBER POLICE BECAME A PARTNER IN THE PROJECT TO IDENTIFY CRYPTO WALLETS ASSOCIATED WITH TERRORIST AND SANCTIONED ACTIVITIES

As part of the Scamfari initiative, the cyber police will identify and block criminal virtual assets. Cooperation will be within the framework of the signed memorandum.

The project stipulates joint efforts to establish the addresses of crypto-wallets to which "donations" are collected to support the Russian Federation's military aggression against Ukraine and subsequently blocking the assets. In addition, Scamfari offers a financial reward to users who provide a crypto wallet address and evidence that its owners are involved in illegal activities.

## CYBER POLICE EXPOSED A KHMELNYTSKYI OBLAST RESIDENT FOR CREATING A "VIRUS" TO STEAL USER DATA

The department for countering cybercrimes, the investigative department of the Khmelnytskyi Oblast police, and the regional SBU department exposed a 25-year-old offender. The man developed malware that he positioned as applications for computer games. Once on users' devices, the program could download and upload files, install and uninstall programs, take screenshots from a remote screen, capture sound from a microphone and video from built-in or external cameras. Having collected certain data, the attacker processed it to further steal credentials or withdraw electronic funds in accounts.

It was established that the attacker gained access to more than 10,000 computers. At the time of the search, almost 600 infected computers he could connect to in real-time were "under control" of the suspect.

A criminal investigation was opened under Criminal Code of Ukraine Part 5 of Art. 361 (Unauthorized interference in the work of information (automated), electronic communication, information and communication systems, electronic communication networks). The sanction provides for 10-15 years of imprisonment. The. investigation is ongoing.

## CYBER POLICE OFFICERS IMPROVE THEIR SKILLS IN DETECTING CRIMES COMMITTED USING VIRTUAL ASSETS

The global blockchain ecosystem and cryptocurrency infrastructure provider Binance organized an online training seminar for Ukrainian law enforcement officers. The initiative is aimed at combating the laundering of criminal proceeds and the financing of terrorism.

The training program included material on the legal and regulatory environment and detailed information on Binance's anti-money laundering policies and investigative techniques developed by the company to detect and prevent potential fraud. Cyber police officers deepened their knowledge of blockchain technologies, cryptocurrencies, and methods for combating financial and cybercrimes.

## CYBER POLICE EXPOSED A HACKER GROUP MEMBER INVOLVED IN RANSOMWARE ATTACKS THAT CAUSED €40 MILLION IN DAMAGES TO EUROPEAN COMPANIES

The group member was identified by the Kyiv Department of Countering Cybercrimes, the Main Investigative Department of the National Police, and the Prosecutor General Office in cooperation with law enforcement officers from Germany, the Netherlands, and the Federal Bureau of Investigation and with the support of Europol.

The 39-year-old citizen of Ukraine, who currently lives in Germany, was involved in large-scale cyber attacks using the DoppelPaymer ransomware. Attacks by this virus became possible thanks to the widespread EMOTET malware.

The ransomware was distributed through various channels, in particular through phishing and spam emails with attached documents containing malicious JavaScript or VBScript code. Once on the equipment, the malicious program encrypted the data and the attackers demanded a ransom to restore access.

Among the victims are almost four dozen European companies, critical infrastructure, and industry facilities. The total amount of damages reached €40 million.

## THE CYBER POLICE TEAM GOT TO THE TOP FIVE AT THE NATO TIDE HACKATHON 2023

The jury noted the decision of the Ukrainian police to develop the concept of visual navigation of a small UAV as one of the best. Among the proposed solutions, the cyber police officers chose “Creating a concept and tool for studying disinformation” and “Development of a visual navigation concept for a small unmanned aerial vehicle.”

Based on their solution, the law enforcement officers developed two conceptual solution descriptions and one working software prototype. The cyber police team’s achievements were presented to the jury and were included in the top five solutions for developing a visual navigation concept for a small UAV.

While participating in the event, the cyber police officers improved their knowledge and skills, and the experience gained will be useful for building new software solutions, in particular for countering disinformation and investigating cybercrimes.

## CYBER POLICE EXPOSED A CRIMINAL GROUP THAT TOOK OUT LOANS ON BEHALF OF MISSING AND CAPTURED SERVICEMEN

To implement the criminal scheme, the perpetrators reissued SIM cards and gained access to online banking; then, credit cards were issued and loans were appropriated. The total amount of damages is more than 2 million UAH.

The organized criminal group was exposed by the Cyber Police Department, the investigative department of the Kyiv Oblast Police, the SBU, and the security services of PrivatBank, Monobank, and Sensbank and under the procedural guidance of the regional prosecutor’s office.

