Aspen Institute Germany

Security Network Munich

The Cyber Conundrum:

Cyber Threats and Resilience in a Changing Geopolitical Environment

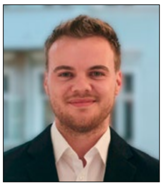
www.it-security-munich.net

Cyber Security Study
published by
Aspen Germany
in corporation with
Security Network Munich

AN OVERVIEW

The cybersecurity landscape of 2024 is defined by rapid technological evolution and the increasingly sophisticated nature of cyber threats, which now permeate every aspect of society, as well as a changing geopolitical environment. Attackers are leveraging Artificial Intelligence (AI) and machine learning to automate attacks, evade detection systems, and optimize the effectiveness of their campaigns. The intersection of AI and cybersecurity is characterized by a continuous arms race between cybersecurity professionals and cybercriminals, making AI both disruptive and indispensable. At the same time, nations find themselves at a critical juncture, facing adversaries keen on leveraging the cyber domain to exploit technological vulnerabilities. These developments call for comprehensive risk assessments, continuous monitoring, and collaborative security practices among all stakeholders to mitigate vulnerabilities and become more resilient. The intricate relationship between national security, public order, defense, and cybersecurity underscores the imperative of fortifying digital frontiers and the urgent need for international collaboration.

AUTHORS:



Driss Köhler is Junior Program Officer at the Aspen Institute Germany and part of the Institute's Digital Program. Here, he is responsible for the conception, design, and implementation of the Institute's high-level events and publication formats on the most pressing digital topics. He primarily works and writes on geopolitics and geoeconomics, primarily focusing on transatlantic trade and technology relations. Before joining Aspen, Driss worked in the German Bundestag and at a consulting firm, focusing on public affairs mandates in EU regulation, digital, and cyber. Driss holds a Master's Degree in International Affairs from the Hertie School of Governance and a Bachelor's Degree in Public Governance from the University of Münster and the University of Twente.

In January 2021, Dr. Stormy-Annika Mildner (M.Sc.) became Director of the Aspen Institute Germany in Berlin, a renowned policy-oriented think tank focusing on transatlantic relations and issues of global importance. As an adjunct professor, she teaches political economy at the Hertie School. From 2014 to 2020, she served as head of the department External Economic Policy at the Federation of German Industries (BDI), where she was responsible for international trade and investment issues. As Sherpa, she spearheaded the German Business7 Presidency (2015) and the German Business20 Presidency (2016-2017). Prior to joining BDI, she was Member of the Board of the German Institute for International and Security Affairs (SWP), worked as a lecturer at the John F. Kennedy Institute of the Free University of Berlin, and headed the program Globalization and the World Economy at the German Council on Foreign Relations (DGAP). She completed research fellowships at the American Institute for Contemporary German Studies and the Transatlantic Academy of the German Marshall Fund in Washington. She earned a Master of Science in international political economy from the London School of Economics and a PhD in economics from Freie Universität Berlin. During her doctoral studies, she conducted a one-year fellowship at the Yale Center for International and Area Studies (YCIAS) at Yale University.

The Changing Cyber Threat Landscape in a New Geopolitical Environment

The 21st century has witnessed an unprecedented escalation in cyber threats, necessitating robust cybersecurity measures to protect national assets and sensitive information. Both, the number of financially and politically motivated cyber-attacks has risen considerably. While the threat of cyber-attacks carried out by non-state and state actors is nothing new, the changing geopolitical environment is heightening the risks considerably.

The geopolitical landscape is fraught with political uncertainty, social fragmentation, and escalating tensions. The most recent Conflict Barometer of the Heidelberg Institute for International Conflict Research counts an increased number of over 360 conflicts worldwide with about 60 percent being fought violently. Moreover, great power competitions and protectionism each influence the cyber domain in profound ways. The Freedom House Index 2024 finds that "armed conflicts and threats of authoritarian aggression made the world less safe and less democratic." Shared democratic principles and norms of sovereignty and self-determination are being subverted by authoritarian aggressions made by China, Iran, Russia, and others, the report finds.

These conditions have also fundamentally altered the cyber threat landscape, intertwining geopolitics and cybersecurity more closely than ever. According to a poll by the World Economic Forum (WEF), 70 percent of cyber leaders cite geopolitical concerns as at least moderately influencing their organization's cybersecurity strategy.

