Global trends

The primary focus in the first quarter of 2024 was the vulnerability of the Ivanti Connect Secure zero-day exploit, which the Chinese group exploited for cyber espionage. Discovered in January 2024, this vulnerability remained significant throughout the entire first quarter. During this period, several security agencies, including the American Cybersecurity and Infrastructure Security Agency (CISA), British National Cyber Security Centre (NCSC), European Union Agency for Cybersecurity (ENISA), Computer Emergency Response Team for the EU institutions, bodies and agencies (CERT-EU), and the Five Eyes Alliance cyber security agencies, issued a series of urgent directives and notifications to consumers across various sectors, ranging from federal agencies in the USA to industry, in order to mitigate the scale of the problem. The threat remains relevant, as threat actors may actively exploit this vulnerability to maintain their presence in affected systems. The U.S. National Security Agency (NSA) confirmed that attackers are already using this vulnerability to target defense sector enterprises, and CISA even had to disconnect several of its systems to prevent cyber-attacks. To address these threats from a strategic perspective, the Pentagon promptly approved a separate Cybersecurity Strategy for the Defense Industry Sector.

A notable event during the quarter was British law enforcement's successful operation conducted against the formidable ransomware group LockBit. Using the LockBit ransomware, this group is responsible for a considerable number of ransomware attacks globally, and disrupting their activities will help curb the upward trend of such attacks. The Ukrainian police reinforced British law enforcement efforts by apprehending two LockBit group members. Overall, this marks law enforcement agencies' second significant success in combating major ransomware groups. In the fourth quarter of 2023, American law enforcement dismantled another group, Hive, and efforts to locate its leaders are ongoing. The U.S. Department of State has even announced a reward for information leading to their capture.

Despite these concerted efforts, ransomware remained a significant threat throughout the reporting period. The average initial ransom amount demanded by ransomware operators in 2023 already reached $600,000, and cybercriminals continue to target new sectors, such as the entertainment and casino industries.

This publication was made possible through support provided by the U.S. Agency for International Development, under the terms of Award to the Ukrainian Foundation for Security Studies within the USAID Cybersecurity for Critical Infrastructure in Ukraine Activity. The author's views expressed in this publication do not necessarily reflect the views of the United States Agency for International De velopment or the United States Government.

Relations between the USA and China in the field of cybersecurity are increasingly taking on the characteristics of intense rivalry, reminiscent of the early 2000s. In February 2024, hearings before the House of Representatives' Select Committee on the Chinese Communist Party highlighted the growing concerns of U.S. security agencies regarding Chinese cyber activity. Some of the speeches featured harsh assessments of Chinese hacker groups' actions (such as the Volt Typhoon group), which significantly deviate from cyber espionage activities in favor of direct attacks on critical infrastructure objects or establishing preparatory positions in the event of a large-scale conflict (using the «Living-Off-the-Land» attack method).

The Volt Typhoon group was first identified by Microsoft in May 2023. In February, U.S. cybersecurity agencies and allies such as Australia, New Zealand, Canada, and the UK issued joint guidelines, which state that China not only collects information and engages in espionage activities but also infiltrates U.S. and allied networks to disrupt critical infrastructure operations to create chaos, possibly during a Chinese attack on Taiwan. According to CISA Director Jen Easterly, after warning and joint operations by different countries, their activities did not cease. In March, cybersecurity agencies issued another set of guidelines aimed at «providing critical infrastructure facility leaders with guidance to help prioritize critical infrastructure protection and their functions.» Another threat from Chinese cyber activity is a potential attack on military bases in Guam. American security agencies are concerned that Chinese cyber-attacks could have a significant impact on its operations.

The escalating tension is increasingly evident not only in the relationship between the U.S. and China but also between Europe and China. This was particularly noticeable in March 2024 with a series of accusations leveled against Chinese hacker groups for interfering in the operations of parliamentary structures worldwide:

- The U.S. Department of Justice concluded that Chinese hackers targeted European lawmakers, including members of the Inter-Parliamentary Alliance on China
- The British government formally accused China of cyber-attacks on democratic institutions in the UK
- Finland attributed the breach of its parliament to the Chinese group APT31
- The New Zealand government accused China of cyber-attacks against the country's parliament in 2021

It is evident that such hacker activity is also linked to the numerous electoral processes taking place in democratic countries in 2024, and

countries are concerned about potential electoral interference. In response, ENISA updated its guide to securing the electoral process, and CISA worked on election process protection procedures, exemplified by «Super Tuesday» in March 2024.

