НКЦК

НАЦІОНАЛЬНИЙ КООРДИНАЦІЙНИЙ
ЦЕНТР КІБЕРБЕЗПЕКИ

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

April 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

AI	Artificial Intelligence
APT	Advanced Persistent Threat
CERT-UA	Government Computer Emergency Response Team Ukraine
CERT.PL	Government Computer Emergency Response Team Polska
CIREX	Critical Infrastructure Resilience Exercises
CISA	Cybersecurity & Infrastructure Security Agency
CMMC	
CMU	Cabinet of Ministers of Ukraine
CRDF Global	Civil Research and Development Fund (U.S.)
CSE	Communications Security Establishment (Canada)
CSIS	Center for Strategic & International Studies (U.S.)
CTF	Capture the Flag
DDoS	Distributed Denial-of-Service
DerzhNDI	State Research Institute of Cyber Security and Information Protection Technologies
ECCRI	European Cyber Conflict Research Initiative
EU	European Union
FBI	Federal Bureau of Investigation
FSB	Federal Security Service (russian federation)
GRU	Main Directorate of the General Staff of the Armed Forces of the russian federation
HUMIT	Human Intelligence
ICS	Industrial Control System
ITSTIME	Italian Team for Security, Terrorism and Emergency Management
MISP	
NATO	North Atlantic Treaty Organization
NCSCC	National Coordination Cybersecurity Center
NCSC	National Cyber Security Centre (UK)
NGO	Non-Governmental Organization
NSA	National Security Agency (U.S.)
NSDC	National Security and Defense Council of Ukraine
OSINT	Open-source Intelligence
PGO	Office of the Prosecutor General of Ukraine
R&D	Research and Development
SBI	State Bureau of Investigation of Ukraine
SBU	Security Service of Ukraine
SOC	
SSSCIP	State Service of Special Communications and Information Protection of Ukraine
SVR	Foreign Intelligence Service of the russian federation
TAG	Threat Assessment Group
Trafficom	Finnish Transport and Communications Agency
UK	United Kingdom
VDP	Vulnerability Management

KEY TENDENCIES

In April, researchers focused a lot on a supply chain attack by North Korean hackers against the corporate communications company 3CX. The researchers noted that private companies were able to stop this attack, marking significant progress since the Solar Winds attack. The researchers also noted the complexity of the attack itself, which was a cascading supply chain attack. This was the first such attack and indicates a significant increase in the capabilities of North Korean hackers. At the same time, several critical infrastructure facilities in the USA and Europe were victims of the same North Korean group.

The European Union (EU) continues to reform the legislative framework of its own cyber security. Adopting the EU Cyber Solidarity Law will introduce important additional elements of protecting EU information systems against the growing risks of threats from foreign actors, primarily russia. Creating an SOC network, creating a cyber reserve for rapidly mobilizing qualified human resources, and introducing financial compensation tools for participants in cyber conflicts can all help the EU create a security model better adapted to current threats.

International cooperation is becoming more and more practically oriented and covers not only the exchange of technical information between relevant units but also the publication of common approaches to important problems. Just this month, a number of joint documents were presented: on the security of smart cities, secure-by-design principles, research on cyberattacks by russian advanced persistent threat (APT) groups (using the example of APT28), and Singapore and France began cooperation on using artificial intelligence (AI) in cyber security. Understanding the importance, the U.S. is increasingly turning to the idea of introducing a more integrated international cyber aid campaign of its own, including with an emphasis on Taiwan.

Destructive cyber activity is accelerating the pace of introducing tougher cybersecurity requirements around the world. The Cybersecurity & Infrastructure Security Agency (CISA) released an updated zero-trust maturity model. The U.S. Department of Defense is preparing to implement stricter requirements for subcontractor compliance with CMMC. The United Kingdom (UK) talked comprehensively for the first time about its own model of active (offensive) actions in cyberspace against malicious actors.

Experts warn that malicious groups are increasingly targeting the network equipment of key brands (primarily Cisco), hoping to gain a foothold in the networks and carry out more effective espionage or sabotage operations. Criminals' attention is constantly focused on industrial control systems (ICS). Experts indicate that hackers increasingly carry out successful attacks against such systems (for example, against Israeli irrigation systems) or are looking for opportunities. This is facilitated by the fact that industrial systems do not often update security approaches and it is difficult to replace them with more secure ones.

The Ukrainian side continues to build up the capacity of its cyber security specialists. The National Coordination Cybersecurity Center (NCSCC) holds training sessions on vulnerability management (VDP) for the employees of critical infrastructure facilities. The State Service of Special Communications and Information Protection of Ukraine (SSSCIP) and CYBER RANGES concluded a memorandum of cooperation to improve the employees' cyber defense skills, and the second All-Ukrainian cyber security capture-the-flag competition UA30CTF was held.

Legislative changes continue. In April, Ukraine approved a procedure for cyber incident and cyberattack responses common to all state institutions, decided to create a National Register of Backing up State Information Resources, and adopted a Cabinet of Ministers (CMU) resolution on using the platform for rapidly creating and managing state registers.

Ukrainian officials are focusing their attention on defining the term «cyber war». According to government agency representatives, this will make it possible to prosecute those who commit war crimes against Ukraine. The idea is being discussed both at the all-Ukrainian and international levels (at conferences in which Ukrainian specialists participated).

International cyber security organizations continue to expose russian malicious cyber activity and its sources. In April, several studies were made public about russian federation Federal Security Service (FSB) contractors and a game to create tools for these organizations to attack the critical infrastructure of democratic countries or conduct disinformation campaigns for their populations. Several hackers have been exposed who are supported by the Kremlin to conduct espionage campaigns against EU and NATO countries' diplomatic services.

russian cyber activity continues to grow. While groups such as KillNet cannot seriously disrupt the operation of important systems with their distributed denial-of-service (DDoS) attacks, other groups are looking for opportunities to conduct more complicated and complex operations. For example, there are attempts to attack network infrastructure, use vulnerabilities in Cisco equipment, create new ransomware, attacks on energy companies, and campaigns against diplomatic missions. Most likely, the number of these attempts will grow and russian cyber activity will only increase.

1. FIRST WORLD CYBER WAR

CYBER DIMENSIONS OF THE RUSSIAN-UKRAINE WAR

SOURCE 2

The European Cyber Conflict Research Initiative (ECCRI) published a workshop report on russian cyber warfare methods, commissioned by the UK's National Cyber Security Centre (NCSC). The workshop, held on February 28, focused on what russia has achieved, particularly the high pace of cyber operations, in contrast to the many and obvious ways in which russian cyber operations failed to fit in with pre-war expectations. Key takeaways:

- In line with its doctrine of information confrontation, russia employed a variety of cyber operations during the war at an unprecedented scale.
- The primary goals of wartime operations have remained constant: sabotage, influence, and espionage. Cyber operations provide new opportunities to achieve age-old objectives.
- Cyber activity in Ukraine is associated with kinetic activity bursts and lulls.
- The Main Directorate of the General Staff of the Armed Forces of the russian Federation (GRU) has adopted a flexible approach with «pure wipers» that are easy to manipulate and launch without draining significant resources.
- Western observers may overestimate coordination between russian-aligned criminals and the russian government.
- Distinguishing between cybercriminal groups and political activist groups is becoming increasingly difficult.
- Initiatives such as the IT Army risk blurring important principles of distinction between combatants and non-combatants.
- Responsibilities for cyber defense are shifting between public and private actors, with industry delivering capacity at scale.
- While Ukraine has benefited from unity of purpose across many different Western actors, this conflict may not provide a good roadmap for the future.

