Global trends

The ongoing global competition between the United States and China in the digital realm persists. Chinese Advanced Persistent Threat (APT) groups are intensifying their cyber-espionage operations, targeting both government entities (as seen in a significant campaign against Cambodian government agencies) and the private sector, particularly semiconductor companies in East Asia. According to research from the RAND Corporation, the rivalry between the United States and China for control over digital infrastructure will play a pivotal role in military forces and operations within the region. Concurrently, China is expanding its strategic objectives and displaying increased interest in critical infrastructure. The perceived threat is underscored by a study conducted by Fortress Information Security, revealing that nearly all software utilized by U.S. energy companies incorporates code from Russian and Chinese developers, potentially harboring critical vulnerabilities that can remain dormant for over four years. Security agencies in the United States, including the NSA, CISA, and the Department of Defense, caution that a kinetic attack on Taiwan could coincide with a simultaneous assault on U.S. critical infrastructure, particularly military critical infrastructure. Moreover, China's cyber activities now encompass influence operations leveraging artificial intelligence and disinformation. Meta reports that both China and Russia are anticipated to establish online influence networks in advance of upcoming U.S. elections.

The perpetually evolving cyber threat landscape includes persistent risks to critical infrastructure. Such entities remain attractive targets for attackers due to their financial resources and the imperative to avoid business disruptions. While a majority of attacks focus on the Information Technology (IT) systems of these organizations, primarily through ransomware (with 75% of industrial sector organizations falling victim to ransomware attacks last year), the impact extends to critical organizational functions such as timely delivery and customer interactions. However, the scope of successful cyberattacks goes beyond conventional targets like an Australian port or a municipal water supply plant, as attackers increasingly seek opportunities to compromise industrial systems, particularly Operational Technology (OT) environments, rather than solely focusing on owners' IT systems. This introduces a significant challenge, as OT systems are often less secure than their IT counterparts, lacking security updates for many controllers. Alarmingly, owners of industrial systems often underestimate cyber threats, evident in the presence of nearly 100,000 indus-

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 Development or the United States Government.

trial control systems exposed to the public Internet. Moreover, vulnerabilities in these systems are emerging at an alarming rate, amplified by the discovery of new zero-day vulnerabilities in industrial routers. In the recent quarter alone, cybersecurity recommendations pertaining to various aspects of OT cybersecurity were issued by authoritative bodies such as CISA (providing open-source OT security recommendations and regular notifications of new vulnerabilities) and NSA (publishing the OT Intrusion Detection Signature and Analytics repository). Private cybersecurity organizations like Dragos, through initiatives like the Community Defense Program, offer free tools to small organizations to bolster the cybersecurity of their OT infrastructure. Presently, Ukraine lacks a precise estimate of the number of industrial facilities with vulnerable OT systems susceptible to intrusion. Additionally, there is a traditional shortage of financial resources for their protection. Hence, participation in programs such as the Community Defense Program is not only a potential solution for Western companies but also holds promise as an interim measure for Ukrainian entities.

Trends and forecasts

The concluding quarter of the year traditionally involves reviewing outcomes and making forecasts. In this quarter, Proofpoint, Trellix, and Trendmicro released their projections. Despite variations in emphasis, these companies highlight:

- The escalation of threats stemming from Artificial Intelligence (AI), particularly its exploitation by attackers for orchestrating phishing attacks and voice fraud. This trend underscores the need for companies to thoroughly contemplate the ethical considerations of AI usage and its implications for privacy.
- An upsurge in phishing attacks targeting mobile devices.
- Growing criminal focus on user accounts.
- Anticipated heightened cyberattack risks on election systems, voter databases, and election infrastructure, aligning with the upcoming U.S. elections.
- The increasing prevalence of concealed attacks on peripheral devices.
- Additionally, the cybersecurity talent gap is predicted to widen, although organizations have the potential to mitigate this gap by enhancing the skills of their existing workforce. Furthermore, large-scale ransomware attacks are anticipated to persist and proliferate, given their lucrative return on investment for threat actors.

