НКЦК
НАЦІОНАЛЬНИЙ КООРДИНАЦІЙНИЙ
ЦЕНТР КІБЕРБЕЗПЕКИ

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

January 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

KEY TENDENCIES

The general trend with ransomware in the world is improving. Although the number of attackers and business models for this type of virus is increasing, the number of attacks and the number of those who pay the ransom is decreasing. At the same time, the high crime latency level (they are not reported) continues to be relevant for this sphere and attacks become more and more targeted and better prepared. The decrease is due to both better coordination of different countries in countering the threat (including control over cryptocurrencies) and law enforcement agencies' successful operations.

In a long-term special operation, the U.S. Federal Bureau of Investigation (FBI) managed to destroy the powerful Hive ransomware group. Although this is only one group of this kind, its destruction will have more far-reaching consequences than simply preventing the criminals from receiving the $130 million ransom they demanded from their victims. It also gives law enforcement agencies a better understanding of the internal workings of these malicious groups and will help reduce the activity of a number of smaller groups that have used Hive's Ransomware as a service (RaaS) resources. At the same time, experts already expect that the vacant place will become the subject of competition among other hacker groups.

Ransomware attacks on medical institutions cause increasing concern in the world's leading countries (the U.S., UK, France, Australia). While there are currently no accurate statistics on the number of additional deaths caused by the attacks due to the inability to provide services to patients, the trend is increasingly worrisome. In the U.S., the 2023 appropriations bill introduced requirements for the cybersecurity of medical devices. Although experts welcome this initiative, they emphasize the inadequacy of such measures.

Government institutions remain attractive targets for criminals. In the last half of 2022, the number of cyberattacks on governments increased by 95 percent. Attacks against the UK's Royal Mail, Costa Rica's Ministry of Public Works and Transport, Moldova's public institutions, and a campaign against military and government institutions in the Asia region all point to the growing threats to public sector organizations and the need to use proper cybersecurity measures.

Government cybersecurity agencies realizing the growing risks continue to adjust their policies and strengthen the requirements for cybersecurity legislation. The expected strengthening of mandatory cybersecurity requirements in the new U.S. National Cybersecurity Strategy, the second modification of Cyber Essentials by the UK's National Cyber Security Centre (NCSC) in the last six months, testing of contractors for vulnerability and readiness to implement a zero-trust policy (U.S.), and constant training and cooperation development among government agencies all constitute a logical consequence of new threats.

The number of vulnerabilities detected in various Industrial Control System/Operational Technology (ICS/OT) systems is increasing. In January alone, vulnerabilities became known in Siemens, InHand, and GE Proficy Historian products used in many high-risk industries and for the functioning of industrial robots, oil wells, elevators, medical equipment, and electric car charging stations. Some unconfirmed reports indicate successful external cyberattacks on ICS systems. Attackers' long-term interest in industrial systems is growing and they persist in attempting to find vulnerabilities in the systems. Experts note that this can lead to serious consequences and to cases similar to Stuxnet. Even without ICS access, attackers manage to paralyze the work of large shipping companies (Norway) or cause difficulties for energy facilities (Canada).

The debate on global rules of conduct in cyberspace for all countries is back on the agenda. Observers note that the spread of cybercrime is nearing the scale of a cyberpandemic and countries do not have a solution to this problem. While researchers suggest that the largest states (in particular, the U.S.) should take on increased unilateral obligations to promote cybersecurity norms at the global level, other countries (Ukraine, in particular) initiate creating a common space where states can safely exchange information, support each other, and interact.

Russian hackers continue to attack Ukraine's partners. Poland, Germany, the UK, the Baltic countries, and the U.S. receive special attention. Poland was the target of cyberattacks by the Ghostwriter hacker group. Latvia confirms an attempted phishing attack on the Ministry of Defense, linking it to a Russian hacking group. The UK warns its citizens about cyberattacks by Russian groups. Russian hackers conducted a major campaign targeting the U.S. nuclear sector by trying to attack American nuclear scientists. Experts indicate that these trends will continue in 2023, which will require Western countries to increase their preparedness.

