USAID
FROM THE AMERICAN PEOPLE

USAID CYBERSECURITY FOR CRITICAL INFRASTRUCTURE IN UKRAINE

Cyber Sector Update

JULY 2023 – SEPTEMBER 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

- Cyberattack on State Statistics Service of Ukraine
- Russian Hackers Lured Embassy Workers in Ukraine with BMW Advertisements
- Ukrainian State Services Increasingly Targeted by Armageddon
- CERT-UA Notes Vendor Email Compromise Attack Campaign in July
- Turla's New DeliveryCheck Backdoor Aims at Ukrainian Defense Sector
- Hackers Target Justice Bodies and Notaries in Ukraine
- Cybercriminals Use Attributes of SSSCIP to carry out Phishing Attacks
- Criminals Disguise MerlinAgent Viruses as Recommendations from CERT-UA

PUBLIC SECTOR DEVELOPMENTS

- NCCC Meeting in July Discusses Cyber Diplomacy and Implementation of Cybersecurity Strategy
- USAID Drives Cybersecurity Enhancement in Ukraine
- Verkhovna Rada Committee on National Security and Defense establishes a subcommittee on cybersecurity, government communication, and information protection in Ukraine

LEGAL DEVELOPMENTS

- SSSCIP Approves Methodological Recommendations on the Response of Cybersecurity Entities to Various Types of Events in Cyberspace

- Government Approves the Tasks of the National Program for Digital Transformation, Including Strengthening Cyber Defense
- Government Adopts a Resolution Forming the Legal Basis for a Network of Situation Centers in Ukraine
- USAID Supports SSSCIP with Developing New Cybersecurity Professional Standards
- USAID Facilitates Development of Critical Infrastructure Passport System Resolution

PRIVATE SECTOR DEVELOPMENTS

- USAID Helps Develop Ukraine's Cybersecurity Talent with Student Cybersecurity Competition
- Ministry of Digital Transformation and Cyberfame GmbH Announce Strategic Partnership
- Financial Times: "Ukraine Innovates on Cyber Defense"
- USAID-Facilitated Dialogue Events Address Cybersecurity Community Wartime and Professional Training Challenges
- USAID Launches $500,000 Grant Program to Support Cybersecurity Innovations Deployment

INTERNATIONAL COOPERATION

- NCCC Deepens Collaboration with US and EU in using AI in Cybersecurity
- SSSCIP Starts Collaborating with the Spanish National Cybersecurity Institute
- Ukrainian Delegation Headed by NCCC Secretary visits NATO Headquarters
- NIST Drafts Major Update to Its Cybersecurity Framework
- CISA and SSSCIP Mark One Year of Cooperation
- SSSCIP Deputy Head Viktor Zhora Attends the FBI Atlanta Cyber Threat Summit (FACTS)
- CISA Director Praises Collaboration with Ukrainian Counterparts

Cyberattack on State Statistics Service of Ukraine

Russian hacktivists, linked to the Russian Armed Forces (previously known as GRU), persist in executing intricate attacks on Ukraine through a combination of cyberattacks, information, and psychological operations. On July 5, a post on the official Facebook page of Ukraine's State Statistics Service (Ukrstat) reported a cyberattack that prevented the submission of statistical data to the government.

The post about the cyberattack and its "consequences" appeared because Ukrstat's official Facebook page was compromised. CERT-UA and Ukrstat confirm the attack on information resources; however, its results are greatly exaggerated. Ukrstat reports its information resources were not affected as a result of the incident. The data processed on the Ukrstat resources, server equipment, and information and communication infrastructure were not affected and Ukrstat's capability to provide statistical data remains uncompromised.

