USAID
FROM THE AMERICAN PEOPLE

USAID CYBERSECURITY FOR CRITICAL INFRASTRUCTURE IN UKRAINE

Cyber Sector Update

October 2023 – December 2023

The USAID Cybersecurity for Critical Infrastructure in Ukraine Activity (the Activity), implemented by DAI Global LLC, is designed to reduce cybersecurity vulnerabilities in critical infrastructure (CI) sectors and transform Ukraine from a compromised, reactive cybersecurity actor to a proactive cybersecurity leader. Recognizing the complexity of the threat posed by Russian hybrid warfare, the Activity has adopted a multi-sector approach that engages government, businesses, and academia to improve Ukraine's cybersecurity for CI. Through three strategic objectives, the Activity is improving the enabling environment for cybersecurity, strengthening Ukraine's cybersecurity workforce, and stimulating market development to promote Ukrainian cybersecurity products and services.

This publication is made possible by support of the American people through the United States Agency for International Development (USAID). Its contents are the sole responsibility of the USAID Cybersecurity for Critical Infrastructure in Ukraine Activity and do not necessarily reflect the views of USAID or the U.S. Government.

SUMMARY

INCIDENTS

- Millions of Hryvnias at Risk: CERT-UA Detected at Least Four Waves of Cyberattacks Against Accountants in October
- Ukraine, Israel, and South Korea Top the List of Most-targeted Countries for Cyberattacks
- Sandworm Wages Cyberattacks Against Ukrainian Telecomms Providers
- Russian Hackers Used OT Attack to Disrupt Power in Ukraine Amid Mass Missile Strikes
- Hackers Disguise Themselves as State Security Service
- CISA's Goldstein: Ukrainian response to Viasat hack proves need for redundancy, resilience
- Kyivstar, Ukraine's Largest Telecom Operator, Hit by Massive Cyberattack Causing Network Disruptions

PUBLIC SECTOR DEVELOPMENTS

- USAID-supported Tabletop Exercise CIREX.CoBridge Helps Strengthen Ukraine's Critical Infrastructure Resilience
- USAID Supports Regional Cybersecurity Contest in Kharkiv
- USAID Supports Tabletop Exercise Facilitator Training for SSSCIP Staff
- USAID Restores and Enhances Digital Infrastructure at 25 Ukrainian Universities
- SSSCIP Leadership Undergoes Changes
- USAID Advances Cybersecurity Workforce Development Agenda to the Next Level
- USAID Contributes to Unlocking Ukraine's Innovative Potential and Supports Cybersecurity Efforts

- USAID Facilitated Adoption of New Cybersecurity Professional Standards in Ukraine

LEGAL DEVELOPMENTS

- UN Member States Reform Cybercrime Legislation, Paving the Way for Comprehensive International Convention
- EU Set to Adopt Cyber Resilience Act to Improve Digital Product Security
- Ukraine's AI Road map Seeks to Balance Innovation and Security

PRIVATE SECTOR DEVELOPMENTS

- SSSCIP Takes Steps to Build HR Capacity in Information Security and Cybersecurity
- Ukrainian National Coordination Center for Cybersecurity and IP3 International announce the Collective Defense AI Fusion Center (CDAIC) in Ukraine
- USAID and Cisco Partner to Support Education and Cybersecurity in Ukraine
- Recorded Future Continues to Provide Critical Intelligence to Protect Ukraine from Cyber, Physical and Kinetic Threats

INTERNATIONAL COOPERATION

- NCCC Secretary Nataliya Tkachuk Highlights Importance of Electronic Evidence and OSINT in Investigation of War Crimes at the Internet Governance Forum in Kyoto
- Ukraine and Denmark Deepen Cooperation Against Cyberattacks, Award Ceremony Held for Danish Embassy Representative
- ENISA and Ukrainian Counterparts Sign Working Arrangement to Strengthen Cyber Resilience and Cooperation
- SSSCIP signs a Memorandum of Understanding on Cybersecurity with the Information Technology and Cyber Security Service (STISC) of the Republic of Moldova
- Cisco Provides Custom-built Equipment to Ukraine to Counter Russian GPS Interference
- SSSCIP and German Partners Strengthen Partnerships in Cybersecurity
- EU and US Sign Working Arrangement to Strengthen Cybersecurity Cooperation
- Ukraine's Allies Initiate Tallinn Mechanism to Bolster Cyber Assistance
- Ukraine is Strengthening Cooperation with Czech Partners Within the Framework of a Joint Cybersecurity Forum

INCIDENTS

Millions of Hryvnias at Risk: CERT-UA Detected at Least Four Waves of Cyberattacks Against Accountants in October

Cybersecurity experts at CERT-UA have recently uncovered a series of cyberattacks conducted by the notorious UAC-0006 hacking group. According to their findings, the group launched several waves of attacks between October 2 and 6, 2023, using the SmokeLoader malware. The hackers sent out emails from compromised accounts, using various methods to deliver the virus to their targets' devices. These emails typically contained a PDF attachment, which would trigger a download of an archive upon opening. Once the malicious content was executed, the SmokeLoader malware would infect the target device. CERT-UA's specialists have traced the malware control server to a technical site in Saint Petersburg operated by Trader Soft LLC. The UAC-0006 threat actor group has a history of targeting accounting officers' devices, stealing authentication data, and creating unauthorized transactions. In fact, the group made multiple attempts to steal tens of millions of hryvnias between August and September 2023. According to CERT-UA, the UAC-0006 group was observed as active from 2013 until July 2021 and was primarily motivated by financial gain. However, they resumed their activities in May 2023, with the October attacks being the latest in their ongoing campaign. To protect corporate networks against financial cybercrimes, CERT-UA researchers recommend applying reliable security software, restricting the launch of wscript.exe, cscript.exe, powershell.exe, mshta.exe, and similar tools, along with filtering outbound information flows.