The world continues to assess the consequences of the first world cyberwar and the actions that allowed Ukraine to effectively counter the enemy. In addition to the importance of international assistance provided to Ukraine for cybersecurity over the past eight years, experts also say that Ukraine was ready for cyber war not only because of the assistance provided but also because of the focus on ensuring the resilience of the most important functions. Of course, the strengthened public-private partnership became an important factor in countering Russian cyber activity. The fact that even a 20-fold increase in the number of cyberattacks aimed at Ukraine in the fourth quarter of 2022 did not lead to serious consequences speaks to the effectiveness of this cybersecurity policy.

1. FIRST WORLD CYBER WAR

POLAND WARNS OF ATTACKS BY RUSSIA-LINKED GHOSTWRITER HACKER GROUP

In an official announcement on Poland's government website, the country has been the target of cyberattacks since the beginning of Russian aggression against Ukraine. They intensified in late 2022. The Polish government attributes this to its ongoing support for Ukraine and advocacy against Russian aggression in the international arena.

Hacking groups "linked to the Kremlin" use ransomware, Distributed Denial-of-Service (DDoS), and phishing attacks with the goals of "destabilizing, intimidating, and wreaking chaos," a Polish government agency wrote.

CYBERATTACKS TARGETING UKRAINE INCREASE 20-FOLD IN Q4 2022 — TRELLIX

According to a report released by Trellix on January 24, email cyberattacks on Ukraine's public and private sectors saw a 20-fold increase in the last quarter of 2022. The Trellix Advanced Research Center links this activity to the Gamaredon group.

A STRONGER PUBLIC-PRIVATE PARTNERSHIP HAS BECOME AN IMPORTANT FACTOR IN COUNTERING RUSSIAN CYBERACTIVITY — TRELLIX

On January 24, the cybersecurity company Trellix released its analysis of key cybersecurity trends in 2022. According to Trellix, the Russian-Ukrainian cyber warfare has become a key factor in the threat landscape. It also revealed a stronger public-private partnership as an important factor of effective resistance, which has contributed to the active exchange of intelligence about threats, rapid response teams supporting each other and quickly eliminating malware around the globe, disrupting botnets, and warning of dangerous cyberattacks.

RUSSIAN CYBERSECURITY ECOSYSTEM GETTING POLITICIZED BY SANCTIONS AGAINST RUSSIA — BROOKINGS INSTITUTION

On January 12, researcher Justin Sherman of the Brookings Institution offered an overview of trends in the Russian cybersecurity community in the context of ongoing cyber warfare and sanctions newly imposed on the Russian Federation. Using the topics of the Positive Hack Days annual conference as an illustration, he notes a strengthening nationalist rhetoric and a generally more politicized cybersecurity sector in Russia. Sherman points to the more frequent rhetoric of "turning away from foreign products," public support for the Russian government's actions, and an effort to steer the external vectors of development from the Western to Asian market.

RUSSIAN HACKERS TARGETED AMERICAN NUCLEAR SCIENTISTS

Last summer, a Russian hacking group known as Cold River targeted three nuclear research laboratories in the U.S., according to electronic records verified by Reuters and five cybersecurity experts.

In August and September, when Putin said Russia was prepared to use nuclear weapons to defend its territory, Cold River struck Brookhaven, Argonne, and Lawrence Livermore National Laboratories. The study showed that the hackers set up fake login pages for each facility and sent nuclear scientists emails trying to get them to share their passwords.

UKRAINE PROVED READY FOR CYBER WAR NOT ONLY BECAUSE OF THE AID PROVIDED, BUT ALSO BECAUSE OF ITS FOCUS ON THE STABILITY OF CRITICAL FUNCTIONS

Ukraine's allies continue to take stock and learn the lessons of the Russian-Ukrainian cyber war. In their speeches, they note that Western aid to Ukraine has indeed been a vital factor in its readiness for cyberattacks.

However, in addition to this, Ukraine's bet on the stability of critical functions was also a success—that is, awareness that even the most advanced protection tools can fail, so it is necessary to be ready to provide basic services in other ways.