UKRAINIAN HACKTIVISTS USE NEW WAYS TO OBTAINING DATA ON RUSSIA'S WAR CRIMINALS

On April 1, The Hack Read offered an account of how Ukrainian hacktivists had convinced the wife of an active russian federation army colonel to take part in a patriotic photo shoot. She then convinced 12 more wives of servicemen to join, which allowed the hacktivists to obtain personal and confidential information about their husbands.

UKRAINIAN HACKTIVISTS CHANNEL FUNDS COLLECTED BY A RUSSIAN TO PURCHASE DRONES FOR OTHER PURPOSES

On April 3, the Liga news website reported that Ukrainian hackers from the Cyber Resistance group had prevented a russian blogger from purchasing drones for the russian army. They «played» with his card and, instead of drones, ordered sex toys worth $25,000 from an online store. The news item was reported via the group's Telegram channel.

THE WEST'S CYBER APPEASEMENT HELPED GIVE PUTIN A GREEN LIGHT

In a column published by The Washington Post on April 3, former supreme allied commander of NATO in Europe, retired U.S. Navy admiral James Stavridis expressed an opinion that the lack of an adequate response from the West to the russian federation's aggressive behavior in cyberspace had given a green light to putin's aggression. In his opinion, there was a failure in containment and diplomacy.

Admiral Stavridis suggested enhancing the training of American diplomats in technical matters and developing clear criteria for a clear and tough response to a cyberattack. He also underlined the need to realize that tolerance for low-intensity conflict in cyberspace is necessary to establish long-term deterrence mechanisms, even though the existence of such conflict poses the risk of escalation. «The U.S. needs to develop a sense of deterrence in cyber, and doing so will require more aggressive responses than it has been willing to employ thus far», Stavridis said.

UKRAINE WAR PLANS LEAK PROMPTS PENTAGON INVESTIGATION

On April 7, The New York Times reported that U.S. authorities were investigating an apparent leak of classified information related to U.S. plans to support Ukraine. The files were distributed via russian Twitter and Telegram accounts. Much of the information appears to be true (although at least some of it can be obtained from well-known open sources) and true enough to prompt an investigation. Other data, particularly casualty estimates, appear to have been falsified in russian interests (with russian casualties understated and Ukrainian casualties overstated) and seem to be a mixture of disinformation, which may be the main reason for their publication.

UKRAINIAN HACKERS HACK THE E-MAIL OF A RUSSIAN SPY WHO INTERFERED IN THE U.S. ELECTIONS

On April 11, Ukrainska Pravda reported that Ukrainian hackers had hacked the e-mail of russian spy Sergey Morgachev, who was wanted by the American FBI for hacking Hillary Clinton's presidential campaign in 2016. According to Inform Napalm, Morgachev's mailbox could potentially contain information about russia's hacking operations, including the operation against Clinton and the Democrats.

PRO-RUSSIA HACKERS SAY THEY WERE BEHIND HYDRO-QUEBEC CYBERATTACK

Pro-russia hacker group NoName057 (16) announced that it was behind the DDoS attack on Hydro-Quebec's website on the morning of April 13. Parts of the Quebec power utility's site were still down as of around 11:00 a.m. Hydro-Quebec says no personal data was compromised. In an online post, the group NoName057 (16) announced it was behind the hack but did not specify why it reportedly targeted Hydro-Quebec.

Earlier that week, there were attacks on Prime Minister Justin Trudeau's website, the Laurentian Bank of Canada website, and the websites of various Canadian ports, including the Port of Montreal and Port de Québec.

KREMLIN-BACKED BACKERS BLAMED IN SPYING CAMPAIGN ON EU AND NATO DIPLOMATIC AGENCIES – CERT.PL
SOURCE 2

russian state-affiliated hackers launched a spying campaign targeting foreign ministries and diplomatic entities in NATO countries, the EU, and, «to a lesser extent», Africa, Poland's top cybersecurity agency reported on April 13.

The campaign is linked to the Kremlin-backed hacking group Nobelium, also known as APT29 or BlueBravo. Nobelium is responsible for several high-profile incidents, including the SolarWinds supply chain attack in 2020. Nobelium's operations have been previously attributed to russia's Foreign Intelligence Service (SVR). Although Nobelium is closely tracked by researchers, the Government Computer Emergency Response Team Polska (CERT.PL) said the hackers employed tools and software that had not been previously reported on.

RUSSIAN HACKERS SUCCESSFULLY ATTACKED AN UNNAMED COMMERCIAL SATELLITE COMPANY IN 2022 - CSIS SPACE THREAT ASSESSMENT 2023

On April 14, the Center for Strategic and International Studies (CSIS) published its Space Threat Assessment 2023 report, which provides a comprehensive analysis of the aerospace dimension of the russia-Ukraine war. The report also considers the cyber component and its impact on satellites and electronic warfare. The report indicates (referring to a CISA representative's speech at a conference) that in 2022, russian hackers managed to penetrate an unnamed commercial satellite company and the incident was discovered only months later. Among other things, the report concludes that the Ukrainian example shows how countries that are smaller than their adversaries can effectively oppose the latter if they have an advantage in space.

RUSSIAN CYBERATTACKS CAUSE NO SIGNIFICANT DAMAGE TO CANADA – INTELLIGENCE

Robin Hauko, spokesperson for the Canadian governmental Communications Security Establishment (CSE), said on April 15 that the special service was investigating a series of cyberattacks that occurred during the visit of Ukrainian Prime Minister Denys Shmyhal to Canada. At the same time, he emphasized that cyberattacks on Canadian governmental websites had little impact on the affected systems. russian hackers managed to disable the official website of the head of the Government of Canada for several hours. The day before, there were technical problems on the website of the Canadian Senate.

«CSE and its Canadian Center for Cyber Security have observed that it is not uncommon to see DDoS attacks against countries hosting visits by Ukrainian government officials», noted the spokesman.

UKRAINIAN HACKERS ON THE FRONT LINE OF RESISTANCE TO RUSSIA IN THE CYBER WAR – BBC

In his article dated April 15, Joe Tidy talks about the results of his discussions with representatives of the Ukrainian hacker community, who put up their own resistance against russian aggression. He points out that a significant number of Ukrainian hackers not only take defensive measures, but also carry out counterattacks against russian information resources. At the same time, they often conducts these activities at their own discretion. Although the links between such hacktivists and Ukrainian authorities are often discussed, they do not come into direct contact or they have dealings only in cases when they are mobilized for military service.

KILLNET LAUNCHES A DDOS ATTACK ON THE EUROCONTROL WEBSITE

On April 19, criminal members of the KillNet group attacked the Eurocontrol website. The attack caused interruptions to the website and web availability, however there was no impact on European aviation. The attack partially affected the agency's internal and external communication systems, forcing the organization's 2,000 employees to use other means of commercial communication.