Ukraine, Israel, and South Korea Top the List of Most-targeted Countries for Cyberattacks

On October 6th, Microsoft released the Digital Defense Report 2023, which revealed a staggering number of cyberattacks across the globe in the past year. More than 120 countries have fallen victim to these attacks, with Ukraine, Israel, South Korea, and Taiwan being the most targeted nations.

The report, which tracked cybersecurity trends from July 2022 to June 2023, detailed nation-state attacks by Russia, China, Iran, North Korea, Palestinian threat actors, and mercenary groups. The attacks ranged from espionage to information theft and disinformation campaigns. The report highlighted that while destructive attacks like ransomware often make headlines, the primary objectives for these attacks have shifted towards stealing information, monitoring communications, and manipulating information.

The report provided insights into the evolving strategies of nation-state actors. Russia continued cyberattacks on Ukraine but increasingly focused on espionage. China maintained its prolific espionage and data theft campaigns while developing destructive capabilities. Iran improved its cyber capabilities and engaged in more destructive attacks, expanding its disinformation networks. North Korea continued stealing cryptocurrency and evolved its attack methods, even targeting allies like Russia.

Despite the dispiriting scale of threats outlined in the report, Microsoft emphasized the progress made in technology and partnerships to combat these attackers. It also highlighted the importance of safeguarding elections and strengthening democratic institutions, especially with 2024 being a significant election year worldwide. The report raised concerns about vulnerabilities in operational technology (OT) and the widespread use of spyware and digital forensics technology by governments.

The findings underscore the ongoing challenges in the ever-evolving landscape of cybersecurity. As the report highlights, the threat landscape is constantly changing, and it is vital to be aware of the evolving strategies of nation-state actors and other cyber criminals to stay protected.

Sandworm Wages Cyberattacks Against Ukrainian Telecomms Providers

On October 16, a report was released by CERT-UA revealing a disturbing, months-long series of cyberattacks on Ukrainian telecommunication providers. The destructive attacks, attributed to a group assigned the codename UAC-1065, were carried out by an organized cybercriminal group, which had been actively tracking at least 11 service providers from May 11 to September 29, 2023. The attacks resulted in significant disruptions to services provided to customers across the country.

CERT-UA specialists and security professionals from compromised telecom providers collaborated to identify the common attacker tactics, techniques, and procedures (TTPs), and investigate the offensive intentions. Their findings revealed a malicious intent to deliver cyber threats to a number of similar companies and the findings warned industry peers of the long-running reconnaissance and exploitation campaign. CERT-UA has attributes UAC-1065 as an affiliate of the Sandworm Advanced Persistent Threat (APT) group. The Sandworm criminal group operates under the control of Unit 74455 of the Russian GRU's Main Center for Special Technologies. The situation serves as a reminder of the increasingly complex and evolving nature of cybercrime and the need for continued vigilance and preparedness in the face of such threats. CERT-UA published Indicators of Compromise for these attacks and recommends security professionals to read the article "How to be responsible and hold the cyber front."

Russian Hackers Used OT Attack to Disrupt Power in Ukraine Amid Mass Missile Strikes

On November 9, Mandiant's threat hunters uncovered two previously undisclosed operational technology (OT) attacks orchestrated by Russia's Sandworm APT in October of the previous year. These attacks, lasting several months, led to an unplanned power outage and coincided with mass missile strikes on critical infrastructure in Ukraine. The attackers utilized a novel technique to impact industrial control systems (ICS) and OT, caught executing code within an end-of-life MicroSCADA control system. Sandworm's use of "living off the land" (LotL) techniques in the OT environment is highlighted as a significant shift in attack techniques, demonstrating the rapid evolution of Russia's cyber-physical attack capabilities.

The attacks targeted MicroSCADA, a Hitachi Energy product deployed in over 10,000 substations worldwide. Sandworm's initial access to the organization's systems in June 2022 involved deploying a webshell on an internet-exposed system. The attackers then deployed an ISO image file as a virtual CD-ROM in a hypervisor, containing files that executed a legitimate MicroSCADA utility, 'scilc.exe,' enabling arbitrary commands. Mandiant suggests that the threat actor had access to the Supervisory Control and Data Acquisition (SCADA) system for up to three months, showcasing the threat actor's ability to quickly develop and deploy capabilities against different OT systems from various manufacturers. SCADA systems are used for controlling, monitoring, and analyzing industrial devices and processes. SCADA consists of both software and hardware components and enables remote and on-site control of industrial processes, direct interaction with sensors, valves, motors, and other components, as well as gathering of data from the industrial equipment.