Some researchers even indicate that Ukraine is now more adapted to cyber confrontation and new challenges in cyberspace than the U.S. and its private (especially industrial) sector.

CISA DIRECTOR: THE U.S. NEEDS TO BE VIGILANT, "KEEP OUR SHIELDS UP" AGAINST RUSSIA

On January 5, during a panel discussion at CES2023 (the largest annual consumer electronics show) in Las Vegas, Cybersecurity & Infrastructure Security Agency (CISA) Director Jen Easterly noted that, although Russia had not made a significant cyber strike against the U.S. to date since invading Ukraine, one could not assume that it would not happen going forward. According to Easterly, the war will take quite some time, so it is important to remain vigilant.

TURLA: A GALAXY OF OPPORTUNITY

A report from Mandiant published on January 5 claims that, Russian hackers from the Turla group used viruses distributed by other hackers via USB in Ukraine. The company stresses that this is the first time since the beginning of Russia's full-scale invasion that Turla has targeted Ukrainians. Follow the link for more about the mechanisms in the company's report.

KILLNET TARGETED A NUMBER OF INFORMATION RESOURCES IN GERMANY WITH DDoS ATTACKS

Russian group KillNet claimed responsibility for a series of DDoS attacks against the websites of German airports, government agencies, and financial sector organizations. German competent authorities, including the Federal Office for Information Security (BSI), note that the attacks did not harm service functionality or delivery and, in general, were fought off fairly quickly.

The group called for the attacks in response to Chancellor Olaf Scholz's announcement that Germany would send Leopard 2 tanks to Ukraine to help repel Russia's invasion.

ZELENSKYI'S ADDRESS BROADCAST ON TV IN RUSSIA AND CRIMEA

On January 25, President Zelenskyi's television address was briefly broadcast on television in occupied Crimea and in Belgorod, Russian Federation. The Crimean authorities attributed the incident to a hack, and Belgorod Oblast authorities referred to an "unauthorized replacement of the TV signal."

POLAND PREPARING FOR A SPIKE IN RUSSIAN CYBER ACTIVITY OVER THE RUSSIAN-UKRAINIAN WAR

Andrzej Kozłowski, head of the Science Department at the Casimir Pulaski Foundation, calls on the Polish authorities to prepare more actively for Russian cyberattacks due to Poland's logistics role in the supply of weapons to Ukraine. He points out that the existing experience of cyberattacks shows the need to take additional steps, including by more actively engaging the U.S. Cyber Command in maintaining the security of Polish networks, promoting information exchange with the private sector, and being ready to raise the cybersecurity alert level to the highest DELTA level, which involves stronger physical security measures of individual facilities and additional network checks.

LEGAL STATUS AND FUTURE OF THE IT ARMY TO BE ADDRESSED – WIRED

In a January 23 article, Wired columnist Victoria Baines raises questions about the legal status of members of the volunteer association IT Army of Ukraine. She stresses that, although this will not be raised during the confrontation, the experience of similar traditional conflicts suggests that non-regular forces involved in the conflict face legal status and protection challenges after it ends.

As for the IT Army, there may be doubts about those who have participated in offensive operations (DDoS) or want to use the acquired expertise of hacktivism for criminal purposes.

LATVIA CONFIRMS A PHISHING ATTACK ON ITS MINISTRY OF DEFENSE, LINKING IT TO A RUSSIAN HACKER GROUP

A Russian cyber espionage group known as Gamaredon may have been behind a phishing attack on the Latvian Ministry of Defense last week, the Ministry told The Record on January 27. Posing as Ukrainian government officials, hackers sent malicious emails to several Ministry staff members. The attempted cyberattack was unsuccessful, the agency added.

Researchers link this phishing campaign to Gamaredon because the hackers used the same domain (admou[.]org) as in its previous cyberattacks. Earlier in December, the cybersecurity company Unit 42 also linked this domain to Gamaredon.

RUSSIA RECRUITED UKRAINIAN KIDS THROUGH A MOBILE GAME

On January 8, Ukraine's Minister of Defense Oleksii Reznikov reported on Twitter that Russian intelligence services tried to recruit Ukrainian children to unwittingly share locations of strategically important facilities through a mobile game.