RUSSIA-BASED HACKERS RAMPING UP ATTACKS ON EASTERN EUROPEAN ENERGY SECTOR – GOOGLE SOURCE 2

russia-based hackers stepped up attacks on Eastern Europe's energy sector during the first three months of the year, according to new research by Google's Threat Analysis Group (TAG). In an April 19 blog post, the researchers outline coordinated campaigns operated by several known state-backed hacking groups, including:

- FROZENBARENTS, linked to the GRU (also known as Sandworm), which targets the energy sector and conducts hacking and data leakage operations;
- FROZENLAKE, linked to the GRU, which is involved in phishing campaigns against Ukrainians;
- PUSHCA, based in Belarus, which continues targeting regional webmail providers.

Ukraine remains one of the main targets of phishing attacks. According to the report, phishing campaigns backed by the russian government accounted for 60 percent of observed attempts from January to March.

RUSSIAN GROUP-IB ANNOUNCES ITS COMPLETE EXIT FROM THE RUSSIAN MARKET

On April 20, Group-IB, a well-known russian cybersecurity company, announced that it had finalized its exit from russia. According to Group-IB representatives, the company's main office is now located in Singapore. At present, the company's main activities are directed by Dmytro Volkov, as Illia Sachkov, the second co-founder, is under arrest on charges of treason.

Group-IB was repeatedly reported to act in close cooperation with Russian special agencies, mainly the FSB.

FINLAND, NOW A NATO MEMBER, SEES AN UPTICK IN CYBERATTACKS

Finnish organizations are increasingly being targeted with cyberattacks, the government announced on April 21, two weeks after the country officially joined NATO.

Kirsi Karlamaa, Director General of the Finnish Transport and Communications Agency (Trafficom), told reporters that its Cyber Security Center «receives more and more notifications every year, and there is a constantly growing interest in Finnish networks and organizations». She emphasized that the growing interest had become a constant trend.

A statement issued by the agency singled out russia as the source of the increase in cyber activity, highlighting Moscow's shift from on-the-ground intelligence gathering to the digital sphere. «russian cyber operations against Finland have also become more frequent because russia has been forced to turn to the cyber environment as its human intelligence operations have become more difficult», wrote the Agency.

Karlamaa added that ransomware attacks had become more targeted, with a shift occurring at the end of last year. Public agencies and critical infrastructure companies are of particular interest.

ANONYMOUS SUDAN CLAIMS RESPONSIBILITY FOR HACKING ISRAELI MOSSAD WEBSITE, MEDIA SAYS

The Times of Israel reported that the Anonymous Sudan group claimed responsibility for hacking the website of the Israeli intelligence agency, Mossad. The group said in a post on Telegram that «This attack is just a preparatory attack... for the big attack». It added that Anonymous Sudan is also responsible for hacking the websites of a number of Israeli banks and institutions over the past month.

NSA CYBER DIRECTOR WARNS OF RANSOMWARE ATTACKS ON UKRAINE, WESTERN SUPPLY CHAINS

russian hackers are attempting to inject ransomware into Ukraine's logistics supply chains and those of the Western countries that back Kyiv in its fight against moscow, National Security Agency (NSA) Director of Cybersecurity Rob Joyce told reporters during a roundtable at the RSA Conference on April 26. He emphasized that this tactic was new for russia and, most likely, resulted from understanding the importance of logistics, which the russian federation had learned from its own failures in this war.

RUSSIAN HACKERS ATTACK GERMAN MINISTRY'S WEBSITE

On April 5, the media reported that russian hacktivists in cooperation with the KillNet group had attempted to disable the recently created website of the German government dedicated to economic reconstruction of Ukraine, but they had failed.

RUSSIAN CYBER WEAPONS «COULD DO A LOT OF DAMAGE» IN THE U.S. – RICHARD A. CLARKE

In an April 4 interview with France 24 in New York, former U.S. counterterrorism czar Richard A. Clarke warned that russia's cyber weapons could potentially «do a lot of damage» in the U.S. To explain why this has not happened so far, he cited an «unwritten rule» he believes the U.S. and russia are both following: «[if] you don't attack me, I won't attack you». At the same time, Clarke stressed that the situation could change any day.

DDOS ATTACKS RISE AS PRO-RUSSIA GROUPS ATTACK FINLAND, ISRAEL

SOURCE 2

On April 6, TechRepublic reported that the pro-russia hacker group NoName057(16) had claimed it was behind DDoS attacks against the Finnish parliament's website on April 4, the day the country joined NATO. The Technical Research Centre of Finland was also hacked, according to Finnish news site YLE. NoName057(16) is the same group that took responsibility for a DDoS attack, taking down the website of the country's parliament last August, and also attacked Ukraine, the U.S., Poland, and other European countries.

russia-aligned hacktivists also attacked one of the biggest names in security, Check Point, along with universities and medical centers in Israel. The group called itself Anonymous Sudan, but Nadir Izrael, CTO and co-founder of asset visibility and security firm Armis, said the attacker is likely aligned with pro-russia hacktivist group Killnet.

Killnet ramped up attacks against U.S. entities this year and last, according to application performance management firm NetScout. In a new study, Unveiling the New Threat Landscape, NetScout said that the U.S. national security sector experienced a 16,815% increase in DDoS attacks in the second half of 2022, many related to Killnet.

RUSSIAN HACKERS ATTEMPT TO DESTROY THE UK'S CRITICAL INFRASTRUCTURE – BLOOMBERG

On April 19, referring to Bloomberg, the Liga news website reported that russia-aligned hackers were attempting to damage or destroy the UK's critical national infrastructure. The hackers, who are working for organizations similar in structure to the Wagner group, have turned their attention to the UK in recent months and pose a threat to businesses, according to Oliver Dowden, the chancellor of the Duchy of Lancaster, one of the highest ranking ministers in the government's Cabinet Office.

RUSSIAN INSURANCE COMPANIES LOSE MONEY DUE TO ATTACKS BY UKRAINIAN HACKERS – RUSSIAN MEDIA

In April 2023, the Ukrainian IT army organized a series of complex DDoS attacks on web resources and infrastructure of insurance companies in russia, which resulted in serious disruptions to their operations, the Liga news website reported on April 25 with reference to Gazeta.ru.

2. CYBERSECURITY SITUATION IN UKRAINE

HARMONIZING CRITICAL INFRASTRUCTURE CYBER SECURITY SYSTEMS WITH EU STANDARDS WAS DISCUSSED AT A MEETING OF THE NATIONAL CYBER SECURITY CLUSTER IN WARSAW

The 17th meeting of the National Cyber Security Cluster was held in Warsaw on the «Harmonization of critical infrastructure cyber security systems with EU standards». The NCSCC and the U.S. Civilian Research and Development Foundation organized the event with the support of the U.S Department of State.

