USAID
FROM THE AMERICAN PEOPLE

USAID CYBERSECURITY FOR CRITICAL INFRASTRUCTURE IN UKRAINE

Cyber Sector Update

APR 2023 – JUNE 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

- Cybercriminals launch another attack campaign using bill-related mails
- Cyber espionage activities detected against organizations in Ukraine — CERT-UA investigation
- Russian hackers ramp up hunt for PII
- Cybercriminals attempt to attack Ukrainian governmental agencies with fake OS updates
- SSU blocks a bot farm in Kropyvnytskyi that created over 3,000 fake accounts for information sabotage attacks against Ukraine

PUBLIC SECTOR DEVELOPMENTS

- Ukraine officially joins NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE)
- The Government adopts a resolution on the use of the Platform for the rapid creation and management of state registers
- USAID-provided analytical tools enhance NCCC's analytical capabilities
- SSSCIP invites businesses and professional associations to submit proposals for expanding the cybersecurity occupation classification
- SSSCIP holds the second All-Ukrainian Competition in Cybersecurity UA30CTF

LEGAL DEVELOPMENTS

- Harmonizing critical infrastructure cybersecurity systems with EU standards at a meeting of the National Cybersecurity Cluster in Warsaw
- The Cabinet of Ministers approves a Resolution for responding to cyber incidents and cyber attacks
- Ukraine's Cabinet of Ministers passes a Resolution for maintaining the Critical Infrastructure Facilities Registry
- Government enacts a Resolution on strengthening the protection of national electronic information resources

PRIVATE SECTOR DEVELOPMENTS

- Google launches the online game Interland: Child Safety on the Internet in Ukraine
- Defense tech cluster BRAVE1 launched in Ukraine to stimulate development of military innovations and defense technologies
- NCCC deepens cooperation with Recorded Future, a U.S.-based cyber threat intelligence company
- USAID launches grant program for cybersecurity players
- SSSCIP conducts the first table-top Critical Infrastructure Resilience Exercise (CIREX), based on CISA scenarios
- NCCC conducts Vulnerability Management training for cybersecurity specialists in Ukraine's energy sector
- USAID facilitates the discussion of Ukraine's cybersecurity market at the 6th Cybersecurity Dialogue
- SSSCIP and CYBER RANGES sign a memorandum of cooperation for cyber education and professional development in cyber defense

INTERNATIONAL COOPERATION

- Romanian technical delegation on cybersecurity visited SSSCIP
- USAID delivers international experience to finalize Ukraine's Cyber Incident Response Plan
- OSCE assists Ukrainian law enforcement in investigating cybercrimes
- Ukraine and the United States hold an annual discussion on cyber policy issues
- Cyber Defense Influencers Meet in Tallin for the Cycon 2023 15th International Conference
- Ministry of Digital Transformation of Ukraine, SSSCIP and the Ministry of Digitalization of Japan sign a memorandum of cooperation

INCIDENTS

Cybercriminals launch another attack campaign using bill-related e-mails

Cybercriminals sent harmful emails with ZIP or RAR archives that contained SmokeLoader malware. These emails appear to originate from legitimate email addresses that have been compromised. The Computer Emergency Response Team of Ukraine (CERT-UA) has observed that the attackers, identified as the UAC-0006 hacking collective, have changed their tactics. They are now using multiple infection chains and disseminating SmokeLoader copies, including 26 URL addresses for the bot network control server. Most of the domains used are unregistered. Furthermore, detecting the use of Cobalt Strike Beacon malware suggests that the group has expanded its toolkit. The individuals responsible for the attacks utilize Russian domain registrars and service providers, including @reg.ru, @nic.ru, @iqhost.ru, @macloud.ru, and @cloudx.ru, to register domain names and host the servers that control the bot network. This is a critical component of their scheme. According to CERT-UA, the group UAC-0006 was active from 2013 until July 2021, mainly driven by financial gain. Their activities seemed to have resumed in May 2023, indicating a sort of "revival" for the group

Cyber espionage activities detected against organizations in Ukraine — CERT-UA investigation

The CERT-UA experts have acted swiftly to detect and respond to a cyberattack that targeted a Ukrainian public agency's information and communication system. The agency received a series of harmful emails on April 18, 20 of which were from the official email account of the Tajikistan Embassy in Ukraine, which was apparently compromised. One of the emails had an attached document with a macro, while another contained a link to the same document. Downloading the document and activating the malicious macro could result in installing spyware on the affected devices, among other things, such as LOGPIE keylogger (records and saves keystroke values and clipboard contents to a log file); CHERRYSPY backdoor (executes a Python code received from the management server). This event is being monitored as linked to the activity of threat actor UAC-0063 and categorized as a cyber-espionage threat.