DEEP FAKES AND INTERNATIONAL CONFLICT

The Brookings Institution published research on deep fakes and their potential use in international conflicts. Researchers emphasize that attempts have been made to use the technology in the Russian-Ukrainian war. Although the attackers did not succeed this time, the technology is evolving rapidly and is likely to challenge national security analysts and policymakers given its wide range of potential uses.

Brookings analysts point out that although it is possible today to teach an algorithm to identify deep fakes, this solution will not work in the long run because any technical solutions that help identify deep fakes can now be included in the next algorithm for creating them.

The authors of the report also emphasize that it is time for democratic countries to start discussing the ethical framework of using deep fakes in a conflict and the mechanisms to control their use. The authors of the report refer to a new United Nations (UN) treaty as a possible solution.

2. CYBERSECURITY SITUATION IN UKRAINE

UKRAINE SIGNED AN AGREEMENT ON JOINING NATO'S JOINT ADVANCED TECHNOLOGIES CENTER FOR CYBER DEFENSE

On January 19, Oleksiy Danilov, Secretary of the National Security and Defense Council of Ukraine (NSDC), signed the Technical Agreement on Ukraine's accession to NATO's Joint Center for Advanced Technologies for Cyber Defense (CCDCOE). The Center's Steering Committee unanimously supported the application of the NSDC National Coordination Center for Cyber Security (NCSCC) for Ukraine's membership in the Center on March 4, 2022.

Signed by the NSDC Secretary (head of the NCSCC), the agreement will be handed over to all of the Center's member countries for signature. Ukraine's membership in the Center will bolster the exchange of cyber experience between Ukraine and CCDCOE member countries. In addition, this is an important step towards Ukraine's NATO accession.

Danilov noted that Ukraine, which has been fighting a terrorist country on all fronts for almost nine years, has shown a high level of resilience in cyberspace, as well. "We did not only survive but also became an example for the whole world. This is also confirmed by our NATO partners," he emphasized.

The NSDC Secretary called Russian hackers a threat to the whole world, repeating that during the past year, they constantly attacked Ukraine's partners, the states that provide comprehensive support to Ukraine to win this war. According to Danilov, it is "about the first world cyberwar, and to counter this war we are forming an effective international cyber coalition, we must unite to confront the common enemy."

NATALIYA TKACHUK: EXCHANGE OF EXPERIENCE WITH THE UK IN COUNTERING DISINFORMATION AND CYBERATTACKS IS IMPORTANT AND TIMELY FOR UKRAINE

Exchanging experience with the UK on countering disinformation and cyberattacks is important and timely for Ukraine, the head of the NSDC Information and Cyber Security Service and Secretary of the National Security Committee Natalia Tkachuk emphasized during a January 23 meeting with representatives of the London Chamber of Commerce and Industry and the City of London Municipality, organized by the Chamber of Commerce and Industry of Ukraine.

Tkachuk noted that the UK is one of Ukraine's key and most important partners, in particular in matters of cyber defense and combating disinformation.

"Last year, the UK updated its national security legislation, in particular on countering disinformation and cyberattacks. The country has strengthened cooperation with Internet providers and the companies Meta and Google to identify and eliminate disinformation from social networks, and strengthened government control in this area. This experience is extremely important and relevant for Ukraine, because the war is going on, and we are fighting with the Russian Federation in information and cyberspace," Tkachuk said.

The head of the service also noted that the UK has supported Ukraine from the very beginning of the cyber war, noting that by now the whole world has realized that the Russian Federation is a terrorist country.

The event was also attended by representatives of the Verkhovna Rada of Ukraine, the Cabinet of Ministers of Ukraine, business associations, and the private sector.

THE SBU NEUTRALIZED AN ATTEMPT BY RUSSIAN HACKERS TO BREAK INTO APARTMENT BUILDING COMPUTER NETWORKS

Security Service of Ukraine (SBU) cyber specialists neutralized a Russian hacker attack on the electronic systems installed in residential infrastructure in one of the border regions of Ukraine. The hackers wanted to remotely connect to the video surveillance system covering the territory of residential complexes, nearby roads, etc., through apartment buildings' Wi-Fi network. They planned to have a secret channel to collect information about the situation in the city.