These projections align with observations from the UK's NCSC, which underscores that Critical Infrastructures (CIs) are confronted with a "continuing and significant threat." This threat is compounded by the rise of state-sponsored groups and the overall escalation of aggressive cyber activities coupled with emerging geopolitical challenges. Across the board, an increasing number of companies are noting a heightened focus from attackers on social engineering. While "human attacks" were historically pivotal in the initial phases of cyberattacks, the advent of AI has injected new momentum into this realm. The capabilities of AI, such as crafting more authentic phishing emails, replicating human voices and videos, and dynamically managing numerous social media accounts, are profoundly reshaping the threat landscape.

Another facet of the assessments involves reflecting on the initial outcomes of the preceding year. Trendmicro was the pioneer in presenting such evaluations and highlighted the following points:

- The perceived impact of artificial intelligence, particularly ChatGPT, on the cybersecurity landscape was overstated, with noticeable effects primarily in the realm of phishing.
- Blockchain technologies have confined themselves to a modest niche, predominantly within the financial sector, and are no longer perceived as a groundbreaking technology in the cybersecurity domain.
- The proliferation of diverse cybersecurity tools within an institution often results in more challenges than enhanced security, as it complicates administration for organizational specialists.
- Despite people remaining the weakest link in cybersecurity, this vulnerability is exacerbated by a prevalent negative culture within organizations that discourages individuals from reporting cybersecurity issues.
- Organizations frequently formulate unrealistic requests for cybersecurity specialists, contributing to challenges in recruitment and contributing to a labor shortage in the field.

United States of America

In the fourth quarter of 2023, significant events unfolded with lasting implications for US cybersecurity policy. Notably, new leaders assumed key roles in two critical cybersecurity agencies. Harry Coker, a former CIA officer, took on the role of National Cyber Director, while Lieutenant General Timothy Haugh succeeded US Army General Paul M. Nakasone, who had led both agencies since 2018, as the head of CYBERCOM and NSA. These leadership changes re-

flect evolving agency policies. The Office of the National Cyber Director is increasingly dedicated to implementing the U.S. Cybersecurity Strategy and the Cyber Workforce Development Strategy. Simultaneously, NSA is expanding its guidance to a wide array of domestic organizations and enhancing its international engagements, actively participating in collaborative projects within the Five Eyes Alliance. These appointments took place against the backdrop of ongoing discussions about the potential separation of NSA and CYBERCOM and the broader trajectory of U.S. cybersecurity reforms aligned with the Solarium Commission's recommendations. Moreover, the recent formulation of a clear plan for implementing the US Cyber Security Strategy in practical American contexts suggests a heightened commitment from the White House to exert greater control over the document, delineate clearer responsibilities for its implementation, and establish a transparent mechanism for assessing its outcomes. The incoming head of the Office of the National Cyber Director is likely to prioritize these control and coordination functions.

Another significant focus is on the advancement and regulation of artificial intelligence (AI). In late October, U.S. President J. Biden signed a new Executive Order, prompting the US CISA to publish its roadmap outlining how this pivotal federal cybersecurity agency will address AI challenges in its operations. Collaboratively with the UK NCSC, they have also released joint recommendations for the secure development of AI systems. The increasingly defined stance of U.S. government agencies in relation to AI development underscores the noticeable impact of these technologies on the country's security sector, compelling states to swiftly establish their support and control mechanisms.

A third area of emphasis involves the ongoing battle against ransomware. The United States is now contemplating the next phase of this fight, aiming not only to combat the infrastructure of criminals or specific groups but also to alter the behavior of victims. This includes reinforcing measures to deter ransom payments, thereby avoiding incentivizing criminals to perpetrate malicious acts. Despite these efforts, ransomware groups continue to achieve significant success, targeting new entities. The healthcare sector remains a prominent target in the United States, with Sophos reporting that nearly three-quarters of attacks resulted in data encryption—a testament to the sector's inadequate attention to cybersecurity.