Russian hackers ramp up hunt for people's personal data

According to CERT-UA, there has been a surge in cyberattacks targeting commercial companies in April, especially those that store a large amount of Personal Identifiable Information (PII) belonging to citizens. A group of Russian "hacktivists" conducted several cyberattacks last month, successfully hacking into the databases of four of Ukraine's top 10 insurance companies. The hackers managed to obtain and publicly disclose the personal data of Ukrainians, such as contact information, addresses, employment history, travel records, medical information, and more.

Cybercriminals attempt to attack Ukrainian governmental agencies with fake OS updates

CERT-UA has issued a warning regarding a potential cyberattack through emails containing deceptive instructions disguised as Operating System (OS) updates. There have been reports of emails with the subject line "Windows Update" being sent by individuals who claim to be system administrators from public domain email addresses, such as "@outlooc.com." These emails may even use the names or initials of real employees in their formatting.

In a common email used for the attack, instructions are written in Ukrainian about updating the system to prevent hacking attacks. Additionally, images demonstrate how to launch a command line and execute a PowerShell command. The process imitates the OS update process while downloading and running a PowerShell scenario for collecting the basic PC data and sending the retrieved data to the Mocky API service. This activity is attributed to the APT28 group (also known as Fancy Bear, Pawn Storm, and Forest Blizzard), associated by many researchers with Russia's military intelligence service.

"The world requires efficient methods of combating government-sponsored cyber terrorism. Such combating should be global-scale and collective", - *SSSCIP Deputy Head Viktor Zhora*

SSU blocks a bot farm in Kropyvnytskyi that created over 3000 fake accounts for information sabotage attacks against Ukraine

Security Service of Ukraine (SSU) cyber specialists neutralized a bot farm based in Kropyvnytskyi that promoted pro- Russian narratives. Kropyvnytskyi is a city in central Ukraine in the Kirovohrad Oblast. Investigative efforts resulted in detaining the person responsible for organizing the hostile activities. The suspect created numerous anonymous social media accounts and sold them through the darknet, mainly to clients representing Russian special services. The average cost of one bot was UAH 200 ($5.40).

The SSU established that the threat actor created almost 3,000 fake accounts, which they planned to sell for over UAH 500,000 ($13,500). Their "clients" were representatives of the Russian special services and pro-Kremlin propagandists. The bots were used to disseminate false information to Ukrainian citizens about the situation at the front and to attempt to discredit the Ukrainian Defense Forces. The key aim was to destabilize the internal political situation in various regions of Ukraine during wartime.

PUBLIC SECTOR DEVELOPMENTS

Ukraine officially joins NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE)

Ukraine has officially joined the NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE), a NATO-accredited cyber security center and think tank specializing in interdisciplinary applied research, analysis, information exchange, and cyber defense training and exercises. USAID provided technical expertise to the National Security and Defense Council (NSDC) and the SSSCIP to develop this resolution that regulates Ukraine's participation in the NATO CCDCOE. Ukraine applied for membership in August 2021, received unanimous approval from the CCDCOE Steering Committee in March 2022, and marked its official accession to the CCDCOE in May 2023.

The Government adopts a resolution on the use of a platform for the rapid creation and management of state registers

Teams of the Ministry of Digital Transformation and SSSCIP work on a platform for deployment and support of state electronic registers. This tool will enable the ministries and state bodies to quickly and conveniently create and manage public registers.

USAID-provided analytical tools enhance NCCC's cybersecurity analytical capability

On June 15, 2023, USAID Cybersecurity for Critical Infrastructure in Ukraine Activity provided the National Security & Defense Council's (NSDC) National Cybersecurity Coordination Center (NCCC) with access to modern digital analytical platforms. This will allow NCCC to enhance its analytical cybersecurity capacity and significantly improve its ability to identify current and predict future cyberthreats. This will also enable NCCC to better execute its national coordinating function, thereby contributing to NSDC's fulfillment of Ukraine's 2025 Cybersecurity Strategy for implementing coordinated detection and disclosure of vulnerabilities of information and communication systems of state bodies, critical infrastructure and private sector.