Russian Hackers Lured Embassy Workers in Ukraine with BMW Advertisements

News broke on July 12 that APT29 (also known as Cozy Bear) hackers had attacked 22 foreign missions located in Kyiv. They achieved this by intercepting an email from a diplomat who was circulating a flyer to various embassies advertising the sale of a used BMW 5-series sedan. The hackers made a copy of the flyer, inserted malware, and sent it to many other foreign diplomats. The legitimate email contained a number of shortened URL links leading to photos of the vehicle, which the APT 29 actors redirected to a malicious website so that when a victim attempted to view any of the photos, which were now actually Windows shortcut files disguised as .png images, the image would display on their screen, but Cozy Bear's malware would execute in the background. The identities of the embassies that were successfully targeted have not been disclosed.

Ukrainian State Services Increasingly Targeted by Armageddon

According to a CERT-UA analysis published in July, Armageddon, a hacking group with ties to Moscow, is still one of the most active and dangerous cyber threat actors targeting Ukraine since Russia's full-scale invasion. The group,

also known as Gamaredon, primarily engages in cyberespionage operations against Ukrainian security and defense services. However, CERT-UA has linked the group to at least one destructive cyberattack against an unspecified information infrastructure facility. The group has infected thousands of government computers.

According to cybersecurity experts, Armageddon is based in the Crimean Peninsula, annexed by Russia, and takes orders from Russia's Federal Security Service in Moscow. The group has continuously improved its tactics and tools to avoid being detected. Researchers have recently observed the group's use of a new technique - infecting USB drives. This allows the threat actor to infect new nodes if the infected drive is shared between computers.

CERT-UA Notes Vendor Email Compromise Attack Campaign in July

In the last 10 days of July, CERT-UA recorded the third cyberattack by UAC-0006 using letters on the subject of "invoice payment."

Vendor email compromise, also referred to as "financial supply chain compromise," is a targeted type of business email compromise (BEC) attack in which attackers impersonate a third-party vendor in order to steal from that vendor's customers. In the wave of July attacks, CERT-UA observed an increase in the number of such attacks using a message with the subject line "invoice payment." The malicious message contains an attached archive file, composed of files and archives named: "Payment instruction and extract from the register", "Extract from the register from 07/24/2023_Document code..." etc. Opening the files leads to download and launch of the SmokeLoader malware. The primary goal of this BEC appears to be to inflict harm on accounting computers used to monitor financial activity. A secondary objective appears to be theft of authentication data such as login credentials, passwords, keys, or certificates, which can lead to unauthorized payments. There have been instances where criminals have deployed bot networks consisting of over 1,000 computers to send out a large number of emails. This could potentially result in an uptick in fraud cases involving remote banking systems. Based on the use of Russian domains to host the SmokeLoader botnet and repurposing of tools, CERT-UA attributes the campaign to a threat group tracked as UAC-0006, a group observed deploying attacks against Ukraine from 2012-2021 using the same malicious strains and phishing attack vector. The main aim is to harm accounting computers that are utilized to monitor financial activity. Another technique is the theft of authentication data such as login credentials, passwords, keys, or certificates, which can lead to unauthorized payments.

Turla's New DeliveryCheck Backdoor Aims at Ukrainian Defense Sector

A malware family discovered in espionage attacks against the defense sector in Ukraine and Eastern Europe was linked to the Turla Russian APT by CERT-UA in July. A new .NET-based backdoor known as DeliveryCheck (also referred to as CAPIBAR or GAMEDAY) targeted Ukraine's defense sector. The DeliveryCheck malware is distributed via email as documents with malicious macros. It persists via a scheduled task that downloads and launches it in memory. Tracked since 2022, the malware was observed proliferating this year in January and February via weaponized Excel sheets, with infections accelerating in May and peaking in July. The Microsoft threat intelligence team collaborated with CERT-UA to attribute the attacks to a Russian nation-state actor called Turla. Turla is also known as Iron Hunter, Secret Blizzard (previously Krypton), Uroburos, Venomous Bear, and Waterbug. It is believed to have ties with Russia's Federal Security Service (FSB).

It also contacts a C2 server to retrieve tasks, including the launch of arbitrary payloads embedded in XSLT stylesheets.