The fourth emphasis lies on partner engagement and the implementation of a zero-trust architecture. Aligned with the new Cybersecurity Strategy, the United States is broadening its network of global partners, actively seeking secure avenues to share information with trusted allies. Recent developments include

the signing of a working agreement between ENISA and CISA, as well as the establishment of a new partnership involving the US, South Korea, and Japan. Concurrently, US military agencies are exploring practical means of collaboration, with a specific focus on the Pacific region. U.S. CYBERCOM is expanding joint cyber exercises with regional partners, NATO is involving Japan and South Korea in its Cyber Coalition 2023 exercises, and the Pentagon is creating a dedicated Mission Partner Environment network for information sharing with the Philippines and Taiwan. These initiatives align with the cyber assistance the US intends to provide to Taiwan through its military budget in the forthcoming years, underscoring the primary concerns of the US military command in averting further escalation of global military tensions.

A new trend observed this quarter is the occurrence of cyberattacks targeting water supply systems in individual small communities in the United States. At least three such attacks occurred in two locations (with groups like Cyber Av3ngers, claiming responsibility), and a similar incident transpired in Ireland. While the companies asserted no threat to consumers (only users in Ireland experienced partial effects), the attacks highlight a consistent trend of hackers attempting to disrupt the functioning of critical infrastructure. These incidents underscore the vulnerability of local-level systems to cyber threats, showcasing a more pronounced shortage of personnel and financial resources for effective cyber defense compared to the central level. It is anticipated that local critical infrastructure facilities will increasingly be targeted by attackers seeking to demonstrate the central government's inability to protect all citizens.

A discernible trend persisting in the latest quarter is the heightened emphasis of cybersecurity organizations globally on developing new service functions and actively offering guidance to industry stakeholders. For instance, CISA is initiating a fresh program for exchanging cyber incident information with the private sector. Simultaneously, the British NCCC is regularly introducing new services and leveraging its expertise to cater to the needs of the private sector (for instance, in the last quarter, the British NCCC provided a roster of organizations offering proficient services for conducting technical tests at all levels). Notably, there is a pronounced surge in the activity of cybersecurity entities within the Five Eyes Alliance, regularly issuing joint messages on prevailing cyber threats almost every week. This underscores the seamless daily collaboration of these organizations, reflecting a high degree of trust in data exchange.

European Union

After nearly a year of deliberations, the European Union has initiated the adoption of the Cyber Resilience Act. This legislation establishes a new framework for the IT sector and manufacturers of IT equipment, mandating heightened attention to cybersecurity measures. The implementation of this act is expected to be complex and may unfold at varying speeds across European countries. This is evident from the experience with the NIS2 Directive, which, more than a year after its enactment, remains inadequately implemented in numerous European nations. Despite these challenges, the EU recognizes the escalating importance of cybersecurity and is prepared to allocate funds accordingly, with the latest proposal aiming to raise 214 million euros for cybersecurity. Furthermore, EU leadership has advocated for the creation of a European cyber force with offensive capabilities.

It is noteworthy that these initiatives, coupled with Brussels' commitment to investing in cybersecurity, exhibit limited correlation with the actual cybersecurity landscape within Critical Infrastructures (CIs). A November 2023 report from ENISA highlights that although the cybersecurity share of IT budgets for CIs reached 7.1% in 2022, this represents only a 0.4% increase from 2021. Additionally, 47% of Critical Service Providers (CSPs) do not anticipate hiring cybersecurity professionals over the next two years, while 83% of organizations report challenges in recruiting for at least one area of information security. Previous research by ENISA has indicated similar trends, with Chief Information Security Officers (CISOs) either unwilling to invest in cybersecurity or not deeming it necessary. Given these trends and the overall trajectory of recent regulatory changes in the EU, it is foreseeable that European cybersecurity legislation will become progressively stringent and imperious, with violations incurring significant fines for companies, akin to the consequences under the General Data Protection Regulation (GDPR).

Similar to the United States, the European Union is gearing up to conduct a comprehensive assessment of the risks associated with Artificial Intelligence (AI). The outcomes of this evaluation will serve as the foundation for crafting a regulatory framework and formulating policies aimed at mitigating risks, thereby fortifying the EU's standing in the global technological arena. The heightened focus on AI risks within the EU stems from the expanding utilization of AI-based technologies, spanning the creation of innovative applications to potential threats to autonomous systems governing maritime transport.