SSSCIP invites businesses and professional associations to submit proposals for expanding the cybersecurity occupation classification

Reforming Ukrainian professional education in cybersecurity requires involving businesses and professional associations in developing professional cybersecurity standards. During the meeting «Professions and Careers in the Area of Cybersecurity», which took place on April 5 in Kyiv, the participants discussed these issues.

"A few years ago, there were only two [cybersecurity-related] 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," - SSSCIP Deputy Head Oleksandr Potii.

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

SSSCIP holds the second All-Ukrainian Competition in Cybersecurity UA30CTF

SSSCIP organized the All-Ukrainian Youth Competition in Cybersecurity on April 25th, using the Capture-the-Flag (CTF) format. More than 400 participants, divided into 107 teams from different parts of Ukraine, joined the competition. Each team had 12 hours to complete 25 tasks that involved searching for and exploiting vulnerabilities,

as well as solving challenging logical problems. The LunarLobsters team earned the top spot, while Knotty Kitten and Arctic Warriors claimed second and third place, respectively.

Oleksandr Potii, SSSCIP's Deputy Head remarked that: "We are happy to give the youth an opportunity to test their skills, to compete with their colleagues and build a young professional community. The number of participants has exceeded all expectations, so we'll be sure to continue the practice of holding such competitions,"

USAID launches grant program for cybersecurity players

In April 2023, the USAID Cybersecurity for Critical Infrastructure in Ukraine Activity announced a grant program to support creative and effective initiatives and solutions to strengthen Ukraine's national preparedness, cybersecurity vulnerabilities and critical infrastructure cybersecurity. The Grant program is soliciting applications from private, science, NGO, or academia players that target strengthening national cybersecurity system, building capacity of the Government of Ukraine (GOU) entities in cybersecurity, and ensuring secure operations of the operators of critical infrastructure (OCI).

The Activity will prioritize initiatives focused on:

- addressing identified gaps on the national as well as sectoral level,
- conceptualized opportunities for GOU cybersecurity stakeholders and OCIs,
- suggested capacity building programs for GOU cybersecurity stakeholders and OCIs,
- strengthening collaboration between cybersecurity stakeholders,
- adopting best international practices in cybersecurity,
- building workforce development programs in cybersecurity,
- targeted cybersecurity projects for GOU cybersecurity stakeholders and OCIs,
- feasibility studies of identified national opportunities and ad hoc surveys in cybersecurity,
- addressing skill gaps among cybersecurity professionals at GOU cybersecurity stakeholders and OCIs.

USAID delivers servers and routers to SSSCIP to strengthen the infrastructure for the government's National Telecommunication Network

On April 21 and June 16, 2023, respectively, the USAID Cybersecurity for Critical Infrastructure in Ukraine Activity transferred 72 servers and 137 routers to SSSCIP to strengthen its infrastructure. This equipment will support the government's National Telecommunication Network (NTN) to secure government IP telephony and video connections, strengthen Ukrainian government IP communications channels, and enable safe communication between civil servants while working remotely. SSSCIP will use another two powerful servers to deploy the Critical Information Infrastructure Registry in the second half of 2023. The registry will list the core IT systems of critical infrastructure operators subject to SSSCIP cyber protection monitoring. The USAID Cybersecurity for Critical Infrastructure in Ukraine Activity will continue to support SSSCIP in strengthening its technical capacity and modernizing its infrastructure.

The Cabinet of Ministers approves a Resolution for responding to cyber incidents and cyber attacks

On April 4, 2023, the Cabinet of Ministers of Ukraine approved the resolution for response by cybersecurity entities to various types of events in cyberspace, developed by SSSCIP. The document was adopted as a measure to execute Ukraine's Cyber Security Strategy Implementation Plan.

"The order approves a single mechanism for the implementation by cyber security entities of operational procedures for responding to cyber incidents. It also defines clear and understandable levels of criticality of cyber incidents and the stages of response to them," said Oleksandr Potii, SSSCIP Deputy Head.

The procedure will enable the formation of response actions to cyber incidents and cyber-attacks according to pre-planned cyber protection measures aimed at (i) rapid detection and protection against cyber incidents and cyber-attacks; (ii) proper notification of such events, and (iii) restoration of the stability and reliability of the functioning of information, electronic communication, information and communication systems, technological systems, and other cyber protection objects.