The aggressor was also interested in the residential addresses of Ukrainian law enforcement officers and the possible movement of military equipment. However, the SBU employees were proactive and promptly exposed the occupiers' attempt to carry out reconnaissance and subversive activities in the border region.

According to operational data, a Russian hacker group controlled by the Russian Federation security services that specializes in hacking the electronic systems of infrastructure facilities was involved in the cyberattack.

NATALIYA TKACHUK: A EUROPEAN CYBER COALITION FOR A JOINT RESPONSE IN CASE OF LARGE-SCALE CYBERATTACKS SHOULD BE CONSIDERED

Head of the NSDC Information and Cyber Security Service and Secretary of the National Security Committee Nataliya Tkachuk took part in an online meeting with the Swedish Association of Local Authorities and Regions, the political leadership of 290 municipalities and 21 regions of Sweden. She shared Ukraine's experience in countering the enemy in cyberspace during the ongoing first global cyber war and emphasized the need to create a European cyber coalition.

"Thanks to the joint coordinated efforts of all cybersecurity entities, Ukraine has demonstrated the remarkable resilience of the national cybersecurity system. Now it is necessary to consider the possibility of creating a European cyber coalition, not only to ensure the exchange of information, intelligence data, and uniform cybersecurity standards, but also to provide for creating joint response mechanisms in the event of large-scale cyberattacks and joint action protocols both at the national and international levels. And Ukraine is ready to share its own experience," she said.

Tkachuk also emphasized the need to have a global discussion about norms of international law that would clearly define the essence of cyber war, the rules for conducting it, cyberattacks, and responsibility for these actions: "It is already necessary to form a clear vision of what types of cyberattacks should be considered war crimes and to determine the legal status of cyber combatants and the protection mechanism for our cyber volunteers under international law."

The NCSCC secretary thanked international partners for their help. "In this cyber war, the entire democratic world is on Ukraine's side today, cyber volunteers, government agencies, IT business. We greatly appreciate their support. But to win, we really need weapons, in particular cyber weapons," she said.

A REPRESENTATIVE OF THE UKRAINIAN MINISTRY OF DEFENSE GAINED MEMBERSHIP IN THE BOARD OF DIRECTORS OF THE REGIONAL CYBER DEFENSE CENTER IN KAUNAS

According to the Memorandum of Understanding between the Ministry of Defense of Ukraine and the Ministry of National Defense of the Republic of Lithuania, the Ukrainian military actively participates in the operation of the Regional Cyber Defense Center (RCDC) in Kaunas, Lithuania.

RCDC's tasks include cyber threat analysis, trainings for cyber security specialists, scientific research in cybersecurity, and cooperation with strategic partners.

Joint events involving military cybersecurity specialists are held to deepen mutually beneficial cooperation in intelligence and cyber threat analysis. In addition, they make for an exchange of experience in response, processing, and protection against cyber threats. Ukraine's specialists will study the RCDC's capabilities to provide cyber defense (hardware and software) in the interest of developing the cyber defense systems of the Ministry of Defense of Ukraine and the Armed Forces of Ukraine, as well as expanding the RCDC's technical capabilities. Practical training as part of RCDC cyber units and at the RCDC training center gives Ukrainian specialists practical experience in responding to cyber threats.

SBU PREVENTED ATTEMPTS TO HACK THE GOVERNMENT ELECTRONIC SYSTEM IN THE CONSTRUCTION INDUSTRY

SBU cyber specialists exposed and stopped suspected criminals who tried to legalize illegal constructions by hacking the Joint State Electronic System for construction and also issued fake architect certificates.

“We exposed illegal schemes in time and did not allow criminals to hack the state electronic system. We are not talking about ordinary cyber hacking, but about crimes that could lead to very serious consequences in the future. If it were not for the SBU’s reaction, hundreds of ‘problematic’ buildings that were built in violation of current requirements and standards would have been legalized in Ukraine. This poses the risk of man-made accidents and other emergencies. And that means it is a risk for thousands of Ukrainians,” Ilya Vityuk, head of the SBU Department of Cyber Security, emphasized.