Hackers Target Justice Bodies and Notaries in Ukraine

In August, CERT-UA reported that hackers have been targeting the justice and notary bodies of Ukraine for a long time. The criminals send emails with attachments containing BZIP, GZIP, or RAR archives. Once the file is opened, it infects the computer with the AsyncRAT malware, which allows remote access to the device.

Experts from CERT-UA have observed that hackers tend to use particular email subjects and file names when sending malicious emails. These include examples such as "Letter of the Department of Notary Affairs in Dnipropetrovsk Oblast.rar", "Letter for information and implementation.cmd", and "Letter of the Ministry of Education for information and consideration in the work.exe.bzip". Cybersecurity experts infer that the primary targets of these attackers are Ukraine's justice and notary organizations.

Cybercriminals Use Attributes of SSSCIP to carry out Phishing Attacks

In August, CERT-UA discovered a large-scale distribution of phishing emails among government agencies. These emails had the subject line "[CERT-UA#5086] Suspicious login to your mailbox" and were purported to be from CERT-UA. The emails also contained SSSCIP's branding. The emails contained a message requesting the recipient to change the password and a link to a website that mimics the Roundcube mail software's interface. Upon clicking on the link and inputting their authentication details, the authorized user unwittingly shares with the hackers their login and password credentials through an HTTP POST request.

The fake web resource was created using the free InfinityFree service. In addition, the attackers used the mlcrosoft.rf[.]gd subdomain, which was supposed to impersonate Microsoft services.

Criminals Disguise MerlinAgent Viruses as Recommendations from CERT-UA

On August 5th, 2023, CERT-UA investigated emails sent by criminals using the email address cert-ua@ukr.net. The messages using the subject line "CERT-UA recommendations on the settings of MS Office programs" contained an attached file "INTERNAL CYBER THREAT.chm" ostensibly included in the message by CERT-UA.

Opening the CHM file runs a JavaScript code that activates a PowerShell script which in tun infects the user's computer with MerlinAgent. This compromise allows hackers to gain remote access to the computer, execute commands, download, and delete files without the user's knowledge or consent. Merlin is an open-source post-exploitation and command and control framework with a cross-platform post-exploitation toolkit available for free via GitHub, offering extensive documentation for security professionals to use in red team exercises. As a red team tool, Merlin offers a wide range of features, allowing red teamers (and attackers) to obtain a foothold on a compromised network. MerlinAgent attacks were recorded on July 10, during a cyberattack against a Ukrainian state organization. In that campaign, attackers sent e-mails using the subject line "UAV Training."

PUBLIC SECTOR DEVELOPMENTS

NCCC Meeting in July Discusses Cyber Diplomacy and Implementation of Cybersecurity Strategy

On July 28, NSDC Deputy Secretary Serhiy Demediuk held the 22nd meeting of the NCCC, during which participants discussed issues related to developing cyber diplomacy, implementing the Cyber Security Strategy of Ukraine, improving the effectiveness of annual planning for the strategy's tasks, and additional cybersecurity measures for Operational technology (OT) systems at critical infrastructure facilities.

Deputy Secretary Demediuk's proposal was supported by the meeting participants. They agreed that cyber diplomacy approaches should be formed as proposed by the Ministry of Foreign Affairs. Communication with international partners should include the NCCC and key entities of the national cyber security system to ensure an agreed-upon position. The participants also discussed issues related to creating an interagency working group and a relevant digital platform in this context.

"In the context of armed aggression waged by Russia against Ukraine both on the battlefield and in cyberspace, cyber diplomacy is becoming increasingly relevant for our country", – Serhiy Demediuk, Deputy Secretary, National Security & Defense Council of Ukraine.

USAID Drives Cybersecurity Enhancement in Ukraine

On July 3, 2023, SSSCIP officially adopted the Cyber Incident Response Guidelines, shaping a more resilient cybersecurity landscape. Developed with support from the USAID Cybersecurity for Critical Infrastructure in Ukraine Activity, the guidelines aim to assist cybersecurity stakeholders – ranging from government entities to individuals in information protection – in quickly assessing and properly responding to cyber incidents. Incorporating U.S. best practices into these Guidelines fortifies Ukraine's cybersecurity posture and critical infrastructure resiliency.