Russian cyber activity

Russian cyber operations show no signs of slowing down. With numerous elections scheduled worldwide in 2024, including in the United States and the United Kingdom, security agencies are alert to the preparations of Russian and Chinese APT groups gearing up to interfere in these events. This targeted cyber activity is underscored by recent research indicating that over 60% of Distributed Denial of Service (DDoS) attacks are now politically motivated. Cybersecurity experts emphasize that incident response teams must not only monitor their information systems but also stay vigilant to geopolitical events, which are emerging as catalysts for new threats affecting both public and private sectors.

In the recent reporting period, hostile activity persisted, with Russia's APT29 targeting embassies across Europe, and the UAC-0165 group attempting to interfere with 11 Ukrainian service providers. These incidents align with a report from the Ukrainian State Special Communications Service, highlighting that the number of registered cyber incidents more than doubled in the first half of 2023.

Cybersecurity in Ukraine

In October-November 2023, Ukrainian law enforcement agencies achieved notable success in combating international cybercrime groups. One significant accomplishment involved dismantling a group responsible for inflicting $80 million in damages through ransomware attacks. These achievements extend to collaborative efforts with Czech colleagues and an operation against a group that targeted 168 companies since 2020. The international recognition of these efforts aligns with the global concern over ransomware threats. Substantial contributions to countering this menace can foster trust between Ukraine and partner countries, potentially catalyzing the initiation of more coordinated measures to combat cybercrime systematically.

The ongoing development of international cooperation remains a pivotal aspect of these efforts. In November 2023, Ukraine, represented by the NCCC of the National Security and Defense Council and the the State Service of Special Communications and Information Protection of Ukraine (SSSCIP), signed a Working Agreement on Cooperation with ENISA. This marked ENISA's first such agreement with a non-EU partner. While the signing of such documents is a crucial step in forming a global cyber coalition against threats originating from Russia and aligned aggressor states, it is imperative to back this cooperation

with tangible actions and measures on the Ukrainian side. The effectiveness of collaboration will hinge significantly on Ukraine's commitment not only to proposing a clear roadmap for cooperation but also to actively advancing it.

In December 2023, Ukraine faced another significant cyber onslaught from Russian cyber forces, targeting one of the national mobile operators, Kyivstar. The impact of the attack was severe, resulting in a communication blackout for the company's subscribers lasting several days, with the recovery process spanning several weeks. This incident underscores that the absence of destructive cyberattacks over the two years of war is not solely attributed to robust cyber defense but possibly indicates the presence of undetected adversary hackers within information systems. Russian hackers remain active, aligning their actions with the broader Russian military strategy, such as simultaneous attacks on Ukraine's agricultural sector alongside missile strikes. The patterns of APT groups opposing Ukraine appear relatively unchanged. It might be prudent for Ukraine to enhance coordination between cybersecurity agencies and major telecom operators, considering a format similar to the U.S. CISA, which includes a dedicated committee comprising CISA representatives and telecom industry stakeholders.

Ukrainian cybersecurity agencies, including the SSSCIP and the Security Service of Ukraine (SSU), have recently provided assessments of the current cyber threat landscape in Ukraine, along with forecasts for the near future. These assessments highlight an anticipated rise in sophisticated attacks targeting supply chains, particularly focusing on companies involved in developing software for critical infrastructure and the military. Long-term projections suggest an active and targeted threat environment for these sectors. A significant portion of hostile cyber activity is currently directed at accessing the electronic document flow of Ukrainian government agencies and technological infrastructure systems. In light of this, the SSU and the SSSCIP have alerted energy companies to increased cybersecurity threats from Russia during the winter months. Drawing from past experiences, these security agencies point to the likelihood of Russian hackers actively attempting to influence critical information infrastructure, the energy sector, and the provision of vital services. While supply chain threats are recognized as critical to Ukraine's cybersecurity, there is a notable absence of straightforward guidance on how private companies or government agencies can safeguard themselves against such threats. The complexity is exacerbated by the limited availability of experienced professionals capable of independently implementing existing international standards or recommendations in this domain.