According to Vityuk, the launch of a new large-scale corruption scheme in the construction sector was also prevented.

“The construction sector was the first where the Ministry of Digitalization team successfully implemented real digital transformation. Digitization provides transparent tools to record every action. Thanks to the creation of the Joint State Electronic System for construction, the government saves billions of hryvnias annually. In addition, we can now prevent and detect illegal schemes in the construction sector. After all, the system is designed in such a way that the digital footprint of each user remains for good and is easy to track,” said Mykhailo Fedorov, Deputy Prime Minister and Minister of Digital Transformation.

According to the security service, high-ranking officials at the National Union of Architects of Ukraine, well-known “shadow” intermediaries are involved in the organization of illegal transactions. The involvement of state and local government officials is also being investigated. The perpetrators tried to get money illegally by forging and selling permits to construction business representatives.

Among the fraudulent transactions exposed were illegal registrations of objects that violate construction regulations and a scheme for issuing fake professional architect certificates – anyone could be made an “architect.”

UKRAINIAN EXPERIENCE OF COUNTERING RUSSIAN CYBERATTACKS WAS DISCUSSED IN THE UK

Viktor Zhora, Deputy Head of the State Service of Special Communications and Information Protection (SSSCIP) and a representative of the Government Computer Emergency Response Team (CERT-UA) visited the UK’s NCSC. The key topics of the dialogue with British colleagues was stronger cooperation and joint efforts to counter Russian aggression in cyberspace and the need to intensify the exchange of information on cyber incidents.

Zhora noted that the world is mostly watching the Russian invasion on the ground, while the aggression in cyberspace is less noticeable. However, the number of cyberattacks against Ukraine tripled last year, and a large part of them were coordinated with other areas of military operations, for example, missile strikes.

During the trip, the Ukrainian representatives took part in the CyberThreat 2022 conference in London. Deputy head of CERT-UA Yevhen Bryksin told the participants about the cyber incidents the team addressed. He also presented analytical and technical information on the tactics, techniques, and tools used by hacker groups associated with the Russian Federation government during cyberattacks on Ukrainian organizations and institutions.

NCSCC IS WORKING ON IMPROVING PUBLIC COMMUNICATIONS PROCEDURES IN RESPONSE TO LARGE-SCALE CYBERATTACKS

On January 26, the NCSCC, with the support of the USAID Cybersecurity of Critical Infrastructure in Ukraine Activity, held the roundtable "National response plan to emergency (crisis) situations in cyberspace: practical aspects of effective public communication of cyber incidents."

The meeting was attended by communication managers and cyber security specialists of all key cyber security agencies, the Center for Combating Disinformation, the Ministry of Health, the National Health Service, the Ministry of Culture and Information Policy, the State Service for Emergency Situations, and critical infrastructure enterprises.

The purpose of the event was to form a common understanding among all parties about the importance of coordinating actions and messages to society about detected incidents and crises in cyberspace. The participants discussed the current situation with informing society about crises in cyberspace and about individual cyber incidents. Based on the discussion, recommendations were made to improve the processes of informing society about cyber incidents and the contents of the National Response Plan.

THE WINNING TEAMS OF LAST YEAR'S NATIONAL DEFENSE HACKATHON WILL TAKE PART IN THE NATO HACKATHON IN WARSAW

The C.O.P. cyber police team, which won first place in the technical area at the National Defense Hackathon 2022 among the Ukrainian public sector teams, will represent Ukrainian government agencies at the annual TIDE Hackathon 2023 NATO programming competition. Team C.O.P. received the relevant certificate from NATO partners as part of the NATO Trust Fund knowledge exchange project Ukraine C4 (command, control, communication, computerization).

NATO TIDE Hackathon 2023 will be held in Poland at the end of February. Among the main competition tasks, in particular, is to develop new software and hardware solutions, innovative architectural models, and methods for presenting and understanding information by government officials and to ensure the informational interaction among units through the exchange of knowledge during joint problem-solving.