Verkhovna Rada Committee on National Security and Defense establishes a subcommittee on cybersecurity, government communication, and information protection in Ukraine

A subcommittee on cybersecurity, government communication, and information protection was established within the Verkhovna Rada of Ukraine's Committee on National Security, Defense, and Intelligence in August. The subcommittee has been tasked with overseeing matters related to national security. This includes critical infrastructure, cyber defense, cyber intelligence, countering cyber terrorism and cyber espionage, and government communications security. Additionally, the subcommittee will address concerns regarding the technical and cryptographic protection of information, as well as the state system of special communication and the state system of the insurance fund of documentation.

"Russia uses cyber space to deprive Ukrainian of electricity, water supply, banking services, or steal personal data. And Ukraine has successfully defended itself in this cyber war. The significance of communications in the current circumstances can hardly be overestimated. Establishing a specialized Parliamentary sub-committee will allow us to deal with these important issues in a more dedicated and focused manner" - Oleksandr Fediienko, Member of Parliament, Head of Parliamentary Sub-committee on Special Communications and Information Protection

LEGAL DEVELOPMENTS

SSSCIP Approves Methodological Recommendations on the Response of Cybersecurity Entities to Various Types of Events in Cyberspace

On July 3rd, the SSSCIP approved methodological recommendations for cybersecurity entities to respond to various types of cyber events in accordance with the Cybersecurity Strategy of Ukraine and the Government's resolution. The recommendations also incorporated version 2.0 of the General Rules for Exchange of Information on Cyber Incidents, or Traffic Light Protocol (TLP), approved by the NSDC NCCC, and a list of categories and types of cyber incidents.

The Recommendations, developed with the support of USAID's Cybersecurity for Critical Infrastructure in Ukraine Activity, considered the approaches of the Cyber Security and Infrastructure Protection Agency (CISA), the National Institute of Standards and Technology (NIST) and other relevant regulatory acts.

Government Approves the Tasks of the National Program for Digital Transformation, Including Strengthening Cyber Defense

On July 21st, the Government adopted a resolution that focuses on implementing digital systems in government administration and reinforcing cyber defense for government agencies, financial institutions, and enterprises. By

putting the National Program for Digital Transformation into action, digital technologies can be implemented more efficiently. This program will also aid in creating, modernizing, and developing information and communication systems and digital tools. Additionally, it will strengthen the cyber defense of critical information infrastructure. By doing so, government agencies will become safer, more effective, and more efficient.

Government Adopts a Resolution Forming the Legal Basis for a Network of Situation Centers in Ukraine

In July, the Government adopted a Resolution to enable a network of situation centers in Ukraine. To effectively manage crises and ensure the national security of Ukraine, it is important to establish suitable situation centers. The resolution titled "Issues of the network of situation centers" outlines the necessary components, responsibilities, and requirements for these centers' software, hardware, subsystems, and networks. Additionally, this resolution creates a foundation for future expansion and development of the network of situation centers through legal means.

USAID Supports SSSCIP with Developing *New Cybersecurity Professional Standards*

The creation of the National Cybersecurity Workforce Framework envisages 21 cybersecurity professional standards to meet current market demands and global standards. SSSCIP specialists, with the support of the USAID Cybersecurity for Critical Infrastructure in Ukraine Activity, have developed 15 new cybersecurity professional standards in addition to six standards developed last year.

"Following the discussion, new professional standards will be adopted and included in the National Qualifications Registry. Then standards can be used to evaluate compliance of professional knowledge, skills and abilities with the established requirements and relevant needs, to carry out advance trainings, and so on. The professional standards will serve as a basis of advanced curricula for higher educational institutions," - SSSCIP Deputy Head Oleksandr Potii.