To address this challenge, cybersecurity agencies in the UK, US, and France are working on simplified guidelines and automated tools, such as MITRE, aimed at non-specialists. In Ukraine, efforts to enhance cyber incident response capabilities are ongoing. This includes the expansion of cyber exercises, the launch of new cyber hygiene tools, and initiatives to stimulate innovation within the cybersecurity sector. Examples include cybersecurity competitions like the NCCC's HackWave, INCIDENT RESPONSE DAYS 2.0, and the first sectoral cyber exercise for the transport sector, CIREX CoBridge. Additionally, the Ministry of Digital Transformation introduced a security rules knowledge test in the Cybergram network, while the SSSCIP organized an all-Ukrainian online cybersecurity lesson with over 20,000 viewers.

The First World Cyber War

The ongoing First World Cyber War continues, and the aggressor shows no signs of reducing its intensity. According to Microsoft, in 2023, authoritarian governments such as Russia, China, Iran, and North Korea are intensifying their focus on cyber-espionage operations to gather information about critical foreign policy initiatives. These activities are not limited to targeting Western companies and governments, as indicated by Solar, a Russian state-owned company, which reports that China and North Korea are significant sources of offensive cyber campaigns against Russia in 2023.

Russia's cyber aggression is extending to disrupt the logistics of Ukraine's international partners, involve in information theft from diplomatic missions, and attack critical infrastructure. While the majority of these attacks still involve DDoS attacks by groups like Killnet or Anonymous Sudan, there is an increasing involvement of APT groups. As 2024 approaches, a year with the highest number of elections in history, it is anticipated that Russian malicious actors will target electoral infrastructure and pre-election discussions. Key elections to be impacted include the US presidential election, European Parliament elections, UK Parliament lower house elections, and elections in several other critical European partner countries of Ukraine.

Attacks on CIs remain a significant objective of Russian cyber operations, exemplified by Mandiant's report on the Sandworm group's cyber assault on the operational technology (OT) systems of a Ukrainian energy company in late 2022. The actor employed OT-level live-off-the-land (LotL) techniques to likely disrupt the victim's substation circuit breakers, leading to an unplanned power outage coinciding with extensive missile strikes on critical infrastructure throughout Ukraine. Notably, Russian criminal groups are increasingly targeting

the energy sector globally, as seen in the coordinated cyberattack on 22 Danish energy companies in May 2023, suspected to involve the same Sandworm (APT28). In response, both Ukraine and its partner countries are not merely adopting defensive measures but are actively engaging in counterattacks. Ukrainian special services, particularly the Defense Intelligence of Ukraine, executed successful cyber operations against Rosaviatsia and the central servers of the Russian Federal Tax Service. These operations resulted in acquiring classified documents from Rosaviatsiya and disrupting the configuration files integral to the extensive tax system of the Russian Federation. This shift indicates a broader evolution in the cybersecurity discourse, moving beyond a paradigm of attack and defense to one of equal competition, wherein defenders can launch counterattacks and assume an offensive posture.

Globally, there is ongoing debate about the creation of cyber forces as distinct military branches and their integration into effective joint operations with other military branches. Major General Murray Thompson of the Australian Ministry of Defense has called for a reevaluation of defense sector tasks, drawing parallels to the creation of the Air Force in 1918. In Ukraine, discussions are also underway about establishing Ukrainian cyber forces. N. Tkachuk, secretary of the NCCC under the National Security and Defense Council of Ukraine, during the interdepartmental event on “Ensuring cyber defense of the state” emphasized the need for the fastest possible creation of Ukrainian cyber forces based on the Ukrainian experience and successful international cases. Additionally, there are proposals, such as the one from the President of the EU Council, advocating for the formation of a “European cyber force” with “offensive capabilities,” though such proposals are yet to garner support from EU defense ministers.