Other winners of the National Defense Hackathon 2022 will also participate in the NATO TIDE Hackathon 2023, including the Valkyrie team, which won first place in the technical area in the competition among private sector participants, and the SSSCIP's DDK DSSZZI team, which came in second among public sector teams at the 2022 National Defense Hackathon.

RECTOR, TEACHERS, AND CADETS OF THE NATIONAL SECURITY SERVICE ACADEMY AWARDED WITH THE NSDC HONORS

To mark the anniversary of the National Security Service of Ukraine Academy, Deputy NSDC Secretary Serhiy Demedyuk presented awards to its employees and cadets.

“First of all, I want to thank the cadets, boys and girls who currently during the war help the state fight the enemy and punish the guilty in the future. After all, your invaluable experience and ideas will contribute to the development of the national security and defense system. I also want to note the Academy’s volunteer activities and thank its management, every teacher and employee who continues to train future specialists in such a difficult time the country is going through,” Demedyuk said.

The academy’s rector Andriy Chernyak and academy professors were given the NSDC awards effective cooperation with the National Coordination Cybersecurity Center (NCCC) in the interests of Ukraine’s national security and defense, a significant contribution to the training of highly qualified cybersecurity specialists, high professionalism, initiative, and perseverance. On the occasion of the holiday, Demedyuk also thanked the academy’s cadets who were most active in cooperating with the NCCC for their diligence and perseverance in learning, initiative, and support for NCCC activities during martial law.

UKRAINE AND FINLAND WILL COOPERATE ON DIGITIZATION AND DIGITAL SUSTAINABILITY, SIGNED A MEMORANDUM

The Ministry of Digital Transformation of Ukraine and the Ministry of Transport and Communications of Finland signed a memorandum in the sphere of digital transformation. During the meeting, the parties discussed further experience exchange and cooperation between the countries in rebuilding digital infrastructure and strengthening cyber defense.

“We are grateful to Finland for supporting digitalization in Ukraine at such a difficult time. The memorandum will help strengthen the digital transformation and modernization of the telecom infrastructure in Ukraine. We will also adopt the best practices to prevent cyber threats and hybrid threats and develop the state’s digital stability,” said Minister Mykhailo Fedorov.

“I am very impressed with the work that Ukraine has done to promote digitalization. With this agreement, we are already looking into the period of recovery of Ukraine. I believe that we can learn a lot from each other,” added Minister Timo Garakka.

The memorandum will enable the countries to exchange experience in the areas of digitization, information technologies, and cybersecurity. Ukraine and Finland will also cooperate in the fields of digital sustainability, reconstruction, and modernizing digital infrastructure.

THE FOURTH EDUCATIONAL MODULE OF THE SJC-2022 STRATEGIC LEADERSHIP PROGRAM FOR CYBERSECURITY MANAGERS HELD WITH NCSCC SUPPORT

The fourth training module of the SJC-2022 strategic leadership program for managers in the cybersecurity was devoted to "(un)obvious but crucial partnerships 2.0." Two teams took part in the training, Civil Officer Academy and Sophos Joint Cyber. Almost 70 participants – civil servants, military personnel, law enforcement officers, managers, volunteers, entrepreneurs, and international partners – developed strategies for mutual relations and ecosystems of the future in cyberspace.

"The NCSCC's key task is to build an effective national cybersecurity system, and the main component of this system is human resources. Therefore, one of the priorities is to increase the state's high-quality cybersecurity personnel potential, in both the public and private sectors," said Nataliya Tkachuk, head of the NSDC Information and Cyber Security Service and NCSCC Secretary.

A CYBERATTACK FAILED TO STOP THE OPERATION OF UKRINFORM NEWS AGENCY

Thanks to the prompt actions of the CERT-UA, the January 17 attack by Russian hackers on the Ukrinform National Information Agency failed to stop its operation. Ukrainians and the whole world can continue to receive prompt and objective information about the country.

"Since the first days of the full-scale invasion, Russians have been trying to deprive Ukrainians of information about the state of affairs in the country and the progress of the war. They turned off Ukrainian television, the Internet, and mobile communications in the temporarily occupied territories and launched rocket attacks on TV and radio towers in many Ukrainian cities. They carried out cyberattacks on Ukrainian media. The attack on Ukrinform is another attempt to destroy the truth," said Yuriy Shchygol, head of the SSSCIP.