«This is the first Cluster outside of Ukraine. It deals with an extremely urgent issue, harmonizing the Ukrainian cyber security system with EU standards. But it is worth noting that, in this process, we have to take into account the experience of our country in the war with the russian federation. Therefore, our meeting not only contributes to a deeper understanding of the specifics of the EU cyber security sphere but also allows us to share Ukraine's unique experience in cyber warfare with our partners», said Deputy Secretary of the National Security and Defense Council of Ukraine (NSDC) Serhii Demedyuk, opening the Cluster meeting.

Participants discussed issues related to Ukrainian and EU legislation on cyber security, practical steps for approximation, the importance of public-private partnership in this process, and reviewed the EU's best practices and experience. About 300 representatives of the public sector, the international and donor community, embassies, and private institutions took part in the meeting.

SERHIY DEMEDYUK: DEFINING THE CONCEPT OF «CYBER WAR» WILL CONTRIBUTE TO BRINGING TO JUSTICE THOSE WHO COMMIT WAR CRIMES AGAINST UKRAINE WITHOUT SETTING FOOT ON ITS LAND

Serhii Demedyuk, NSDC Deputy Secretary, took part in the annual All-Ukrainian scientific and practical conference on solving the issues of state information security management.

Organized by the National Academy of the Security Service of Ukraine, the event was also attended by representatives of the Ministry of Internal Affairs; the Security Service of Ukraine (SBU); the General Staff of the Armed Forces of Ukraine; the National Police; the State Security Service; the Committee of the Verkhovna Rada on National Security, Defense, and Intelligence; the Kyiv Chamber of Commerce; the National Academy of Sciences; higher education institutions; and the media.

Among the issues discussed during the conference, special attention was paid to the importance of a normative definition of the term «cyberwar».

«Today, everyone defines the concept of «cyber war» according to their knowledge and experience. But no country in the world still has a single clear formulation. We have to define the concept of «cyber war» and its interpretation. This will contribute to bringing to justice those who commit war crimes against Ukraine and its citizens without setting foot on Ukrainian soil», said Serhii Demedyuk, NSDC Deputy Secretary.

The conference participants discussed ways to counteract the russian federation's information and psychological influence on the Ukrainian military and strengthen the protection of information with limited access in wartime. It was also proposed to start unique scientific study of cyber warfare, involving representatives of all agencies in charge of cyber security, critical infrastructure facilities, non-governmental organizations (NGOs), and scientific institutions.

THE NCSCC INVESTIGATED CYBERATTACKS BY THE RUSSIAN APT28 GROUP CONNECTED TO THE MAIN INTELLIGENCE DIRECTORATE OF THE GENERAL STAFF OF THE RUSSIAN MOD

The NCSCC investigated attacks by the russian hacking group APT28 that actively exploits critical vulnerability CVE-2023-23397. Among the main conclusions:

- The APT28 group has been conducting attacks using a zero-day vulnerability in the Outlook mail client for at least a year.
- During this time, the following companies were victims of attacks: gas transportation system operators, private satellite intelligence companies and radar systems, institutions and organizations of the Ministry of Foreign Affairs and NATO, companies developing and supplying IT solutions, etc.
- The first attack was detected in March 2022 after the start of Russia's full-scale invasion. Since then, a number of attacks have been recorded on enterprises and organizations in Europe and the Middle East using the new critical vulnerability.

A detailed report on APT28 attacks using the CVE-2023-23397 vulnerability is available online.

DEFENSE TECH CLUSTER BRAVE1 LAUNCHED IN UKRAINE TO STIMULATE DEVELOPMENT OF MILITARY INNOVATIONS AND DEFENSE TECHNOLOGIES

The Ministry of Digital Transformation, the Ministry of Defense, the General Staff of the Armed Forces of Ukraine, the NSDC, the Ministry of Economy, and the Ministry of Strategic Industries presented the defense tech cluster BRAVE1. It is a single platform for the cooperation of defense tech companies, the state, the military, investors, volunteer funds, the media, and everyone who helps to bring victory closer through technology. Any person, startup, or company will be able to present their idea or product to BRAVE1 and receive a grant from the government. Thus, businesses will have opportunities for development and Ukraine's military will receive technologies for victory.

Defense tech industry companies will receive organizational and expert support for their designs and access to accelerators and incubators. The platform supports systematic work to improve developments, increase knowledge about business scaling, acquire value for investors, and mentoring.

BRAVE1's public and private stakeholder engagement experience and industry support will both help the Army and be a powerful export product. After all, Ukrainian defense tech solutions prove their effectiveness in the fiercest battles.

Submit project proposals and get access to military expertise, grants, and other opportunities provided by the cluster at: brave1.gov.ua

ILYA VITYUK: THE INTERNATIONAL TRIBUNAL SHOULD CONSIDER RUSSIAN CYBERATTACKS ON UKRAINE AS A WAR CRIME

The results of the SBU's criminal investigations into russian cyberattacks on Ukraine should be considered war crimes by the International Tribunal. This will make it possible to bring to justice the higher military and political leadership of the aggressor country, in particular, the special services, Head of the SBU Cyber Security Department Ilya Vityuk said at the annual the National Academy of the Security Service's All-Ukrainian scientific and practical conference.

«Today, when the question of the International Tribunal regarding the crimes of the russian federation in Ukraine arose, russian cyberattacks should also be considered a war crime. For example, the cyberattacks on energy facilities, especially in winter. Failure of these systems results in civilian casualties. And this is a real war crime», Vityuk emphasized.

«If we talk about personal responsibility for these crimes, it should be borne not only by those who commit the attacks, but also by people who give the criminal orders. For example, the director of the FSB and heads of other russian special services should be punished», Vityuk believes.

NCSCC STARTED COOPERATION WITH THE NATIONAL CYBER SECURITY DIRECTORATE OF ROMANIA TO CREATE A SAFE CYBERSPACE AND COUNTER CYBERATTACKS

The NCSCC and the National Cyber Security Directorate of Romania signed a memorandum of understanding on cyber security cooperation.

«russian hackers are a threat not only to Ukraine but also to the whole world. They continue to attack our partners, the states that provide comprehensive support to Ukraine to win this war. Therefore, joint efforts and coordination in countering cyber threats are extremely important today. In addition, Ukraine is currently gaining unique experience we are ready to share with the international community in order to ensure peace and security in cyberspace», said Serhiy Demedyuk, NSDC Deputy Secretary.

The memorandum provides for exchanging experience and best of cyber security; participating in educational, scientific, and technical projects; and exchanging information on cyber incidents, methods of detecting vulnerabilities, and responding to cyber threats.

THE MINISTRY OF DIGITAL TRANSFORMATION, SSSCIP, AND THE MINISTRY OF DIGITALIZATION OF JAPAN SIGNED A MEMORANDUM OF COOPERATION

Ukraine and Japan agreed to cooperate on digital transformation. The Ukrainian Ministry of Digital Transformation, SSSCIP, and the Ministry of Digitalization of Japan signed a tripartite memorandum for the first time, marking the beginning of powerful digital cooperation between the two countries.

The memorandum was signed at an online meeting between the Deputy Prime Minister for Innovation, Development of Education, Science, and Technology — Minister of Digital Transformation of Ukraine Mykhailo Fedorov and Minister of Digitalization of Japan Taro Kono.