Trends and forecasts

Given the critical role that satellites play in global communication, navigation, and security systems, the United States is increasingly concerned about the cybersecurity of space assets. There is growing recognition that they could become targets for cyber-attacks by adversaries, which could lead to signal interruption, interception, or complete satellite shutdown. To address this issue more systematically, CISA plans to assess the need for new security requirements for space assets and expand incident response capabilities. Additionally, in the event of an attack, CISA aims to bolster support for critical infrastructure dependent on space-based capabilities. Lawmakers in the U.S. Senate introduced legislation to enhance satellite cybersecurity by requiring CISA to develop relevant online resources and the White House to create a federal strategy to combat cyber threats to satellite systems. However, its consideration is still in the early stages.

Although the debate about the extent of Artificial Intelligence's (AI's) impact on cybersecurity continues, nearly all organizations point to it as a factor reshaping the cybersecurity landscape. Criminals are preparing to use Generative AI (GenAI) to generalize the data they have already stolen and effectively create new attack vectors or ransomware opportunities. Defenders are exploring opportunities to leverage AI more broadly for cyber threat analysis. At the same time, experts point out certain conceptual challenges on this path, including related to the data sets used to train AI. The UK NCSC believes that over the next two years, AI will increase in application scope and strengthen the impact of cyber-attacks.

The challenges of quantum computing and post-quantum encryption are once again troubling security structures. For instance, as NATO adopts its first quantum strategy, cybersecurity bodies in European countries emphasize the need to pay more attention to this issue and not be distracted by approaches that are dubious in terms of effectiveness, such as quantum key distribution (QKD). The U.S. NSA is initiating open discussions on the future of quantum computing and its impact on security, while IBM believes that there will be more cyberattacks in 2024

aimed at stealing encrypted data in hopes of gaining access to their content with the advent of quantum computers.

Government concerns about offensive actions in cyberspace have also affected the commercial sector. In February, the UK and France jointly held the inaugural conference dedicated to combating the threat of commercial cyber proliferation: the uncontrolled dissemination of tools created by commercial firms for unlawful purposes, which could be used in offensive cyber operations. As a result, participants signed the Pall Mall Process declaration, which outlines the initiative's plans to explore alternative policies and innovative methods to combat this threat. Currently, Israel is barely participating in these initiatives, as Israeli companies hold a significant share of the export market for spyware.

Cybersecurity threats to Operational Technology (OT) are not only persistent but also becoming increasingly systemic. Equipment and OT solution manufacturers are frequently discovering new vulnerabilities in their products. In February alone, Siemens identified 275 vulnerabilities in its products actively used in industrial automation processes. The Dragos Inc. report confirms that malicious actors are increasingly targeting this relatively new domain; in 2023, three more cyber groups focused on OT infrastructure emerged (Dragos currently tracks 21 such groups). The challenges extend beyond vulnerability detection to attempts to rectify them, and studies have shown that organizations with OT systems often know about flaws exploited in their environment but struggle to address the issue due to the expiration of warranties on some outdated systems and the complexities of technical processes or business interests that hinder updating these assets to the latest operating systems.

Incidents involving the physical security of underwater cables can have long-term consequences for the global availability of the internet. This quarter, attention was drawn to the issue of underwater cables by an incident in which four major data transmission underwater cables serving Africa were severely damaged in the area of Cote d'Ivoire just weeks after another cable was ruptured near Yemen. This affected internet access in Africa as well as data exchange between Africa and Europe. To prevent long term consequences, the European Commission issued recommendations on the security and resilience of underwater cable infrastructure, which include improving coordination within the EU, in terms of both management and financing.

United States of America

Against the backdrop of escalating strategic rivalry between the U.S. and China, concerns are mounting in the U.S. about the presence of Chinese components in its port infrastructure. According to the U.S. government, 80% of ship-to-shore cranes handling goods in U.S. ports are manufactured in China. Congressional investigations into Chinese-made cargo cranes have uncovered communication equipment that appears to be unnecessary for their normal operation, posing a potential hidden risk to national security. While lawmakers have sent a letter to the Chinese company manufacturing these cranes demanding explanations, President Biden announced in February his intention to issue an Executive Order aimed at strengthening the security and cybersecurity of American ports, which will expand the authority of the Department of Homeland Security in this area.

After a series of cyberattacks against water supply and sewage systems in the U.S. and the UK in December 2023, the organizations responsible for them have come under scrutiny from both security agencies and lawmakers. Despite this attention, attacks on this sector have not ceased. In January, the British Southern Water, which provides water supply services to 2.5 million consumers and wastewater services to 4.7 million clients in the southern regions of England, was targeted. By mid-January, CISA and its partners published an Incident Response Guide for the water supply and sewage sector to help organizations enhance their cybersecurity. However, the owners of such companies say that they often lack the resources for cybersecurity measures altogether. The White House has also gotten involved, announcing plans to establish a new working group aimed at protecting the water sector from state-sponsored cyberattacks. Analysts are also working on this issue, proposing that the government implement support and incentive measures to help companies ensure adequate cybersecurity levels.