The Mandiant team warns of the growing maturity of Russia's offensive OT arsenal, emphasizing the need for OT asset owners to take action to mitigate this evolving threat. Sandworm's use of Living off the Land binary (LotLBin) in disrupting an OT environment signifies a significant shift in techniques, raising concerns among defenders at critical infrastructure installations. The security firm provides a range of detections, hunting and hardening guidance, and MITRE ATT&CK mappings in its report, urging vigilance and proactive measures against this emerging class of OT attacks.

Hackers Disguise Themselves as State Security Service

On November 13th, CERT-UA reported that it uncovered a malicious email campaign by hackers disguising themselves as the Security Service of Ukraine (SSU). This campaign involves mass emails containing a password-protected RAR archive named "Electronic request from the SSU of Ukraine.rar", which houses another archive with the same name, containing yet another password-protected RAR file named "SSU Request 543 of 11/13/2023.pdf.rar". The final archive includes an executable file titled "SBU requirement 543 dated 11/13/2023.pdf.exe", which, when run, installs a remote administration tool called Remcos RAT on the victim's computer.Further investigation by CERT-UA revealed that the configuration file of this malware contains eight IPs of management servers that are currently functioning under the technical framework of Shinjiru Technology Sdn Bhd in Malaysia. The domain names associated with the malware were registered via the cybercrime-tolerant Russian company REG.RU, on November 11, 2023. This discovery raises serious concerns about the prevalence of cybercrime and highlights the need for heightened vigilance, ensuring all incoming email comes from a legitimate source.

CISA's Goldstein: Ukrainian Response to Viasat Hack Proves Need for Redundancy, Resilience

Top U.S. government cybersecurity officials have warned that cyber threats to space infrastructure are evolving beyond nation-state actors and extending into the criminal realm. Speaking at the Aspen Cyber Summit in New York, on November 15, Eric Goldstein and Jack Weinstein discussed the critical importance of redundancy and resilience in space technology and organizations. They highlighted the impact of the Russian military's cyberattack on satellite internet provider Viasat, which left its KA-SAT modems inoperable in Ukraine and affected various European sectors. Despite the consequences, the Ukrainian military demonstrated resilience by quickly adapting and maintaining operational capability. The officials emphasized the need for increased awareness about cybersecurity threats facing space technology and ongoing efforts by the U.S. Space Force to enhance resilience. The discussion also called for formally designating space as a critical infrastructure sector, with increased protection against cyber threats to satellites and space systems.

Kyivstar, Ukraine's Largest Telecom Operator, Hit by Massive Cyberattack Causing Network Disruptions

Ukraine's largest telecommunications operator, Kyivstar, suffered a massive cyberattack on December 12, disrupting cell service and internet access for millions of its customers. The company's subscribers started reporting network and internet outages in the early hours of the day. Kyivstar reported CEO, Oleksandr Komarov stated that the objective of the attack appears to have been to destroy network infrastructure and no ransom was sought. As of 13 December, Kyivstar maintained that its investigation had shown personal data of subscribers had not been compromised. Sources within Kyivstar told local media outlets that hackers breached a part of the operator's internal systems. According to Illia Vitiuk, head of the Security Service of Ukraine's (SBU) cybersecurity department, Russian hackers were inside Ukrainian telecoms giant Kyivstar's system from at least May 2023, causing a "disastrous" destruction and aiming to land a psychological blow and gather intelligence. The company is reportedly working to launch duplicate systems to mitigate the impact of the attack. In a news release, Kyivstar's parent company, the Netherlands-based VEON, confirmed that the incident was a "hacker attack." The decision to completely shut down the Kyivstar system was made by the operator and security forces to contain the attack's impact, one of the sources said. Containment and eradication efforts proceeded throughout December under difficult conditions with the participation of the Kyivstar IT and IS teams along with law enforcement and CERT-UA specialists. Full restoration of the Kyivstar network may take some time as containment and eradication steps necessarily require significant effort, given the severity of the damage and the complexity of the attack.

Russian actors from the so-called Solntsepek group claimed responsibility on a Telegram channel for the cyberattack on the Ukrainian mobile operator. The group's activities are believed to be linked to Sandworm, a Russian cybercriminal group operating under the GRU. Sandworm's NotPetya virus campaign caused $10 billion in global losses from a single act of sabotage.

PUBLIC SECTOR DEVELOPMENTS

USAID-supported Tabletop Exercise CIREX.CoBridge Helps Strengthen Ukraine's Critical Infrastructure Resilience

On October 20th, SSSCIP in collaboration with the USAID Cybersecurity Activity conducted a large-scale drill in CIREX.CoBridge format. The drill brought together central authorities, law enforcement, and critical infrastructure sectors to practice preventing hostile attacks on major transport infrastructure. Participants practiced various scenarios and improved information exchange and coordination during such an attack. The drill aimed to enhance the capabilities of key players in Ukraine's critical infrastructure to respond to any potential attacks.

"Critical infrastructure protection is our common mission. Such drills are an important opportunity for officers from various agencies, institutions, and companies to test their capacity to address threats and respond to both physical and cyber-based enemy attacks using specific example cases. They let us identify weaknesses in our defenses, fill the gaps, and avoid mistakes in real-life situations," says Oleksandr Potii, the SSSCIP Deputy Head.