«The Japanese government has now focused on improving public services. Therefore, a year and a half ago, the Ministry of Digitalization was established there. In Ukraine, this process has been going on for more than three years. We are building the most convenient digital state, launching new online services, even despite the challenges of war. I am convinced that Japanese-Ukrainian relations have great potential because the exchange of digital cases between our countries will be useful for both sides», Fedorov noted.

Under the memorandum, Japan will help Ukraine develop innovations and strengthen cyber defense. Today, Ukraine is facing the enemy not only at the front, but also in cyberspace. Japan's technological solutions will help strengthen Ukrainian digital borders and protect information systems of critical infrastructure facilities. The ministers also agreed to exchange best practices in developing the IT industry and e-government.

THE MINISTRY OF DEFENSE AND THE COMPANY INTERNET2.0 SIGNED A MEMORANDUM OF COOPERATION IN COMMUNICATION AND INFORMATIZATION

Deputy Minister of Defense for digital development, digital transformations, and digitization Vitaliy Deineha and co-founder of the Australian company INTERNET2.0 Robert Potter signed a memorandum on cooperation.

The memorandum officially confirms the parties' intentions to exchange experience with communication and informatization, implementation and development of the latest information technologies and processes, and digitalization in the field of defense. The memorandum also includes studying and demonstrating innovative technologies in defense, software, and hardware developed by the Australian company, in particular Cloaking Firewall and Malcore.

Among other things, the signatories' main efforts will be focused on exploring the use of the Advanced Practices information and analytical system INTERNET2.0 developed to improve situational awareness, threat assessment, crisis forecasting, response, and recovery.

CYBER EDUCATION, TRAINING AND PROFESSIONAL DEVELOPMENT IN CYBER DEFENSE: SSSCIP AND CYBER RANGES SIGNED A MEMORANDUM OF COOPERATION

Representatives of leading international CYBER RANGES Corp visited the SSSCIP. The company specializes in developing technological solutions and conducting cyber defense exercises using next-generation technologies and high-precision modeling.

The SSSCIP Deputy Heads Viktor Zhora and Oleksandr Potiy introduced the CYBER RANGES head of marketing and business development Marcello Hinksman-Allegri to the training center's capabilities at the Cyber Center UA30, and talked about the work of the Governmental Computer Emergency Response Team (CERT-UA) and the SSSCIP's important role in ensuring Ukraine's cyber defense.

During the visit, the SSSCIP and CYBER RANGES signed memorandum of cooperation that stipulates, among other things:

- Exchanging information, experience, and best practices in cyber defense, conducting training courses, trainings, and joint exercises on the CYBER RANGES PCTE platform
- Educational activities related to cyber threats
- Participating in advanced cyber defense training programs and organizing qualification examinations and procedures for assigning/confirming professional qualifications according to Ukrainian cyber defense professional standards based on CYBER RANGES technologies.

NSDC HELD A 5-DAY WORKSHOP FOR SPECIALISTS OF CRITICAL INFRASTRUCTURE ENTERPRISES WITH THE SUPPORT OF THE U.S. STATE DEPARTMENT

The NSDC held the 5-day seminar «Security and stability of critical infrastructure» for critical infrastructure specialists in the Ukrainian public and private sectors. The event was held with the support of the U.S. Department of Homeland Security, CISA, and the U.S. Civilian Research and Development Foundation (CRDF Global).

The purpose of the training is to build the capacity and stability of Ukrainian critical infrastructure facilities, as well as their interaction at both the individual facility and the national level. CISA experts led various interactive sessions, lectures, discussions, and group sessions. In addition, the participants could exchange experiences and discuss joint efforts in relevant fields.

About 20 specialists participated in the event, including representatives of the NSDC, SSSCIP, SBU, the State Emergency Service, Ministry of Health, Ministry of Energy, Ukrtransgaz, Ukrenergo, Naftogaz, and National Institute for Strategic Studies Center for Security Studies.

NCSCC INTRODUCED OF NATIONAL DEFENSE UNIVERSITY STUDENTS TO THE NATIONAL CYBER SECURITY SYSTEM AND NCSCC POWERS

Over 50 students in the training course for strategic-level security and defense sector officers at the Ivan Chernyakhovsky National Defense University of Ukraine were introduced to the principles of operating and developing the Ukrainian cyber security system and the technical capabilities of the NSDC NCSCC.

Natalia Tkachuk, head of the NSDC information security and cyber security service and NCSCC specialists participated in the meeting at the NCSCC technical site. Participants discussed Ukraine's national cyber security system and the importance of the NCSCC's coordinating role and place. The military personnel were shown the NCSCC's technical capabilities, which specialists use to promptly detect and analyze cyber incidents. They also discussed problematic issues in the cyber security and ways to solve them.

Special attention was paid to coordination during cyberattack responses. NCSCC specialists informed the audience about technical capabilities and tools for detecting signs of cyberattacks. They also emphasized the importance of mutual exchange of information between all subjects to ensure Ukraine's cyber security, in particular using the NCSCC's MISP platform.

NCSCC CONDUCTED «VULNERABILITY MANAGEMENT» TRAINING FOR CYBER SECURITY SPECIALISTS IN UKRAINE'S ENERGY SECTOR

With CRDF Global support, the NCSCC held a training from the Vulnerability Management (VDP) series on March 13-April 20, 2023.

More than 30 dedicated technical specialists attended the tenth program, representing 20 Ukrainian energy sector organizations, including the Ministry of Energy, Energoatom, Ukrenergo, and regional energy companies. The participants were very interested in solving the tasks at the final CTF. The winners of the 6-week training received prizes that will help them further develop their professional skills.

The purpose of these events is to develop practical skills to identify vulnerabilities in information systems and provide comprehensive cyber defense at the main entities in charge of cyber security, government institutions, critical infrastructure facilities, and other organizations as part of public-private partnerships.

THE FIRST CERTIFIED OSINT AND HUMINT TRAINING WAS HELD FOR SECURITY AND DEFENSE FORCES

The SSSCIP's State Research Institute of Cyber Security and Information Protection Technologies (DerzhNDI), in partnership with the Italian Team for Security, Terrorism, and Emergency Management (ITSTIME) conducted the first certified intelligence training based on data from open sources (OSINT) and search for information using human intelligence (HUMINT) for Ukraine's security and defense sector specialists.

The Italian specialists focused on the strategies and practices the enemy uses in digital technologies and social networks in order to collect information on the Internet, the deep web, and the dark net. The Ukrainian specialists also learned to navigate the enemy's digital networks, identify possible targets, and conduct information operations in enemy networks.

Participants honed their skills in monitoring various types of threats, forming prevention strategies and developing emergency response plans, risks, and crises. Among other things, the certified training deepens understanding about the importance of strategic communication and preventing enemy propaganda in hybrid warfare.

THE CERT-UA TEAM WON THE QUANTICO CYBER EAGLE TROPHY AT THE U.S. MARINE CORPS CYBER TRAINING

At the invitation of the U.S. Marine Corps, four SSSCIP teams took part in the Quantico Cyber Eagle cyber security training at the end of March at the CYBER RANGES technology training ground in Quantico (USA).