February and March 2024 proved to be a test for the American healthcare system. In late February, hackers from Blackcat launched an attack against the Change Healthcare system (part of the UnitedHealth Group), which processes approximately 50% of medical claims (insurance) in the United States, including about 900,000 doctors, 33,000 pharmacies, 5,500 hospitals, and 600 laboratories. The attack had negative consequences for the entire country's healthcare system, which heavily relies on insurance. The Department of Health and Human Services announced an investigation into the incident, and the U.S. Department

of State offered a $10 million reward for information about the Blackcat group. The attack occurred against the backdrop of discussions about the need to strengthen cybersecurity requirements in the medical sector, to the extent of an idea proposed in January 2024 to link budget funding for hospitals to their confirmation of implementing cybersecurity measures. Overall, attacks on hospitals have become commonplace, as have patient data breaches. Attackers seek new tools not only to conduct attacks but also to compel the attacked entities to pay ransoms, extorting both the attacked organizations as well as patients. The federal government is becoming less tolerant of such payments. At the same time, even private companies (such as Palo Alto Network) are beginning to issue guidelines for healthcare facilities.

European Union

The EU is in the final stages of adopting the Cyber Resilience Act, which is expected to bring significant changes to security regulations throughout the EU. This initiative is supplemented by the development of measures to regulate the use of AI. The European Parliament is planning to pass an Artificial Intelligence Act that will regulate AI based on potential risks and impacts. While the primary focus of EU leadership remains on strengthening cyber resilience, analysts are assessing how existing cybersecurity structures, such as the Computer Security Incident Response Team (CSIRT), can be more effective in ensuring cybersecurity on a pan-European scale. One of the key findings suggests that these organizations should take a more proactive approach in their operations.

In the first quarter, the first European certification scheme for ICT products based on the Common Criteria came into operation. It incorporates elements of various national certification schemes and aims to make the use of IT products safer for European consumers. Currently, the scheme is still in the introduction process, but the EU has high hopes for it and its further development.

Cybersecurity in Ukraine

In March 2024, the leadership changed at the National Security and Defense Council of Ukraine (NSDC of Ukraine), the key coordinating and supervisory body of Ukraine, including in the field of cybersecurity. During the presentation of the newly appointed NSDC of Ukraine Secretary, Oleksandr Lytvynenko, the Ukrainian president identified information security and cybersecurity among the five new priorities. According

to NSDC of Ukraine Deputy Secretary Serhii Demediuk, based on its experience in cyber warfare with the russian federation, Ukraine is no longer a testing ground for russia's capabilities but can and should become a regional leader in cybersecurity, initiating changes in international approaches to aggression in cyberspace.

Hostile cyber activity against Ukrainian IT systems continues. In January, several particularly powerful cyberattacks were carried out: one targeted a banking center and another that significantly affected one of Ukraine's largest data centers. The latter led to disruptions in the availability of services for several government organizations and information systems. russian hacker groups continue to conduct cyber espionage operations against Ukraine, including one against Ukrainian military tracked by Securonix Threat Research, or attack government websites, such as the Ministry of Education's website.

Overall, these data correlate with the general increase in russia's cyber activity against Ukrainian information systems. According to the State Service of Special Communications and Information Protection (SSSCIP), the number of cyber incidents last year increased by 62.5%, and the number of incidents processed by the Government Computer Emergency Response Team Ukraine (CERT-UA) increased by 15.9% compared to 2022, totaling 2,543 cyber incidents. The most common types of incidents include malware distribution, phishing, malicious connections, account compromise, and system compromise. Attackers traditionally conduct reconnaissance operations, engage in long-term espionage, and destroy data and information systems.

In response, Ukraine has taken countermeasures, such as military intelligence actions against one of russia's IT system suppliers for industry. In the first quarter of 2024, Ukraine's Main Intelligence Directorate (HUR) reported an attack on a russian drone management system, resulting in russians losing access to servers. The Security Service of Ukraine (SBU) also emphasized the importance of cyber intelligence gathered for conducting complex kinetic operations. In March, Ukrainian cyber experts carried out a series of successful attacks on russian resources. As a result of the UA25 hacker group's actions, five terabytes of personal and corporate confidential information were extracted, including logistics materials related to russia, lawyer materials, and data from certain marketplaces. On March 11-18, HUR also targeted private and state structures financing the war against Ukraine. The losses from these attacks could amount to hundreds of thousands of dollars. HUR also conducted a successful special operation against

the russian federation Ministry of Defense, gaining access to servers and a massive amount of classified documentation. SBU cyber experts halted the supply of components for russian drones and cruise missiles and are working on the front lines to destroy enemy electronic warfare and reconnaissance systems and intercept drones coordinating missile and artillery strikes against the Ukrainian Armed Forces.