USAID Facilitates Development of Critical Infrastructure Passport System Resolution

On August 4, 2023, the Cabinet of Ministers of Ukraine adopted Resolution #818 on a Critical Infrastructure Passport System, approving the specific Critical Infrastructure Safety Passport Approval Procedure. The USAID Cybersecurity for Critical Infrastructure in Ukraine Activity facilitated the development of the Procedure by providing the services of five embedded legal consultants. The Procedure itself complements the Resolution for Maintaining the Critical Infrastructure Facilities Registry adopted in April 2023 and sets requirements for the actual Critical Infrastructure Safety Passports that will contain key information about any specific individual Critical Infrastructure entity. This brings Ukraine one step closer to establishing an efficient national system of Critical Infrastructure protection and USAID will continue to support these efforts assisting Ukraine in its implementation of the national Critical Infrastructure Law.

USAID Helps Develop Ukraine's Cybersecurity Talent with Student Cybersecurity Competition

On July 1-2, 2023, the USAID Cybersecurity for Critical Infrastructure in Ukraine Activity in partnership with Amazon Web Services held an online cybersecurity competition for high-school and university students in together with the Igor Sikorsky Kyiv Polytechnic Institute – National Technical University of Ukraine (KPI). Organized in the

popular capture-the-flag (CTF) format, the Sikorsky CTF attracted an impressive 542 participants comprising 153 teams representing 109 schools and universities from across Ukraine. AWS provided Amazon Elastic Compute Cloud (Amazon EC2) platform to host the competition servers and secure the event from DDoS attacks.

Over the course of 48 hours, navigating through real-life cybersecurity scenarios, participants gained hands-on experience in countering simulated cyberattacks enhancing their problem-solving skills and teamwork. An ideal platform for honing individual skills, the Sikorsky CTF allowed young participants to learn new cyber techniques, forge new friendships, and establish peer-to-peer connections that will contribute to the growth and development of Ukraine's cybersecurity community. The Activity will continue to support such initiatives to foster Ukraine's cybersecurity talent and contribute to building a more resilient and robust cybersecurity ecosystem in Ukraine.

Ministry of Digital Transformation and Cyberfame GmbH Announce Strategic Partnership

The Ministry of Digital Transformation of Ukraine and the German company Cyberfame GmbH signed a memorandum of cooperation in July. The partnership aims to address important areas such as digitalization, digital security, software development, and professional development in the fields of digital and cybersecurity. The memorandum lays out a plan to enhance digital resilience and cybersecurity measures by sharing experience, knowledge, and best practices. Cyberfame GmbH will provide specialized training for technical specialists and managers of state institutions as part of this partnership. This will help create a skilled workforce capable of tackling cyber challenges.

George Dubynskyi, Deputy Minister of Digital Transformation in Ukraine explained that the Ministry is working hard to create a stronger cybersecurity ecosystem for public services. Thanks to a new partnership with Cyberfame GmbH, Ukrainian specialists will have access to valuable tools and knowledge from European experts, which will help them build a more secure cyberspace. This collaboration is expected to significantly impact web resource security, making public services more resistant to potential attacks or unauthorized access to sensitive data.

Financial Times: "Ukraine Innovates on Cyber Defense"

In July, the Financial Times published an article praising Ukraine's cyber defense strategy as an innovative model for other countries to follow in their efforts to combat a dangerous enemy. Ukraine has maintained constant vigilance and formed unprecedented partnerships with private sector groups from the US and Europe, including major corporations like Microsoft and Cisco's Talos, as well as smaller firms like Dragos. These companies have taken on contracts to protect Ukraine and gain insight into Russian cyber tradecraft. The article suggests the successful, layered, and collaborative defense has yielded a practical, replicable model leveraging the vigilance of supply chain participants around the world to identify threats early, successfully thwart vulnerability exploit attempts, and respond rapidly and effectively to compromises.