The event brought together 11 teams to train elite cyber specialists capable of conducting modern defense operations and confronting a smart and resourceful enemy. These challenges require cyber professionals to train in simulated environments that reflect ever-changing threats.

The scenario imitated a russian special services cyberattack on the embassy of a fictional NATO country. The similarity of tactics, techniques, and procedures used to carry out real cyberattacks on Ukraine and NATO countries gave the Ukrainian teams the opportunity to practice and hone their skills to promptly respond to cyber incidents. Participants were also able to test their teamwork skills in a high-fidelity simulation environment that replicated the tactics and methods enemy actors use in cyberspace.

NCSCC JOINED THE INTERNATIONAL CONFERENCE «CYBER WARFARE: INTELLIGENCE, DEFENSE AND COUNTERMEASURES»

On April 20, Serhiy Prokopenko, Head of the NCSCC Department for Ensuring the Activities of the NSDC Specialized Service, took part in the international conference «Cyber Combat: Intelligence, Defense and Countermeasures». The Kruty Heroes Military Institute of Telecommunications and Informatization organized the event with the support of the NCSCC, the Command of Communications and Cyber Security Forces of the Armed Forces of Ukraine, and international partners CRDF Global, E-Governance Academy (Estonia), Regional Cyber Defense Center (Lithuania), and Nikola Vaptsarov Naval Academy (Bulgaria).

The goal of the conference was for scientific teams of European countries to cooperate in modern peace and security projects and to use modern cyber training grounds and platforms for training cyber security specialists.

«Now it is necessary to focus on an in-depth analysis of Ukraine's experience in cyber warfare and the possibilities to forecast situation developments. We must share this experience with our international partners, interacting at all levels – interstate, private, and academic. After all, only this kind of cooperation will contribute to creating new approaches to countering our common enemy and help prevent future cyberattacks more effectively», Serhiy Prokopenko said opening the event.

Security and defense sector representatives from Ukraine, the United States, Norway, and Estonia took part in the conference. They discussed cryptographic solutions for cyber security, intelligent analysis of incidents, signal structures in cyberspace, and support for solutions to ensure cyber defense.

INNOVATIONS AND DIGITAL TRANSFORMATION INITIATIVES IN THE ARMED FORCES: VITALY DEINEHA PARTICIPATED IN THE NATO TIDE SPRINT CONFERENCE SOURCE 2

Deputy Minister of Defense for Digital Development, Digital Transformation and Digitalization Vitaliy Deineha took part in the NATO TIDE Sprint conference organized by the NATO Transformation Command in Norway (Lillehammer).

At the plenary session, Deineha informed the participants about current innovations and digital transformation initiatives in support of the Armed Forces of Ukraine. In particular, he talked about developing situational awareness solutions and using unmanned aerial vehicles and non-standard approaches in russia's war against Ukraine. The Deputy Minister emphasized the importance of closely cooperating with the civilian sector and focusing on and taking into account the technological needs of military personnel in the area of hostilities.

UKRAINE IS READY TO DEEPEN COOPERATION WITH PARTNERS ON CYBER DEFENSE

Countering hostile military cyber operations requires high-quality interaction and significant intellectual resources, which must be accumulated. Ukraine has gained unique practical experience during the nine years of war and is ready to more closely interact with colleagues from the Black Sea region, in particular by participating in joint research and development (R&D) and educational projects.

This was discussed during an expert discussion at the Black Sea Security Conference of the International Crimean Platform in Bucharest, Romania. «We have to deepen our cooperation. I mean not only sharing information about incidents and certain knowledge, but also working together and participating in joint R&D and educational projects. Together, we will be able to achieve better results», emphasized Nazar Tymoshyk, a member of CERT-UA.

PUBLIC-PRIVATE PARTNERSHIP IS ONE OF THE KEY FACTORS OF OUR CYBER RESILIENCE - SSSCIP DEPUTY HEAD

The SSSCIP paid considerable attention in recent years to constantly and systematically developing public-private partnerships, which helped Ukraine to resist russian cyberattacks more effectively. Viktor Zhora, SSSCIP Deputy Head, noted during the panel discussion Advancing Public-Private Partnerships in Cyber Threat Intelligence and Cyber Crisis Response at the European Cyber Agora hybrid conference in Brussels.

«Cooperating with the private sector to jointly combat threats, strengthen our ability to resist russian cyber aggression, and develop human resources is one of the key factors of our stability during the full-scale war», Zhora emphasized during his online speech. He shared the Ukrainian experience of establishing effective public-private cooperation mechanisms and called on the conference participants to pay more attention to this kind of cooperation, deepening the existing partnerships and developing new ones.

UKRAINE IS STARTING TO BUILD A CRITICAL INFRASTRUCTURE PROTECTION SYSTEM IN ACCORDANCE WITH THE BEST GLOBAL PRACTICES AND THE CURRENT EUROPEAN LEGISLATION REQUIREMENTS

SSSCIP Deputy Head Oleksandr Potiy spoke at the panel discussion, «Protection of critical infrastructure during the future restructuring of the energy industry». He noted that Ukraine is studying the EU directives NIS 2 (EU 2022/2555) and RCE (EU 2022/2557) on the protection of critical infrastructure and is cooperating with countries that have already started implementing them.

In addition, Ukraine cooperates fruitfully with CISA, which organization has leading experience in protecting critical infrastructure. The SSSCIP and CISA signed a memorandum of cooperation and have already conducted training in accordance with the CISA methodology.

The event participants talked about how one of the enemy's main targets during a full-scale war is energy infrastructure. From October 2022 to February 2023, the russian federation fired 1,500 missiles and kamikaze drones at the Ukrainian energy system, and 100 of them hit large energy facilities. As a result of the shelling, Ukraine lost 61% of its power generation. In order to get through the next winter, it is necessary to intensify efforts to prepare for threats and protect energy infrastructure.

The panel discussion was part of the EUROSCOPE project, which examines Ukraine's approach to EU membership.

GOVERNMENT APPROVES THE PROCEDURE FOR RESPONDING TO CYBER INCIDENTS AND CYBER ATTACKS
SOURCE 2

The CMU approved the resolution «Procedure for Responding to Various Types of Events in Cyberspace by Cyber Security Actors» that the SSSCIP developed. The resolution was adopted as part of the Ukrainian Cyber Security Strategy Implementation Plan.

The procedure will make it possible to initiate cyber incident and cyberattack response processes in line with pre-planned cyber security measures to:

- rapidly detect and protect against cyber incidents and cyber attacks
- ensure proper notification of such events and prevent, minimize, and eliminate negative consequences
- address vulnerabilities and restore the stability and reliability of information, electronic communication, information and communication, technological, and other systems whose cyber security should be protected.

Within three months from the date the resolution enters into force, the SSSCIP is expected to issue guidelines on how cyber security actors should respond to cyberspace events covered by the procedure.

The Procedure for Responding to Various Types of Events in Cyberspace by Cyber Security Actors contributes to developing the approaches outlined in the organizational and technical model of cyber security the SSSCIP developed at the end of 2021.