USAID Aids Ukraine to Boost Critical Infrastructure Security

On April 28, Cabinet of Ministers of Ukraine (CMU) passed a Resolution for maintaining the Critical Infrastructure Facilities Registry. The USAID Cybersecurity for Critical Infrastructure in Ukraine Activity supported the development of this Resolution by providing a team of four legal advisors embedded in SSSCIP. The team provides legal advice to SSSCIP by contributing to drafting legal acts, including CMU resolutions and law amendments. It adds to the regulatory framework from the Critical Infrastructure Law and strengthens the State Service of Special Communications and Information Protection (SSSCIP) as the main agency for critical infrastructure security in Ukraine. Creating the Registry improves coordination, information exchange, and threat database for critical infrastructure security. It also allows issuing safety certificates.

Government Resolution on strengthening the protection of national electronic information resources

In April 2023, the Government adopted the resolution "Some issues of the functioning of the National Center for Reservation of State Information Resources" that regulates (i) the functioning and purview of the National Center for Reservation of State Information Resources, and (ii) the procedure for the transfer of backup copies of national electronic information resources to the National Center by state authorities, military formations, enterprises, institutions and organizations, as well as the mechanism of their preservation and access to them.

Government adopted Bug Bounty Procedure Developed by SSSCIP

On May 16, 2023, the Cabinet of Ministers of Ukraine adopted a Resolution on the Procedure for Finding & Detecting Potential Information (Automated), Electronic Communication, Information & Communication Systems, and Electronic Communication Grid Vulnerabilities. This legally permits network owners to perform vulnerability tests on their systems and grids using third-party experts. This legislative change is expected to reduce time and cost to identify and remediate vulnerabilities in full compliance with regulation, while at the same time deploying industry-standard best practice to significantly enhance cybersecurity in general. This is a major step forward in implementing coordinated, distributed detection of information and communication systems vulnerabilities at the national level. Such an approach, also known as Bug Bounty, is widely used globally to engage third-party experts to finding and fixing software and system errors and vulnerabilities. The Procedure was developed with the support of Better Regulation Delivery Office (BRDO) and EU-funded EU4DigitalUA project.

Google launches the online game Interland: Child Safety on the Internet in Ukraine

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

Defense tech cluster BRAVE1 launched in Ukraine to stimulate development of military innovations and defense technologies

In April 2023, the Government of Ukraine launched an initiative to streamline and promote innovation in the development of drones and other technologies that have been critical in the war with Russia. 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 can 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.

NCCC deepens cooperation with Recorded Future, a threat intelligence company

Deputy Secretary of NSDC of Ukraine Serhiy Demediuk, the Head of the Information and Cybersecurity Directorate at the Office of NSDC of Ukraine, the Secretary of NCCC Nataliya Tkachuk, and the Head of NCCC Operations Support Department Serhii Prokopenko met with the CEO and co-founder of Recorded Future Christopher Ahlberg. They discussed ways to deepen practical cooperation between the NCCC and the company.

Recorded Future has been instrumental in providing intelligence to safeguard Ukraine's crucial infrastructure and aiding in investigating Russian war crimes since the start of the full-scale invasion. Additionally, the firm granted access to the Intelligence Cloud software platform worth $10 million.

NCCC conducts Vulnerability Management training for cybersecurity specialists in Ukraine's energy sector

With CRDF Global support, the NCCC held a training from the Vulnerability Management (VDP) series in March and April, 2023. Over 30 skilled technical specialists attended the tenth program, representing 20 organizations from Ukraine's energy sector, including the Ministry of Energy, EnergoAtom, UkrEnergo, and regional energy companies. The participants were highly engaged in completing the tasks for the final CTF, demonstrating their interest in the training. The winners of the six-week training program were awarded prizes to further enhance their professional skills.

The training aimed at equipping participants with skills for detecting vulnerabilities in information as well as skills for building and supporting comprehensive cyber defense to the primary entities responsible for cybersecurity, government institutions, critical infrastructure facilities, and other organizations in public-private partnerships.

USAID facilitates the discussion of Ukraine's cybersecurity market at the 6th Cybersecurity Dialogue

On June 29, 2023, USAID Cybersecurity for Critical Infrastructure in Ukraine Activity conducted the 6th Cybersecurity Dialogue titled *Cybersecurity Market Development in Ukraine: Tools and Cooperative Activities*. The participants included private sector and civil society representatives, who provided an in-depth review of the most tangible challenges and market development strategies applicable to the cybersecurity sector. Discussing best practices of other markets, the dialogue explored effective tools and techniques that can help build cybersecurity market in Ukraine and prioritize joint activities of the cybersecurity sector stakeholders.