It was established that three persons received data on the mobile phone numbers of servicemen whose relatives had lost contact with them or who are currently in captivity. The criminals reissued SIM cards and checked whether the reissued numbers were financial. Then they got access to online banking. The money remaining in the account was transferred to other accounts and credit cards were issued and loans were appropriated.

According to preliminary data, the group managed to gain access to the mobile phone numbers of more than 20 servicemen who are in captivity or missing. The total amount of damages is more than 2 million UAH.

## CYBER SECURITY AND CYBER INTELLIGENCE TRAINING FOR SECURITY AND DEFENSE SECTOR SPECIALISTS AT THE NCCC

The NSDC NCCC and the MDT, with support from the U.S. Civil Research and Development Fund (CRDF Global) and the U.S. Department of State, organized a 2-day training on cyber security and cyber intelligence for security and defense sector specialists, "Cyber security, cyber incident/ cyber threat management and cyber intelligence."

Representatives of this leading organization in the field of cyber security conducted the training as part of the signed memorandum of cooperation between the NCCC and the U.S.-Australian cyber security company Internet 2.0. More than 40 representatives of the security and defense sector took part in the training.

The main topics mastered by the training participants included the latest methods and technologies in the field of cyber security such as threat detection and response, data protection and incident management, intelligence gathering, and document analysis. The participants also had the opportunity to practice the acquired skills.

## THE NCCC IS WORKING ON IMPROVING THE REGULATORY AND LEGAL FRAMEWORK IN THE FIELD OF CYBER SECURITY

The NSDC NCCC, the National Academy of the Security Service of Ukraine, and the Institute of Information, Security and Law of the National Academy of Legal Sciences of Ukraine, with the assistance of the Verkhovna Rada of Ukraine and the Institute of Cyber War Research, held the scientific and practical seminar "Organizational legal principles of developing Ukraine's cyber security system."

Representatives of the SBU, the SSSCIP, the National Police, and the National Technical University Ihor Sikorskyi Kyiv Polytechnic Institute also took part in the event.

"In recent years, for the first time in Ukraine, the minimally necessary regulatory and legal framework for cyber security was formed. The second edition of the Cybersecurity Strategy of Ukraine and the relevant provisions, which are enshrined in presidential decrees, government resolutions, and laws, have been adopted. The first steps have been taken, and we must continue to systematically approach the issue of improving the regulatory framework, taking into account the experience gained in the world's first cyber war," said Serhiy Demedyuk, Deputy Secretary of the NSDC.

Head of the Information Security and Cyber Security Service of NSDC and NCCC Secretary Nataliya Tkachuk noted that, for the first time, the NCCC, key agencies in the national cyber security system, the Verkhovna Rada, scientific institutions, and the private sector work as a united front. "Today, not only do we study the international experience of rulemaking, but our international partners also seek to study Ukraine's experience. And the main topic on which attention is now focused is the legislative regulation of the creation of cyber troops in Ukraine, which is a top-priority task for us," said the head of the Service.

The event participants discussed problematic issues of cyber security legal regulation in Ukraine. The developed proposals will be used in the rule-making work of the Committee of the Verkhovna Rada on National Security, Defense and Intelligence, whose responsibilities includes cyber security issues.

## UKRAINE IS WORKING ON TECHNOLOGICAL SOLUTIONS TOGETHER WITH EUROPEAN PARTNERS

SSSCIP Deputy Head Viktor Zhora and MDT Deputy Minister for European Integration Valeriya Ionan met with Paul Hofheinz, the president and co-founder of the Lisbon Council, a well-known analytical center and political network that brings together experts and public figures from all of Europe.

The meeting participants discussed prospective areas of further cooperation. In addition, Viktor Zhora spoke about the course of the world's first cyber war waged by Russia. The SSSCIP deputy head drew special attention to the service's achievements in countering threats from Russian hackers and the exchange of information between Ukraine and other states on countering cyberattacks. He emphasized that the Ukrainian experience of resisting Russian cyber aggression is important for partner countries.

Zhora also emphasized the need to strengthen joint international work to form new, more effective approaches to countering cybercrime and protecting information systems.

## THE CABINET OF MINISTERS ADOPTED A RESOLUTION STANDARDIZING THE IMPLEMENTATION OF AN INDEPENDENT AUDIT OF INFORMATION SECURITY SYSTEMS AT CRITICAL INFRASTRUCTURE FACILITIES

The government adopted the resolution "Some issues of conducting an independent information security audit at critical infrastructure facilities" and approved the audit procedure, which provides for the mandatory audit of information security once every two years for critical infrastructure facilities belonging to critical categories I and II and once every three years for facilities belonging to critical category III. At the same time, in case of a crisis at a critical infrastructure facility, an audit is carried out immediately.