GOVERNMENT APPROVES A RESOLUTION TO INTRODUCE A PLATFORM TO STREAMLINE CREATING AND MANAGING STATE REGISTERS

The Ministry of Digital Transformation and SSSCIP teams are involved in developing an innovative solution, the State Electronic Register Deployment and Support Platform. The platform will allow ministries and governmental agencies to quickly and conveniently create and manage public registers.

There are currently over 450 state registers in Ukraine, 80 percent of which are technologically outdated and vulnerable to cyberattacks. The platform will provide the basis for digital transformation: all data will be structured and stored in registers, which will speed up launching online services and digitalization efforts in general. The platform allows creating new registers as well as also technically rebuild and gradually transfer outdated registers. All changes are recorded and take place only as business processes, which prevents unauthorized data manipulation.

The platform makes it possible to develop registers without large teams or highly qualified specialists. A person can easily and quickly learn how to use the development tools. Training and consulting will be available for developers.

STRENGTHENING SECURITY OF NATIONAL ELECTRONIC INFORMATION RESOURCES (GOVERNMENT RESOLUTION)

The state's task is not only to build an efficient security system, but also ensure data backup for quick recovery if the need arises. As early as 2021, for this purpose within the framework of the Cybersecurity Strategy of Ukraine, a decision was supported to create the National Register for Backing up State Information Resources, and the SSSCIP was named the agency responsible for operating and developing the register.

Another important resolution the Government passed is «Some Issues Related to Operation of the National Center for Backing up State Information Resources», which establishes the:

- Procedure for operating the National Center for Backing up State Information Resources, which clearly defines roles and responsibilities for those involved in the National Backup Center.
- Procedure for transferring backup copies of national electronic information resources to the National Center by Public Authorities, Military Units, Enterprises, Institutions, and Organizations, as well as the mechanism for storing and accessing them. Among other things, it defines the types of national electronic information resources to back up, the contract requirements for storing backup copies, requirements for information protection and cyber security during storage, and the procedure for transferring to Ukraine's foreign diplomatic institutions during martial law and return after it is lifted.

«The approved resolution will allow us to minimize risks, ensure the continuous operation of national electronic information resources, and creates the possibility of restoring data in case of damage or deletion. Our common aim is to secure and protect critically important information related to our governmental agencies, businesses, and citizens», said Yurii Shchyhol, SSSCIP Head.

THE SSSCIP INVITES BUSINESSES AND PROFESSIONAL ASSOCIATIONS TO SUBMIT PROPOSALS FOR EXPANDING CYBER SECURITY OCCUPATION CLASSIFICATIONS SOURCE 2

Reforming Ukrainian professional education in cyber security requires involving businesses and professional associations, particularly in developing professional cyber security standards. Participants discussed this issue during the meeting «Professions and Careers in the Area of Cyber Security», which took place on April 5 in Kyiv.

«A few years ago, there were only two professions in the state classification of professions, an information security professional and a specialist in information protection. So far, we have added 27 relevant job titles and developed and approved professional standards for six of them. This year, we are going to develop professional standards for another 14 professions», noted SSSCIP Deputy Head Oleksandr Potiy at the event.

Incorporating these professional standards into the Qualifications Register, which was developed with the support of the USAID Cybersecurity for Critical Infrastructure in Ukraine Activity, allows higher education institutions to adjust educational programs and introduce appropriate training specializations, and gives specialists and employers an opportunity to select specialists by profession.

FREQUENCY AND INTENSITY OF RUSSIAN CYBERATTACKS REMAIN HIGH (REPORT)

SOURCE 2

The number of attacks by pro-russian groups on the commercial and financial institutions, the Government and local authorities, and the security and defense sector has decreased since the beginning of 2023, compared to the previous quarter. At the same time, the intensity of attacks on the energy sector and mass media remains at the same level, according to the State Cyber Protection Center's «Report on Performance of the System for Detecting Vulnerabilities and Responding to Cyber Incidents and Cyber Attacks».

During the first quarter of 2023, the System for Detecting Vulnerabilities and Responding to Cyber Incidents and Cyber Attacks detected 7 million suspicious information security events (as part of an initial analysis); processed 34,000 critical information security events (potential cyber incidents detected as a result of examining suspicious information security events and conducting a secondary analysis); and recorded 202 cyber incidents that were processed directly by security analysts.

SBU CLOSES THE KROPYVNYTSKYI BOT FARM THAT CREATED OVER 3,000 FAKE ACCOUNTS FOR INFORMATION SABOTAGE ATTACKS AGAINST UKRAINE

SBU cyber specialists neutralized a bot farm based in Kropyvnytskyi that was operated in the interests of the russian special services. Investigative and operational efforts resulted in detaining the person responsible for organizing the hostile activities. He created large quantities of anonymous social media accounts and sold them through the darknet. The average cost of one bot was UAH 200 ($5.40).

The SBU established that the threat actor created almost 3,000 fake accounts, which he planned to sell for over UAH 500,000 ($13,500). His major «clients» were representatives of the russian special services and pro-Kremlin propagandists they control.

The aggressor needed the bots to disseminate false information to Ukrainian citizens about the situation at the front and to attempt to discredit the Ukrainian Defense Forces. The enemy tried to destabilize the internal political situation in various regions of Ukraine during the wartime.

CYBER POLICE DISCOVER AN OFFENDER INVOLVED IN SELLING DATABASES WITH PERSONAL INFORMATION OF UKRAINIAN AND EU CITIZENS

A man was selling information via a messenger that contained the personal data of more than 300 million people from different countries. During an authorized search, the suspect interfered with the actions of law enforcement officers and caused bodily injuries to a cyber police officer. The offender was detained.

The 36-year-old resident of Netishyn was an administrator of closed Telegram groups and channels, which he used to sell the personal data of more than 300 million citizens of Ukraine and EU countries. In particular, the offender had passport data and information related to taxpayer ID numbers, birth certificates, driver licenses, and bank accounts. The offender charged $500-$2,000, depending on the amount of data.

It was previously established that there had been citizens of the aggressor country among his buyers, as well. The offender received payments for databases sold to russian federation citizens using currencies prohibited in Ukraine.

Law enforcement officers came to the suspect to conduct a search as part of the pre-trial investigation of criminal proceedings initiated under paragraph 2 of Article 361-1 (creating malicious software or hardware solutions for illegal use, distribution, or sale, including distribution or sale) and Article 362 (unauthorized operations using information processed in computers, automated systems, computer networks, or stored on data carriers of such information, performed by a person who has relevant access rights) of the Criminal Code of Ukraine and on the basis of a court order.

In response to the attack on the cyber police officer, Shepetivka District Police Department investigators started a pre-trial investigation under paragraph 2 of Article 345 (threats or violence against a law enforcement officer) of the Criminal Code of Ukraine. The article provides for restricting or depriving liberty for a period of up to five years . An investigation is currently underway.

TWO TRAITORS WHO HELPED THE FSB CARRY OUT HACKER ATTACKS ON THE GOVERNMENT OF UKRAINE WILL BE TRIED BASED ON SBU MATERIALS

SBU cyber specialists in cooperation with the State Bureau of Investigations (SBI) and Prosecutor General's Office (PGO) collected evidence against two more military traitors who assisted the russian federation in the war against Ukraine. The suspects are two former SBU employees in the Autonomous Republic of Crimea who defected to the enemy in 2014 and joined the FSB. They became members of the Armageddon hacker group controlled by the russian special services.