USAID-Facilitated Dialogue Events Address Cybersecurity Community Wartime and Professional Training Challenges

In September 2023, USAID Cybersecurity Activity, in collaboration with the Aspen Institute Kyiv, played a vital role in cultivating Ukraine's cybersecurity landscape through two significant dialogues. The September 14th Cyber Dialogue titled 'Nurturing Ukraine's Cybersecurity Ecosystem: Cooperating and Finding Effective Solutions' united cybersecurity market players and IT/cyber associations to address wartime challenges and identify areas of cooperation. Emphasizing the need for a united cybersecurity community advocating for industry interests, the participants discussed collaborative mechanisms and unified approaches for market development.

The September 26th dialogue event 'Who is a Modern Cybersecurity Specialist?' aimed to address challenges in Cybersecurity Workforce Development. Participants tackled issues from the perspectives of future employers, higher education cybersecurity instructors, and young talent.

USAID Launches $500,000 Grant Program to Support Cybersecurity Innovations Deployment

On September 29, 2023, the USAID Cybersecurity Activity, in collaboration with the Ministry of Digital Transformation of Ukraine, announced a $500,000 grant program aimed at fostering innovations within the realm of cybersecurity. This new grant program aims to unveil the potential of Ukraine's talented cybersecurity experts and foster their innovative thinking. USAID will support the innovations at their deployment phase to stimulate cybersecurity market growth and expose local cyber talents to the world.

NCCC Deepens Collaboration with US and EU in using AI in Cybersecurity

On July 5, Nataliya Tkachuk, head of the NSDC Information Security and Cyber Security Service, and Serhiy Prokopenko, head of the NCCC Department of Security, met with the Director of US Institute for National Security and Counterterrorism, former Advisor to the President of the U.S. James Baker, Head of National and State Security Department of the EU Advisory Mission Ukraine Seppo Rutsalen, and EUAM National Security Adviser Maksym Budakov. During the meeting, the parties discussed the potential of utilizing AI for national security purposes, exchanged opinions on the use of AI in cybersecurity, and deliberated on the issues and opportunities concerning cybersecurity in Ukraine.

SSSCIP Starts Collaborating with the Spanish National Cybersecurity Institute

During an official visit to the SSSCIP in July, a delegation from the Spanish National Cybersecurity Institute (INCIBE), led by Director General Felix Barrio and run by the Ministry of Economic Affairs and Digital Transformation through the State Secretariate for Digitalization and Artificial Intelligence, signed a Memorandum of Understanding on cyber defense. The main focus of cooperation between the entities will be on sharing information, recommendations, and best practices to improve incident management, response, and recovery systems related to cyberthreats. Legislative aspects, information, and communication technologies of a strategic, technical, and scientific nature will also be given special attention.

Ukrainian Delegation Headed by NCCC Secretary visits NATO Headquarters

On July 6-7, a delegation of representatives of Ukraine's key cybersecurity entities visited NATO headquarters, NATO Operations Command, and the NATO Communication and Information Agency as part of the C4 knowledge exchange project for the NATO-Ukraine Comprehensive Assistance Package Trust Fund. The Ukrainian delegation, led by NCCC Secretary and head of the NSDC Information Security and Cybersecurity Service Nataliya Tkachuk, presented an overview of Ukraine's cybersecurity system and the lessons of the ongoing cyber war. It also presented Ukraine's needs and proposals for future cooperation with NATO in cybersecurity.

The partners noted the coordinated work of all of Ukraine's cybersecurity entities during the war and emphasized their readiness to expand support and cooperation with Ukraine in the field of cybersecurity.

"The experience we have gained in countering Russia's cyberaggression is crucial for strengthening collective cybersecurity, and we will eagerly share it with our key partners and allies. Russia's threat can only be overcome by working together", – Nataliya Tkachuk, NCCC Secretary and head of the NSDC Information Security and Cybersecurity Service

NIST Drafts Major Update to Its Cybersecurity Framework

On August 8, The US National Institute of Standards and Technology (NIST) released a draft version of its Cybersecurity Framework (CSF) 2.0, which has been developed following a year's worth of community feedback. It is an updated version of the tool first launched in 2014 to help organizations understand, reduce, and communicate cybersecurity risks. The new update is aimed at reflecting the latest changes in the cybersecurity landscape and makes it easier for organizations of all types to put the CSF into practice.