The training was developed based on guidelines provided by the US Cybersecurity and Infrastructure Security Agency (CISA). The objective of the event was to implement the National Plan for Critical Infrastructure Protection and Resilience, which was approved by the Cabinet of Ministers of Ukraine.

USAID Supports Regional Cybersecurity Contest in Kharkiv

On October 21, the USAID Cybersecurity Activity, with the Kharkiv National University of Radio Electronics educational cyber laboratory, organized a regional online competition – a 12-hour 'Capture-the-Flag' (CTF) event for cybersecurity students. Forty-seven participants from seven universities representing Ukraine's eastern regions gained valuable hands-on experience and the opportunity to tackle real-world cybersecurity challenges. The Activity developed dedicated tasks for the CTF platform to simulate the most common cyberthreats to hone student skills in responding to real-life cyberattacks.

USAID Supports Tabletop Exercise Facilitator Training for SSSCIP Staff

On November 14-16, 2023, the USAID Cybersecurity Activity supported a Tabletop Exercise (TTX) Facilitator training for 10 staff of the State Service for Special Communications and Information Protection of Ukraine (SSSCIP). The training, developed and delivered by the U.S. Cybersecurity and Infrastructure Security Agency (CISA), was held in Krakow, Poland, and focused on TTX Design and Development, Facilitation Practice and Evaluation. USAID is proud to facilitate cooperation between the key US and Ukrainian cybersecurity agencies ensuring that SSSCIP is well equipped to counter current and future cyberthreats.

USAID Restores and Enhances Digital Infrastructure at 25 Ukrainian Universities

On November 22, 2023, the Ministry of Education and Science officially inaugurated two state-of-the-art cybersecurity laboratories at Kyiv National University of Construction and Architecture (KNUCA) and Mariupol State University (hosted by KNUCA since March 2022 due to the war) for which the USAID Cybersecurity Activity provided equipment and software. As Ukraine returns to a standard offline academic experience, in the fall of 2023 the USAID Cybersecurity Activity delivered 5,000 pieces of hardware and more than 4,000 licenses to 25 Ukrainian higher education institutions, amounting to a total value of $2.5 million. This assistance addresses the needs of nearly 50% of institutions offering cybersecurity education in Ukraine, with a goal of restoring the digital infrastructure of those affected by physical damage, relocation, or those hosting displaced universities.

SSSCIP Leadership Undergoes Changes

On November 20, 2023, the Cabinet of Ministers of Ukraine dismissed Yurii Shchyhol from the position of SSSCIP Head. With the same decree, CMU also dismissed Viktor Zhora from the position of SSSCIP Deputy Head. At a CMU meeting on December 1, the Government appointed Yurii Myronenko as the new Head of SSSCIP. Myronenko is reported to have extensive corporate management experience and served in the military prior to his appointment to lead SSSCIP. On December 5, the CMU also dismissed Dmytro Makovskyi from the position of SSSCIP First Deputy Head, replacing him with Oleksandr Semyrha.

USAID Advances Cybersecurity Workforce Development Agenda to the Next Level

On November 16, 2023, the USAID Cybersecurity Activity organized a National Cybersecurity Workforce Development Workshop facilitated by MITRE Corporation. Forty-three representatives from government, academia, and business worked together to build an ecosystem-wide commitment to skills-based training through the deployment of international best practices and shifting workforce development towards generating the specific skillsets needed for specific jobs. The workshop participants developed a joint action plan summarizing the ideas brainstormed on how to advance the cybersecurity workforce development agenda to the next level to increase the availability of skilled cyber professionals in Ukraine. The Activity will facilitate collaboration with cross-sectoral stakeholders to implement the identified initiatives, ensuring the sustainable short- and long-term development of National Cybersecurity Workforce Development in Ukraine.

USAID Contributes to Unlocking Ukraine's Innovative Potential and Supports Cybersecurity Efforts

On December 14, 2023, the USAID Cybersecurity Activity, in close cooperation with the Ministry of Digital Transformation (MDT), conducted an Innovations Summit, attracting over 210 representatives from government institutions, the donor community, private sector and think tanks. During the event, Mykhailo Fedorov, Deputy Prime Minister for Innovation, Education, Science & Technology/Minister of Digital Transformation, presented the GOU's National Innovations Strategy and Innovations brand, supported by the USAID Cybersecurity Activity. The Strategy delineates the vision for Ukraine's innovation ecosystem and identifies priority sectors crucial for the country from both a domestic and foreign perspective. The Strategy covers 13 areas, one of which is cybersecurity. It establishes a robust foundation for maintaining a cybersecurity agenda at the national level and adopts a comprehensive approach to address Ukraine's specific cybersecurity needs to withstand current and future cyber threats.

The National Innovations Strategy is available for public comment at https://winwin.gov.ua/.

USAID Facilitated Adoption of New Cybersecurity Professional Standards in Ukraine

On December 21 and December 27, 2023, the National Qualification Agency approved 15 new cybersecurity professional standards, marking the culmination of a 12-month effort by the USAID Cybersecurity Activity in support of SSSCIP, the country's national special communications and information protection service. USAID support centered around the development, collection of cyber community feedback and adoption of the second batch of standards within the Ukrainian National Cybersecurity Workforce Framework.