The audit is provided by critical infrastructure operators. At the same time, they will be able to independently choose auditors who will coordinate the criteria for evaluating information security, the program, procedures, and methods for conducting an independent audit with the operators.

Based on the results of the information security audit, the auditors will provide recommendations to eliminate identified deficiencies in the information security systems.

The SSSCIP will ensure the reports are analyzed based on the results of an independent information security audit and generalized information is provided to the NSDC and the Cabinet of Ministers of Ukraine.

## CYBER ATTACKS ON UKRAINE: WITH THE HELP OF HACKERS, RUSSIA TRIES TO GET ANY INFORMATION THAT CAN GIVE IT AN ADVANTAGE IN ITS CONVENTIONAL WAR

In January–February 2023, the CERT-UA, which operates under the SSSCIP, processed more than 300 cyber incidents and cyber attacks. This is almost twice as many as in the corresponding period last year, when Russia was preparing for a full-scale invasion and hacker activity was abnormally high.

As experts note, in January 2023, cybercriminal activity was somewhat reduced. This is probably related to the New Year holidays in the enemy country. However, in February, hackers returned to their usual activity level.

Since the beginning of this year, CERT-UA has recorded an increase in the number of espionage attacks with an emphasis on maintaining constant access to the organization. And even among the malware distributed by Russian hackers, programs for data collection and remote access to users' devices predominate. This may be one of the signs that Russia is preparing for a long war. With the help of hackers, it tries to obtain any information that can give it an advantage in the conventional war against Ukraine: from data on mobilization to revealing the logistics secrets of Western weapons.

## SBU EXPOSED AN ENEMY BOTNET IN KHMELNYTSKYI OBLAST THAT AMPLIFIED FAKES ABOUT THE WAR IN UKRAINE

SBU cyber specialists eliminated a pro-Kremlin botnet in Khmelnytskyi Oblast. More than 2,000 bots amplified disinformation about the situation at the front and urged Ukrainians to avoid mobilization. The pro-Russian cell was also engaged in discrediting the military-political leadership and the Ukrainian Defense Forces.

According to operational information, the main botnet "customers" were representatives of Russia's special services. They bought fake accounts and used them in popular social networks supposedly on behalf of ordinary Ukrainians. The aggressor tried to destabilize the internal political situation in the western regions of Ukraine by carrying out information sabotage.

The perpetrators will be charged under Part 5 of Art. 361 of the Criminal Code of Ukraine (unauthorized interference with the operation of electronic computing machines (computers), automated systems, computer networks or telecommunications networks). The investigation is ongoing to establish all the circumstances of the crime and bring the culprits to justice.

## CYBER POLICE EXPOSED SUSPECTS IN FINANCING THE OCCUPIERS

The suspects made "donations" for the needs of Russia's military and the illegal armed formations of the so-called Luhansk and Donetsk People's Republics (LDNR). Eight residents of different regions of Ukraine transferred money for the needs of the occupying forces and representatives of the pseudo-republics. They obtained information about the fundraising from propaganda Telegram channels. In total, those involved transferred about 200,000 UAH to a crypto wallet created by the Russians.

In the course of operational measures, the cyber police blocked eight cryptocurrency wallets that were used for criminal purposes. The total balance in the accounts is about 2 million UAH.

A criminal investigation was opened under Part 1 of Art. 258-5 (Financing of terrorism) of the Criminal Code of Ukraine. The sanction provides 5-8 years of imprisonment and confiscation of property. Investigations are ongoing

## MEMBERS OF A CRIMINAL ORGANIZATION WILL BE TRIED IN LVIV OBLAST FOR FRAUD UNDER THE GUISE OF GOVERNMENT BENEFITS

The suspects obtained data about citizens' bank cards with the help of phishing sites and later appropriated money from them. Law enforcement officers completed the pre-trial investigation and sent the indictments to court.

The group members were exposed by the Cybercrime Countermeasures Department in Lviv Oblast and the Lviv Oblast Police investigative department in January 2023.

Four of the defendants created phishing sites whose interface was similar to sites for registering social benefits, in particular eSupport, aid from the EU, and various charitable fund programs. The attackers used online bulk SMS services to distribute phishing links to obtain citizen bank card data and appropriate money from the accounts. Cyber police officers blocked the fraudulent websites.

The suspects face up to 15 years in prison.