These efforts are complemented by traditional measures aimed at detecting and apprehending cybercriminals. For instance, in February, two international criminals were apprehended. Through a joint operation, the SBU and law enforcement agencies of the USA, UK, EU, and other partner countries exposed members of the powerful international extortion group LockBit. To prevent further large-scale attacks, Ukrainian cyber experts are actively studying the consequences of the massive cyberattack against the telecommunications operator Kyivstar in 2023. According to the SBU, russian hackers were preparing for a second wave of attacks, intending to cause even more damage to the operator.

Collaboration with international partners is essential. Ukraine anticipates receiving $13 million in cyber assistance from Denmark, while the United States Agency for International Development (USAID) is helping to bolster cybersecurity in the energy sector. However, the Tallinn Mechanism was launched to streamline coordination of joint efforts, holding its inaugural session in The Hague in mid-February.

On February 7-8, Kyiv hosted the inaugural Kyiv International Cyber Resilience Forum 2024: «Building Resilience in Cyber Warfare.» Organized by the National Cybersecurity Coordination Center (NCSCC) under NSDC of Ukraine in collaboration with partners, the forum drew over 1,000 participants, including high-ranking officials from Ukraine, the USA, EU, and NATO. Featuring 10 panel discussions and more than 40 expert presentations, the event covered various topics, including the role of cybersecurity in modern warfare, Ukraine's cyber warfare experience, cyber warfare and international law, cyber diplomacy, enhancing national cybersecurity resilience through education, messenger security, the importance of cyber threat intelligence, cybersecurity in regional contexts, and more. The forum also included cyber security competitions with 21 teams of experts from both the public and private sectors participating.

In the first quarter, the first European certification scheme for ICT products based on the Common Criteria came into operation. It incorporates elements of various national certification schemes and aims to make the use of IT products safer for European consumers. Currently,

the scheme is still in the introduction process, but the EU has high hopes for it and its further development.

The First World Cyber War

russian federation attacks continue on a wide range of targets, both related and unrelated to Ukraine. In January, several cybersecurity companies and departments at large companies were attacked, including Microsoft, which fell victim to an attack by the russian state-sponsored attacker Midnight Blizzard. The extent of the Midnight Blizzard group's cyber intrusions is still not fully understood; currently, Microsoft has only confirmed that the attackers were able to access some of its source code repositories and internal systems. The attack also affected some email accounts of high-ranking U.S. officials, prompting CISA to conduct its own investigation and take measures to mitigate the consequences.

At the beginning of February, the Mandiant cybersecurity company's account on the X network fell victim to attackers. Over a short period of time, the attackers used it to promote fake cryptocurrency operations. Hackers associated with the Kremlin also targeted email accounts for the cybersecurity department of the technological giant HP Enterprise. In February, it became known that the Russian cyber group Turla had targeted a Polish non-governmental organization (NGO) supporting Ukraine starting in December 2023. As of March, cybersecurity companies continue to investigate this operation.

russian hackers have also targeted political parties in Germany and are actively testing a virus designed to destroy data in the infected system, the wiper AcidPour, a modification of AcidRain that was used at the beginning of the military invasion against KA-SAT modems. It appears that the updated virus is aimed at Linux x86 systems and may have been used against a number of telecom operators in Ukraine. The focus on political parties may serve as additional evidence of russia's intention to actively interfere in electoral processes in Germany.

Western researchers continue to study russian actions in cyberspace and provide their own forecasts and recommendations for preventing them. For instance, civil society organization (CSO) Online describes the structure and operational methods of the pro-russian hacktivist group NoName057(16) and asserts that such an organization could become a model for cybercriminals in the future. However, the publication emphasizes that the group's activities, which primarily focuses on distributed denial-of-service (DDoS) attacks, do not currently pose

a serious threat to the West. Researcher Monica Kello argues that public shaming and sanctions employed by Western governments today, in an attempt to influence russia's actions in cyberspace, are not effective. In her view, the response should be based on russia's strategic culture and include transparent investigations into the consequences of russian hacking operations and leaks, leveraging the distrust prevalent in russian intelligence services and society to introduce «friction» into the adversary's operational environment.