Established by SSSCIP in 2022, the Ukrainian Cybersecurity Workforce Framework now includes 21 cybersecurity professional standards. This framework serves as the baseline requirement for cyber specialists and guides the development of educational curricula to address broader cyber skills and competencies. The professional standards are modeled after the U.S. National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework, fostering a mutual understanding of the qualifications required for cyber professionals among employees and employers.

LEGAL DEVELOPMENTS

UN Member States Reform Cybercrime Legislation, Paving the Way for Comprehensive International Convention

According to the Cybercrime Programme Office of the Council of Europe, an updated December 2023 report on the Global State of Cybercrime Legislation reveals that a vast majority of UN Member States are reforming their legislation on cybercrime and electronic evidence. The report states that by mid-December 2023, as many as 95% of the UN Member States will have taken steps towards this reform. Out of these, 131 States (or 68% of UN Member States) have already criminalized offenses against and by means of computers in line with the Convention on Cybercrime. Additionally, 99 States (or 51%) have also granted their criminal justice authorities specific procedural powers to investigate cybercrime and secure electronic evidence.

The report highlights that these figures represent a significant increase of almost 100% over the last ten years since 2013, when the first survey of this kind was carried out. These findings hold great significance for the current negotiation of the "Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes" by the United Nations.

EU Set to Adopt Cyber Resilience Act to Improve Digital Product Security

The Cyber Resilience Act (CRA) is a forthcoming legislation in EU that aims to enhance the security of digital products. This legislation is now one step away from being officially adopted, after days of debate within EU institutions. On December 3, the European Parliament and the EU Council reached a political agreement on the CRA. The EU Commission first proposed this legislation in September 2022, with an objective to introduce security requirements for connected device manufacturers within the Union. This first-of-its-kind legislation in the world is set to improve the level of cybersecurity of digital products and benefit consumers and businesses across the EU. The Act introduces mandatory cybersecurity requirements for all hardware and software, with different security requirements for products with varying levels of risk. Notably, less than 10% of products will be subject to third-party assessments.

The Cyber Resilience Act is an important step in combating the growing threat from cyber criminals and other malicious actors. Under the new regulation, all products put on the EU market must be cyber secure. Manufacturers of hardware and software will have to implement cybersecurity measures across the entire lifecycle of the product, from design and development to after the product is placed on the market. Software and hardware products will bear the CE marking to indicate compliance with the Regulation's requirements, and therefore, can be sold in the EU.

Additionally, the Act introduces a legal obligation for manufacturers to provide consumers with timely security updates for several years after purchase, reflecting the length of time products are expected to be used. These measures will empower users to make better-informed and more secure choices, as manufacturers will have to become more transparent and responsible about the security of their products.

The agreement reached is subject to formal approval by both the European Parliament and the Council. Once adopted, the Cyber Resilience Act will take effect on the 20th day following its publication in the Official Journal. Manufacturers, importers, and distributors of hardware and software products will have 36 months to adapt to the new requirements, except for a more limited 21-month grace period in relation to the reporting obligation of manufacturers for incidents and vulnerabilities.

Ukraine's AI Road map Seeks to Balance Innovation and Security

Ukraine has unveiled a national road map for the regulation of Artificial Intelligence (AI) that emphasizes the delicate balance between innovation and security. Recognizing the global race to integrate AI into various sectors, the country seeks to foster growth in its vibrant tech industry, home to over 60 active AI-focused companies. The Ukrainian approach prioritizes a soft, bottom-up regulatory strategy over immediate intervention, focusing on aiding businesses in developing self-regulation practices during an initial two to three-year phase. This phase involves providing practical tools, expert assistance, and voluntary codes of conduct to ensure ethical AI development and usage, with an ultimate goal of aligning Ukrainian regulations with the European Union's AI Act.

The Ukrainian government's current role is not to enforce AI regulations but to prepare businesses for inevitable future regulations, prioritizing business responsibility and fostering an open dialogue. The intention is to transition smoothly into a comprehensive national AI legislation aligned with EU standards, promoting both innovation and adherence to human rights. The strategy aims to create a business-friendly environment that facilitates Ukrainian tech companies' entry into European markets, ensuring that the regulation of AI contributes to safe innovation while minimizing potential risks and abuses. This approach underscores the global nature of AI regulation, emphasizing the need for the right environment to harness the transformative power of this technology responsibly.

PRIVATE SECTOR DEVELOPMENTS AND PARTNERSHIPS

SSSCIP Takes Steps to Build HR Capacity in Information Security and Cybersecurity

The field of cybersecurity is rapidly evolving, and the need for skilled professionals has never been greater. In Ukraine, SSSCIP is taking steps to build HR capacity in information security and cybersecurity while reforming the professional training system. On October 3, the Organization of Cybersecurity HRs and Recruiters NGO, in collaboration with the SSSCIP, organized an event called "Professions and Careers in Cybersecurity 2.0." The event brought together cybersecurity professionals and industry experts to discuss job market trends, the latest changes in the field, and future reform plans.

According to Oleksandr Yudin, Academic Secretary of the SSSCIP's State Scientific and Research Institute for Cybersecurity and Information Protection, the ongoing reform incorporates the most advanced global approaches. Ukraine already has the necessary legal framework in place, with new occupations in cybersecurity and IT security added to the National Occupational Classifier for the first time in years.