The investigation established that the offenders carried out large-scale cyberattacks on Ukrainian government agencies between January 1, 2020, and March 10, 2021. During one of the cyber incidents, the FSB tried to gain access to secret data of Ukraine's highest authorities. However, the SBU's prompt response made it possible to neutralize the consequences of and eliminate the prerequisites for the russian special services to penetrate the Ukrainian governmental information resources.

As a result of a comprehensive set of measures, law enforcement officers established that the traitors had been involved in subversive activities conducted by the aggressor. In 2021, SBU cyber specialists carried out an unprecedented operation and identified the offenders, intercepted their conversations, and obtained indisputable evidence of their participation in cyberattacks on Ukraine, even despite the fact that they used FSB virus software, anonymization tools, for «covering» on the Internet.

At that time, eight enemy hackers were identified at once, five of whom immediately received notifications of suspicion. So far, law enforcement officers have completed the investigation in relation to the two of them. They are charged under two articles of the Criminal Code of Ukraine: paragraph 1 of Article 111 (Treason) and paragraph 2 of Article 361 (Unauthorized interference with operation of electronic computing machines (computers) and automated systems). The perpetrators face up to 15 years in prison.

KHARKIV OBLAST CYBER POLICE IDENTIFIED MEMBERS OF TWO CRIMINAL GROUPS INVOLVED IN EMBEZZLING ALMOST 2 MILLION UAH USING PHISHING TECHNIQUES

The criminals used similar schemes: they obtained citizens' bank card data via phishing links that imitated the interface of online banking pages, advertising services sites, online stores, etc. Over 1,000 citizens suffered from their illegal activities, which caused damage to the victims totaling 2 almost two million UAH ($54,000).

Members of the two criminal groups were identified by employees of the Kharkiv Oblast Cybercrime Prevention Department in cooperation with the National Police's Main Investigation Department and with the assistance of the security services of Monobank and PrivatBank.

One of the groups consisted of 13 individuals who joined together to create and administer a Telegram community where they posted instructions and phishing links for other members of the fraud group. Then the offenders sent out those links via messengers as offers to arrange financial payments and receive funds for goods sold. Users entered data on phishing sites that the offenders automatically obtained.

The organizer of the scheme compromised bank clients' payment cards and transferred the victims' money to controlled accounts using payment systems. A similar scheme was used by three residents of Dnipropetrovsk Oblast.

Criminal proceedings have been initiated under par. 1, 2 of Article 255 (Creating and managing a criminal community or criminal organization, as well as participating therein) and par. 4 of Article 190 (Fraud) of the Criminal Code of Ukraine. The offenders face up to 12 years in prison with confiscation of their property.

«A FRIEND IN NEED OF A LOAN»: DNIPROPETROVSK OBLAST CYBER POLICE IDENTIFY A CRIMINAL GROUP INVOLVED IN FRAUDULENT ACTIVITIES

The offenders created fake pages of messenger users and asked their friends to loan them money. The offenders managed to obtain over 300,000 UAH ($8,100). Law enforcement officers notified the group organizers of the suspicion.

Six citizens, residents of Kamianske and Verkhivtseve, looked for open group chats in messengers and created fake pages. Using clone accounts, they wrote to other chat participants asking to borrow money or give donations allegedly collected as charity for service members. The criminals defrauded about 70 people this way.

SSSCIP CONDUCTS TABLE TOP EXERCISES FOR BETTER PROTECTION OF ENERGY INFRASTRUCTURE AGAINST CYBER ATTACKS

With support from the USAID Cybersecurity for Critical Infrastructure in Ukraine Activity, the SSSCIP conducted the first table-top Critical Infrastructure Resilience Exercises (CIREX), developed based on CISA guidelines.

The main goal of CIREX was to work out issues related to countering cyber threats and coordinating efforts to repel cyberattacks. Energy sector representatives attended the training, working on employing mechanisms to respond to ransomware cyberattacks during the day (ransomware programs in accordance with the current taxonomy of cyber incidents).

Farid Safarov, Deputy Minister of Energy for Digital Development, Digital Transformation, and Digitalization, noted that he is proud of the team responsible for the energy industry's cyber security. He added that «one man no man» when it comes to fighting against hackers.

Participating in the CIREX were representatives of Ukrenergo, DTEK Group, Kyivteploenergo, Naftogaz of Ukraine, Energoatom National Nuclear Power Company, the Ministry of Energy, and specialized agencies responsible for protecting critical infrastructure, in particular the SBU, National Police, and NSDC Executive Office.

SSSCIP HOLDS THE SECOND ALL-UKRAINIAN UA30CTF CYBER SECURITY COMPETITION
SOURCE 2

The SSSCIP held the all-Ukrainian online youth cyber security competition UA30CTF. Over 400 participants, united in 107 teams from different regions of Ukraine, participated in the event.

The competition was in the format of a #Jeopardy CTF game. Over 12 hours, the teams carried out 25 tasks to find and exploit vulnerabilities in combination with solving interesting logical problems.

LunarLobsters took first place, and Knotty Kitten and Arctic Warriors took second and third place.

GOOGLE LAUNCHES THE ONLINE GAME «INTERLAND: CHILDREN'S ONLINE SAFETY» IN UKRAINE
SOURCE 2

The online game is designed to help children acquire important digital skills, which will ensure children's online safety and assist them in growing into responsible digital citizens. The Ministry of Digital Transformation the Diia.Digital Education project provided informational support for launching the game.

Digital threats on the Internet include online hooliganism, cyberbullying, and fraud. Therefore, teaching children online safety skills is important in terms of protecting them and ensuring that they use the Internet responsibly.

Interland: Children's Online Safety is now available in Ukrainian and is free of charge, so it is accessible to everyone, and most importantly, it is provided in a format that is understandable and interesting for children. In the imaginary world of Interland, children will learn how to safely share information online, recognize fakes, and fight hackers, phishers, and cyberbullies.

KYIVSTAR PROVIDES 300 MILLION UAH TO DEVELOPMENT DIGITAL UKRAINE

The national telecom operator transferred the last portion of the total investments of UAH 300 million ($8.1 million) to the state account. The funds were allocated for state projects related to digital development and Ukraine's cyber security.

«Digital infrastructure provides the basis for the state to efficiently function during the full-scale war. Customs authorities work, pensions and salaries are paid, and government departments are fully operational. Almost every week, the Ministry of Digital Transformation launches new Diia services. And all this is happening during the world's first cyber war. We are grateful to Kyivstar for its contribution to developing digital Ukraine. The support allows us to implement top projects to strengthen the security and reliability of digital infrastructure», said Mykhailo Fedorov, Deputy Prime Minister for Innovation, Development of Education, Science and Technology and Minister of Digital Transformation.

According to the Ministry of Digital Transformation, the funds are channeled to priority projects digitally transform notary services (e-notary) and consignment notes (e-CN), digitalize civil registry office services, etc. The funds are also used to modernize and develop state registers, strengthen information security, and enhance the country's cyber protection.