CISA and SSSCIP Mark One Year of Cooperation

On August 1, 2023, SSSCIP and CISA celebrated the first anniversary of their operational collaboration. This partnership is supported by the USAID Cybersecurity for Critical Infrastructure in Ukraine Activity. SSSCIP and CISA have successfully implemented several joint initiatives, focusing on areas such as exchanging data on cyber security risks and incidents, sharing best practices in public-private cooperation, conducting executive and staff exercises, and implementing practices to protect critical infrastructure. They plan to continue exchanging information and practical experience, as well as conducting master classes and trainings on cyber security. They aim to expand executive, and staff exercises and strengthen cooperation to build a safer cyber landscape in Ukraine, protecting critical infrastructure and citizens from cyber threats.

"*State Communications and CISA are the central organizations of Ukraine and the USA in the field of critical cyber infrastructure security. Their cooperation is an example of how we can come together to develop innovative strategies that advance our common priorities and prevent cyber threats*," noted Kevin Covert, Deputy Head of the Mission and representative of the U.S. Embassy in Ukraine.

"*Ukraine and the USA are now countries that are experiencing a huge number of attacks in cyberspace. That is why it was very important for us to start cooperation with CISA, exchange experience, get acquainted with leading practices and technologies and introduce them in our country. The first year was extremely fruitful. Such cooperation makes it possible to strengthen cyber resilience and to more effectively resist cyber-attacks*," noted the deputy head of the SSSCIP, Viktor Zhora. "*We still have a lot to work on within the current Memorandum. However, it is also important for us to understand the possible additional directions of cooperation with the State Intelligence Service and to ensure their compliance with the major strategic goals to which Ukraine is moving in the field of critical infrastructure protection, cyber resilience, and cyber security. We would like to look back in a year and see what really affected the strengthening of cyber security in both countries*," noted Brandon Wells, executive director of CISA, during the event, thanking USAID for helping to organize this cooperation.

SSSCIP Deputy Head Viktor Zhora Attends the FBI Atlanta Cyber Threat Summit (FACTS)

To strengthen their defenses, it is crucial for companies and governments to study the techniques used by their enemies and share information. This was emphasized by Viktor Zhora, the Deputy Head for Digital Development, Digital Transformation and Digitalization at SSSCIP, during the FBI Atlanta Cyber Threat Summit (FACTS) that took place on August 7. The summit was also attended by Christopher A. Wray, the Director of the FBI, and Bryan Vorndran, the Assistant Director of the FBI's Cyber Division.

According to Zhora, sharing information with international partners, such as governments, dedicated security agencies, and especially the private sector, which has provided very valuable cyber threat information, plays a major role in Ukraine's withstanding the current cyberwar waged by Russia. This has helped Ukraine promptly address weak points in many information systems and prevent possible large-scale incidents from happening at critical infrastructure facilities. The SSSCIP Deputy Head thanked the US partners for their assistance in repelling Russia's cyber aggression and called for continued cooperation.

"Due to the close collaboration and training, not only can we prevent cyberattacks, but also recover the systems quickly and keep business processes running after cyberattacks, which is no less important," - SSSCIP Deputy Head Viktor Zhora

CISA Director Praises Collaboration with Ukrainian Counterparts

In a keynote at the Black Hat conference on August 10, Jen Easterly and SSSCIP Deputy Head Viktor Zhora discussed Western support for Ukraine's fight against Russia's invasion. Director Easterly pointed out that the United States has learned from Ukraine how to deal with an active cyberwar, just as Ukraine has learned from America. Zhora mentioned that the ability to learn from and train with U.S. and EU information security professionals had been crucial in protecting core systems. This has ensured that Ukrainian citizens can have a normal life without losing the technology that makes civil life function. The collaboration has also shown how private companies can effectively work with governments to strengthen online defenses.