SSSCIP conducts the first table-top Critical Infrastructure Resilience Exercises (CIREX), based on scenarios developed by CISA, and supported by USAID Cybersecurity for Critical Infrastructure in Ukraine Activity

At CIREX, the focus was on addressing cyber threats and collaborating to defend against cyberattacks. Representatives from the energy sector participated in the training to develop strategies for responding to ransomware attacks. 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, the SBU, National Police, and NSDC Executive Office.

Figure 1Participants of the first Critical Infrastructure Resilience Exercises (CIREX) in the energy sector in April 2023

SSSCIP and CYBER RANGES sign a memorandum of cooperation for cyber education and professional development in cyber defense

In April, the SSSCIP welcomed CYBER RANGES Corp., a company specializing in the development of technology solutions for cyber defense training using next-generation technologies and high-precision modeling. During their visit, the SSSCIP and CYBER RANGES signed a memorandum of cooperation that covered various areas such as sharing information, experiences, and best practices in cyber protection. The two organizations will also engage in joint drills under the CYBER RANGES platform and participate in educational activities on cyber threats. Additionally, CYBER RANGES will assist in skills development programs in cyber defense, organize qualifying examinations, and provide professional certification/confirmation procedures under Ukrainian professional standards for cybersecurity using their advanced technologies.

Romanian technical delegation on cybersecurity visited SSSCIP

On May 26th, 2023, a delegation from Romania focused on cybersecurity, led by State Secretary Dan Cimpean, the Director of the National Cyber Security Directorate of Romania (DNSC), recently visited Ukraine's State Service of Special Communications and Information Protection (SSSCIP). In a meeting with Yurii Shchyhol, Chairman of the SSSCIP, and Deputy Heads Victor Zhora and Oleksandr Potii, Romanian representatives explored ways to enhance cooperation between DNSC and SSSCIP.

"I am grateful for the assistance your country provides to Ukraine. Our cooperation has great prospects. The confrontation in cyberspace and Russia's war against Ukraine have shown that only together, united by the entire civilized world, can we defeat the enemy. Now we are on guard of the cybersecurity of the whole of Europe and are ready to share our knowledge and skills" -Yuriy Shchyhol, Chairman of the SSSCIP

They discussed pressing concerns such as cyber threats and attacks by the aggressor in the context of the Russian full-scale invasion of Ukraine. The discussions focused on sharing knowledge about safeguarding critical infrastructure and aligning regulatory policies with EU standards. Additionally, efforts were made to foster collaboration with NATO and EU entities, and guidance was provided on how to work in tandem with these organizations. The Romanian delegation also visited the UA30 Cyber Center and spoke to representatives of CERT-UA.

USAID delivers international experience to finalize Ukraine's Cyber Incident Response Plan

On May 12, 2023, the USAID Cybersecurity for Critical Infrastructure in Ukraine Activity organized a joint discussion between National Security and Defense Council, SSSCIP, U.S. Cybersecurity & Infrastructure Security Agency (CISA), and MITRE to share learnings on the development and implementation of the US National Cyber Incident Response Plan (NCIRP). Ukrainian participants asked US interlocutors to share their experience on building consensus between cyber stakeholders and challenges faced during the NCIRP implementation phase. The observations and recommendations will be applied during the final review of Ukraine's draft NCIRP to be presented by NSDC and SSSCIP to cybersecurity stakeholders in Ukraine in the upcoming months.

OSCE assists Ukrainian law enforcers in investigating cybercrimes

A group of 30 law enforcement officers from the National Police of Ukraine completed a 3-day training course on countering cybercrime. The training, organized by the OSCE Support Program for Ukraine, took place in Lviv from May 29 to May 31, 2023. During the course, officers learned about the latest methods used by criminals, as well as effective ways to combat cybercrime. Topics covered included police intelligence analytics tools, open-source intelligence (OSINT), and data processing and analysis. Special attention was given to the identification, recording, and analysis of "digital traces," which can be used as electronic evidence in court to prosecute offenders. During the meeting, the attendees covered several topics, including the use of virtual assets and payment methods by criminals to trace and disrupt the activities of organized crime groups. Additionally, they delved into the digital intricacies of human trafficking, examining the details thoroughly. The OSCE Support Program for Ukraine is scheduled to hold nine additional training sessions for officers from the Cyber Police and Migration Police Departments of the National Police of Ukraine. The goal is to train a total of 300 police officers by the end of the year, as part of the Project "Strengthening Capacity of the National Police of Ukraine to Combat Trafficking in Human Beings, including Cyber-Enabled Crime".