In 2022, six initial professional standards in the cybersecurity industry were designed and adopted with the support of the USAID Cybersecurity for Critical Infrastructure in Ukraine Activity. Some higher education institutions have already adapted their curricula to align with these new standards, with another 15 such new standards adopted by Ukraine in December. Additionally, SSSCIP, with the support of the USAID Cybersecurity Activity, is in the process of creating Ukraine's first Qualification Center to enable specialists to verify their knowledge, skills, and competencies. The center will soon open its doors, utilizing the latest technological solutions from CYBER RANGES, a skills validation platform provider in the field of cybersecurity.

"The occupational qualification system is a very acute issue. In the long run, Ukraine needs an extensive network of qualification centers to be established. It is also important for this initiative to involve not only the government, but private businesses as well. Competition contributes to sustainable development, enhancement of the centers' operation, leaving only the best ones in the market," – Oleksandr Bakalynskyi, Deputy Manager of the SSSCIP Cyber Defense Department.

Ukrainian National Coordination Center for Cybersecurity and IP3 International announce the Collective Defense Artificial Intelligence (AI) Fusion Center (CDAIC) in Ukraine

On October 24th, the Ukrainian National Coordination Center for Cybersecurity and IP3 International, an energy security developer, jointly announced the establishment of the Collective Defense AI Fusion Center (CDAIC) in Ukraine. The CDAIC aims to foster collaboration between Ukraine and its allies to enhance their collective defense mechanisms against cyber threats.

As part of the Ukraine Energy Security Fund, a project focused on energy security and infrastructure, CDAIC is a significant step towards the reconstruction of Ukraine. The center provides a platform for cybersecurity companies of Ukrainian allies to work in partnership with the Ukrainian National Cybersecurity Center and the private sector towards product innovation.

CDAIC will also offer access to cybersecurity talent by providing experienced Ukrainian cybersecurity specialists on contract work to cybersecurity companies of allies. This initiative is expected to help strengthen the cybersecurity posture of Ukraine and its allies, while also driving innovation in the cybersecurity industry.

USAID and Cisco Partner to Support Education and Cybersecurity in Ukraine

On December 5th, USAID announced the delivery of essential equipment to support education in Ukraine through a donation from Cisco. The equipment will aid in preparing the next generation of Ukrainian cybersecurity experts. The collaboration between USAID, Cisco, and the Ministry of Education and Science of Ukraine identified and addressed some of the most immediate needs for equipment and training in the country. Cisco, as part of its Country Digital Acceleration program, will provide five instructional labs at Ukrainian universities with state-of-the-art telecommunications equipment. This is a significant step towards training a new cadre of cybersecurity experts in Ukraine. Nearly 200 educational institutions have partnered with Cisco to provide digital skills training to 36,000 learners over the past academic year through the Cisco Networking Academy, which is one of the most longstanding IT skills-to-jobs programs globally. The Ministry of Education and Science of Ukraine is also working closely with Cisco to distribute wi-fi routers to 1,600 schools across the country, in addition to providing 1,000 video camera kits for teachers who are forced to teach remotely due to unsafe conditions. This collaboration is an essential step towards the development of Ukraine's digital workforce.

Recorded Future Continues to Provide Critical Intelligence to Protect Ukraine from Cyber, Physical and Kinetic Threats

Recorded Future, a leading intelligence and analytical company, has committed to supporting Ukraine in safeguarding critical infrastructure from Russian military and cyber threats in 2024, with an investment exceeding $23 million. The company has been aiding Ukraine since the onset of the full-scale invasion, offering intelligence data for infrastructure protection, aiding investigations into Russian war crimes, and providing access to the Intelligence Cloud software platform, amounting to over $20 million in support in 2023.

In the coming year, Recorded Future will collaborate with 16 Ukrainian state entities, including the Ministry of Digital Transformation, SSSCIP, Main Directorate of Intelligence of the Ministry of Defense of Ukraine (GUR), Security Service of Ukraine, Ministry of Defense, General Prosecutor's Office, and Cyber Police. The company's tools contribute to the early detection and mitigation of cyberattacks, such as the collaborative effort with CERT-UA to identify and neutralize an espionage campaign by the BlueDelta/APT28 attacker in Ukrainian government organizations. Recorded Future's ongoing commitment underscores the importance of private sector collaboration in enhancing cybersecurity for nations facing geopolitical threats.

INTERNATIONAL COOPERATION

NCCC Secretary Nataliya Tkachuk Highlights Importance of Electronic Evidence and OSINT in Investigation of War Crimes at Internet Governance Forum in Kyoto

From October 8-12, the Head of the Information and Cybersecurity Directorate at the Office of the National Security and Defense Council of Ukraine, and the Secretary of NCCC, Nataliya Tkachuk, took part in the Internet Governance Forum (IGF 2023) in Kyoto, Japan. In her speech on the topic of the role of electronic evidence and open-source intelligence in the investigation of war crimes, Nataliya Tkachuk emphasized that in addition to defeating the enemy and rebuilding Ukraine, it is important to bring to justice all Russian war criminals responsible for the crimes committed in Ukraine.