KYIV CYBER POLICE EXPOSED A COUPLE IN A PHISHING FRAUD

Suspected attackers gained access to citizens' bank cards and used victims' money for online store payments. The organizer of the scheme was charged.

The 21-year-old native of Mykolaiv Oblast and his partner used phishing links and Telegram bots to obtain bank data from citizens. Phishing was disguised as providing government social assistance. The offenders also bought citizens' compromised bank card data on the Darknet.

Using this information, they paid in online stores with money from the victims' accounts. Most of the goods were bought for personal use and some of them were resold on classifieds platforms.

Police currently identify their victims. Law enforcement officers searched the suspects' place of residence. Mobile phones, laptops, appliances, merchandise receipts, and bank cards were seized. Employees of the special police regiment were also involved in the investigation.

SINCE FEBRUARY 2022, THE NUMBER OF ATTACKS ON UKRAINE'S ENERGY SECTOR HAS INCREASED BY 20-25%

In an article published by The Record on January 11, representatives of Ukraine's energy sector disclosed the details of Russian cyberattacks against the Ukrainian energy sector. In particular, the article states that since February 2022, the number of attacks on the energy sector has increased by 20-25%. The most common attacks were DDoS, phishing, and malicious code execution attempts. According to Ukrenergo, cyberattacks were most intense in March 2022, when Ukraine was connecting to the EU energy system.

RUSSIAN CYBERATTACKS COULD BE WAR CRIMES

In an interview with Politico, published on January 9, Viktor Zhora, Deputy Head of SSSCIP, said that Ukraine is collecting digital evidence for the court in The Hague so that the perpetrators of cyberattacks on critical infrastructure are prosecuted for war crimes.

According to him, cyberattacks carried out by the Russian Federation were coordinated with kinetic attacks on civilian infrastructure, which is a war crime, and therefore are also war crimes. As an example, Zhora cites the attacks on the company DTEK, when physical objects and the company's electronic network were attacked simultaneously.

If Ukraine successfully achieves such a punishment, it will be the first time in history.

UKRAINE CALLS FOR 'CYBER UNITED NATIONS' AMID RUSSIAN ATTACKS

On January 15, Politico reported that SSSCIP Chair Yuriy Shchygol called for creating a "Cyber United Nations", an organization within which states "can exchange information, support each other, and interact." Shchygol believes that civilized countries should have "one space, one cyberspace."

VADYM LEDNEY: "THE GOAL OF THE CYBER FORCES OF THE UKRAINIAN ARMED FORCES IS TO PROTECT THE SOVEREIGNTY OF THE STATE AND REPEL MILITARY AGGRESSION IN CYBERSPACE"

The Armed Forces of Ukraine have been dealing with activities in cyberspace since 2010, says Vadym Ledney, a cyber warfare specialist of the General Staff of the Armed Forces of Ukraine. In an interview with the Global Center for Interaction in Cyberspace, he talks about Ukrainian cyber forces, their goals, composition, and functions.

ACRONУMS

BSI	Federal Office for Information Security (Germany)
CCDCOE	Joint Center for Advanced Technologies for Cyber Defense (NATO)
CERT-UA	Government Computer Emergency Response Team
CISA	Cybersecurity & Infrastructure Security Agency
DDoS	Distributed Denial-of-Service
FBI	Federal Bureau of Investigation
ICS	Industrial Control System
NATO	North Atlantic Treaty Organization
NCCC	National Coordination Cybersecurity Center
NCSC	National Cyber Security Centre (UK)
NCSCC	National Coordination Center for Cyber Security
NSDC	National Security and Defense Council of Ukraine
OT	Operational Technology
RaaS	Ransomware as a Service
RCDC	Regional Cyber Defense Center
SBU	Security Service of Ukraine
SSSCIP	State Service of Special Communications and Information Protection of Ukraine
U.S.	United States
UK	United Kingdom
UN	United Nations
USAID	United States Agency for International Development