Ukraine and the United States hold an annual discussion on cyber policy issues

The annual Ukraine-U.S. Cyber Dialogue took place in Tallinn, Estonia on June 1, 2023. During the discussions, the United States delegation reiterated its steadfast commitment to supporting Ukraine's cyber defense against Russia's unprovoked invasion. To fulfill this commitment, the United States is collaborating with Congress to provide an additional $37 million in cyber assistance to Ukraine, bringing the total to $82 million since February 2022 and over $120 million since 2016. This assistance has greatly enhanced Ukraine's ability to detect, deter, and respond to cyber threats and incidents, as well as safeguard critical networks and digital infrastructure.

Figure 2. High-level participants of the annual Ukraine-U.S. Cyber Dialog in Tallin, June 2023

A delegation from Ukraine, led by Deputy Foreign Minister Anton Demokhin, included Deputy Minister of Digital Transformation George (Yegor) Dubynskyi, Deputy Minister of Defense Vitaliy Deynega, as well as representatives from various agencies such as NCCC, the General Staff of the Armed Forces of Ukraine, the Security Service of Ukraine, the State Service of Special Communications and Information Protection of Ukraine, the National Police of Ukraine, the Foreign Intelligence Service of Ukraine, the Ministry of Energy, and Ambassador of Ukraine to Estonia Mariana Betsa. On the other side, the U.S. delegation was led by Ambassador at Large for Cyberspace and Digital Policy Nathaniel C. Fick from the Department of State. The U.S. delegation included Acting National Cyber Director Kemba Walden from the White House, Deputy Assistant Secretary of Defense Mieke Eoyang, U.S. Cyber Command Deputy Commander Lieutenant General Timothy Haugh, Brigadier General Chad Raduege of U.S. European Command, Deputy Assistant Secretary of Homeland Security Thomas McDermott, and Executive Director of the Cybersecurity and Infrastructure Security Agency Brandon Wales, as well as representatives from the Federal Bureau of Investigation and USAID.

Both delegations presented their viewpoints regarding the significance of cybersecurity in Ukraine's continuous digital advancement. This includes reinforcing the country's workforce, institutions, and critical infrastructure. Moreover, the attendees deliberated on potential Ukraine-U.S. cooperation on cyber concerns, which entails knowledge-sharing of the valuable insights gained by Ukraine in its continuous efforts to improve cyber and digital policies.

Cyber Defense Influencers Meet in Tallin for the CyCon 2023 15th International Conference

The 15th International Conference on Cyber Conflict, CyCon, was held in Tallin on May 30 – June 2. This unique annual event, hosted by the NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE), brought together key experts and decision makers from the global cyber defense community.

Cyberspace has no borders – and the event provided a valuable opportunity for partners to tackle shared challenges. The war in Ukraine has brought new geopolitical tensions and partnerships, tested our ideas, presumptions, and established practices, and presented new challenges. It has also brought new opportunities for the application and interpretation of law, policies, and technology.

CyCon 2023 saw over 600 cyber experts from nearly 50 countries come together to address current cybersecurity challenges through presentations, focus sessions, and breakout groups. This year's CyCon, even though with a special angle on the Russia-Ukraine war, had a theme of Meeting Reality, which included discussions on new technologies, both the benefits and opportunities they provide and the new threats they pose.

Ministry of Digital Transformation of Ukraine, SSSCIP and the Ministry of Digitalization of Japan sign a memorandum of cooperation

During Deputy Valeria Ionan's working visit to Tokyo, the Deputy Prime Minister for Innovation, Development of Education, Science and Technology, Mykhailo Fedorov, signed a memorandum of cooperation with Japan's Minister of Digitalization, Taro Kono, in an online meeting.

Under the memorandum, Japan has pledged to assist Ukraine in enhancing its innovation and cybersecurity capabilities. Ukraine is currently facing threats not only on the frontlines but also in cyberspace. Japan's advanced technological solutions will be instrumental in reinforcing the digital borders of Ukraine and safeguarding the information systems of critical infrastructure facilities. The ministers have agreed to share best practices in IT industry development and e-government initiatives during their meeting.