"Since the beginning of the Russian federation's aggression, Ukrainian law enforcement agencies have registered more than 100,000 war crimes. This is an incredible figure that needs to involve the entire civil society and the international community in the process of documenting them, therefore, OSINT methods and the use of electronic evidence are an important tool," - Nataliya Tkachuk, NCCC Secretary and head of the NSDC Information Security and Cybersecurity Service.

The NCCC secretary pointed out that while discussing threats related to the development of the Internet, such as cyberattacks and disinformation, we should remember that it was Russia who first began to use the Internet and social networks for malicious purposes. In particular, manipulation and propaganda, interference in elections in democratic countries, and the use of cyberattacks as a tool for information operations.

During the event, the Secretary of NCCC conducted a series of working meetings with Japanese and US partners to discuss potential areas of collaboration in the field of cybersecurity. Nataliya Tkachuk expressed her gratitude to the partners for their support in enhancing the capabilities of the National Cybersecurity System of Ukraine. She also thanked them for assisting NCCC in organizing successful events under the NSDC of Ukraine.

Ukraine and Denmark Deepen Cooperation Against Cyberattacks, Award Ceremony Held for Danish Embassy Representative

On November 3, 2023, Serhii Prokopenko, the Head of NCCC Operations Department – Deputy Head of Information Security and Cybersecurity Directorate at the Office of the National Security and Defense Council of Ukraine, met with representatives of the Embassy of Denmark in Ukraine. They discussed ways of deepening practical cooperation in the field of countering cyberattacks, information exchange, and further partnership in educational projects.

"No country can face modern cybersecurity challenges on its own. Our country has a unique experience in countering Russian aggression in cyberspace, which we are ready to share with partner countries. After all, thanks to joint work and information exchange, we will be able to provide security and resilience in cyberspace not only for Ukraine but also for Europe," said Serhii Prokopenko.

Deputy Defense Attaché at the Embassy of Denmark in Ukraine Jakob Torrild Hansen was awarded by the NSDC of Ukraine for his contribution to the national security and defense of Ukraine, effective cooperation with the NSDC of Ukraine and the National Coordination Center for Cybersecurity.

Serhii Prokopenko thanked the Kingdom of Denmark for its comprehensive support of Ukraine and contribution to strengthening the National Cybersecurity System of Ukraine.

ENISA and Ukrainian Counterparts Sign Working Arrangement to Strengthen Cyber Resilience and Cooperation

On November 13, The European Union Agency for Cybersecurity (ENISA) signed a Working Arrangement with Ukrainian counterparts, aimed at boosting capacity-building, exchanging best practices, and enhancing situational awareness. In the wake of the Russian invasion of Ukraine, which has been a major turning point for the global cyber domain, the need for greater international cooperation has been confirmed. The Working Arrangement builds on the discussion that was initiated last year in Warsaw, during the EU-Ukraine Cybersecurity Dialogue. This partnership was signed by ENISA, the NCCC, and SSSCIP on the Ukrainian side.

The new Working Arrangement aims to establish short-term cooperation on enhancing cyber resilience, including cyber awareness and capacity building, best practice exchange, and knowledge sharing. This agreement will pave the way for longer-term alignment of policies and implementation approaches. The cooperation will focus on key areas such as telecommunications, energy, and sharing cyber awareness tools, programs, and exercises. The ultimate goal is to increase common situational awareness and ensure alignment of legislation and implementation.

SSSCIP signs a Memorandum of Understanding on Cybersecurity with the Information Technology and Cyber Security Service (STISC) of the Republic of Moldova

On November 15, SSSCIP signed a Memorandum of Understanding on Cybersecurity with the Information Technology and Cyber Security Service (STISC) of the Republic of Moldova. The agreement was signed in a bid to foster cooperation between the two countries in the area of cybersecurity. Under the Memorandum, both parties have agreed to establish bilateral information exchange channels between CERT-UA and the CERT-GOV-MD Cybersecurity Center, to identify and respond to threats in cyberspace. The agreement also facilitates the exchange of information on cyber incidents, cyberattacks, and cyberthreats, including through the use of MISP.CERT.GOV.UA platform. The Memorandum further provides for notifications on cyber incidents, including information security breach attempts, consulting and information assistance in exploring cyber incidents and mitigating their impact. Additionally, both parties have agreed to exchange experience and best practices in cyber defense. This agreement is expected to strengthen the cybersecurity posture of both countries and enhance their collaboration in the fight against cyber threats.

“Cooperation in cybersecurity is among the decisive factors ensuring each country’s cyber resilience. Both joint effort of private and public sectors within each country and enhanced international cooperation are essential to confront cyber threats efficiently. Having reliable partners willing to help us address cyberspace-based challenges, with whom we can share our experience of countering Russia’s cyber aggression, is very important for us,” said Yulia Volkova, Director of the SSSCIP Department for International Cooperation and European Integration.

Cisco Provides Custom-built Equipment to Ukraine to Counter Russian GPS Interference

On November 21st, CNN broke a story revealing that Ukraine’s power grid operator, Ukrenergo, has received custom-built equipment from US tech giant Cisco to counter Russian interference with GPS systems. The equipment, which allows communication between electric substations even when GPS systems are compromised, was developed and tested by Cisco engineers with assistance from US officials, before being shipped to Ukraine with the help of a US Air Force plane carrying humanitarian aid. The move is part of the Biden administration’s strategy to support Ukraine’s defense efforts without direct confrontation with Russia, with various US companies, including SpaceX and Microsoft, also involved in the effort. The custom-built equipment addresses a specific challenge caused by Russian radio-jammers disrupting GPS systems, the function of which is critical for Ukrenergo to manage power flow.

SSSCIP and German Partners Strengthen Partnerships in Cybersecurity

The Cybersecurity Training Program for Public Sector Specialists is an initiative supported by the Government of Germany and implemented by the Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH. It aims to foster professionals in Ukraine in line with European cybersecurity standards and requirements to enhance global cybersecurity. Three pilot trainings have already been held online, and a study trip for trainees to Bonn, Germany, has been concluded. The trip involved offline workshops on cybersecurity and skill-boosting, with inputs from the German Federal Foreign Office, the Federal Office for Information Security (BSI), representatives from European institutions, and other relevant stakeholders.

"Ukraine has unique experience contributing to better cybersecurity for our partners. Our country has been reinforcing its cyber resilience over the past few years, having become a center for cybersecurity innovations. We seek to provide a robust protection to our information resources as well as to enhance cyber defense at government institutions by training public officials and building HR capacity," – SSSCIP Deputy Head Oleksandr Potii.

The project's next phase will launch in 2024 and include scaled-up trainings based on lessons from the pilot phase in November. The project aims to build a sustainable, open, and secure cyber environment among European partners and Ukraine, while also promoting EU accession and building HR capacity in cybersecurity. Yvonne Miriam Sabin from the German Federal Foreign Office emphasized the importance of cybersecurity in protecting sensitive information and critical infrastructure.

EU and US Sign Working Arrangement to Strengthen Cybersecurity Cooperation

The ever-evolving cyber threat landscape has been shaped by geopolitics, leading to the formation of alliances among nations to combat common challenges and technological advancements. The European Union Agency for Cybersecurity (ENISA) and the Cybersecurity and Infrastructure Security Agency (CISA) of the United States announced the signing of their Working Arrangement at the EU-US Cyber Dialogue on December 7th. This agreement marks a significant milestone in the collaboration between the US and the EU in the field of cybersecurity, following the Joint Statement of European Commissioner Thierry Breton and U.S. Secretary for Homeland Security Alejandro Mayorkas of January 2023.

According to ENISA's International Strategy, the Agency aims to selectively engage with international partners and limit its overall approach to those areas and activities that add high and measurable value to achieving its strategic objectives. CISA is a crucial partner in fulfilling these objectives and ultimately achieving a higher level of cybersecurity within the EU. The Working Arrangement consolidates present areas of cooperation and opens doors to new ones, such as exchanging best practices in incident reporting, organizing and promoting the International Cybersecurity Challenge (ICC), and exchanging ad hoc information on basic cyber threats.

Ukraine's Allies Initiate Tallinn Mechanism to Bolster Cyber Assistance

On December 20th, a coalition of almost a dozen international partners launched a new initiative called the Tallinn Mechanism to provide cyber support for Ukraine in the coming years. The mechanism, named after the Estonian capital where the plan was formulated in May, aims to coordinate and facilitate civilian cyber capacity building to help Ukraine defend itself in cyberspace and address longer-term cyber resilience needs.

Canada, Denmark, France, Germany, the Netherlands, Poland, Sweden, Ukraine, as well as the United Kingdom and the United States have all pledged to participate. The initiative was launched just days after British military intelligence described a cyberattack on Ukraine's Kyivstar as "one of the highest-impact disruptive cyberattacks" since the invasion began.

According to the announcement made on the Estonian Ministry of Foreign Affairs' website, the coalition has warned that "it is likely that Russia's cyberattacks will continue for the foreseeable future." The Tallinn Mechanism is expected to address the ad hoc basis on which states have provided assistance to Ukraine historically. It involves technology companies and non-governmental organizations, as well as regular engagement with the European Union and NATO.

The announcement acknowledges that "the ongoing destruction of Ukraine's critical infrastructure and the disruption of essential services caused by Russian cyber operations will require substantial multi-year assistance for Ukraine to maintain and strengthen its cybersecurity and cyber resilience capabilities." It also warns that "Russian cyber operations and cyber activity are expected to continue well beyond any formal cessation of hostilities."

Ukraine is Strengthening Cooperation with Czech Partners Within the Framework of a Joint Cybersecurity Forum

On December 27th, Ukraine intensified collaboration with Czech partners in a joint cybersecurity forum, emphasizing the importance of democratic nations uniting against cyber threats, particularly those originating from Russia. The forum in Brno focused on sharing experiences, with Ukrainian cybersecurity experts detailing responses to attacks and incidents. The event highlighted the need for cooperation between Czech and Ukrainian businesses, discussed joint scientific research in cybersecurity, and addressed Ukraine's cybersecurity requirements and potential Czech assistance.

The forum also showcased the activities of the CyberSecurity Hub and explored the operations of the Czech Cyber Range Platform (KYPO CRP), offering valuable insights for the training and development of Ukrainian cybersecurity professionals. Organized with the support of the Czech government and the "Smart Industries" project led by CzechInno, the Czech-Ukrainian Cybersecurity Forum aimed to strengthen collaboration and enhance cybersecurity resilience.