Between July 2022 and June 2023, more than 120 countries faced nation-state cyberattacks, according to Microsoft's Digital Defense Report, with Ukraine, Israel, South Korea, and Taiwan the most targeted countries.

From 2000 to September 2024, the European Repository of Cyber Incidents (EuRepoC) documented 3,180 cyberattacks with political motives worldwide, executed by 747 identified actors or groups. The documented incidents encompass attacks targeting political entities and critical infrastructure, executed by both state-linked entities and non-state actors with political agendas. As of 2023, nearly 12 percent of politically motivated cyberattacks have originated from China, closely followed by Russia at 11.6 percent. Iran and North Korea accounted for 5.3 percent and 4.7 percent of these incidents, respectively. Notably, 45 percent of these attacks could not be traced back to any country.

As highlighted in the European Union Agency for Cybersecurity's (ENISA) Threat Landscape Report 2023: Chinese state-sponsored cyber groups continue to target China's rival territorial claimants, and the volume of espionage campaigns is expected to rise. A joint U.S. cybersecurity advisory by the Cybersecurity & Infrastructure Security Agency (CISA), the National Security Agency (NSA), and the Federal Bureau of Investigation (FBI) assesses that Chinese state-sponsored actors compromise and maintain persistent access to U.S. critical infrastructure and are "seeking to pre-position themselves on IT networks for disruptive or destructive cyberattacks against U.S. critical infrastructure in the event of a major crisis or conflict with the United States".

Moreover, cyber groups associated with Russia employ high speed and volume to target the Ukrainian government and fracture support for Ukraine internationally, highlighting the key role information manipulation plays in Russia's security strategy. In addition, thousands of cyberattacks were directed at the European energy grid in an effort to cause economic instability and disrupt operability.

Iran, emerging as a major cyber threat actor, was attested a "growing expertise and willingness to conduct aggressive cyber operations" by the U.S. Office of the Director of National Intelligence's 2023 Annual Threat Assessment. Iranian state-sponsored cyberattacks also play a major role in the wider regional conflict in the Middle East, sparked by the attack of Hamas on Israel on October 7, 2023. Google's recent report on the Israel-Hamas War in Cyber found evidence that Iran was "aggressively" targeting Israeli and U.S. entities.

This development highlights the new reality of hybrid warfare, where the realms of geopolitics and cybersecurity are closely intertwined, showcasing the strategic integration of cyberattacks in geopolitical conflicts.

In 2023, critical infrastructure was the primary target of malevolent cyber actors with a political agenda, according to data from ERCI as reported by Statista, followed by state institutions and political systems, and corporate targets. Breaking down the attacks on critical infrastructure, the data shows that between January 2023 and March 2024, the healthcare sector was the most affected, suffering 14.2 percent of attacks. Financial organizations also represent a significant portion of these attacks, accounting for 8.3 percent since the beginning of 2023. Other frequently targeted sectors include telecommunications, transportation, and energy, highlighting the broad scope of the threat across various essential services.

While the number of politically motivated attacks is increasing, overall, the motivations of cyber attacks vary. The WEF assessed a worrying rise of ransomware activity of up to 50 percent in the first half of 2023, while the number of cases in which data is exfiltrated has also doubled from 2019 to 2022. For instance, in 2021, Ireland's Health Service Executive (HSE) was targeted by a ransomware attack in the midst of the Covid-19 pandemic. This attack, as later assessed by an independent PwC Post Incident Review, triggered a series of events, leading to a temporary nationwide shutdown of IT systems that significantly disrupted patient care. The shutdown was a preventive measure to contain and assess the impact of the cyberattack. The UK's National Cyber Security Center anticipates that the worldwide ransomware threat will intensify over the next two years as AI amplifies the effectiveness of cyber operations and their associated risks.

To this day, the SolarWinds cyberattack in 2020 serves as a stark example of supply chain vulnerabilities in cybersecurity. Hackers infiltrated the software supply chain by inserting malicious code into SolarWinds' software, which is widely used for network management. As organizations globally updated their systems with the compromised software, the attackers gained access to the networks of thousands of SolarWinds' customers, including United States government agencies and major corporations.

Cyber Warfare and National Security

The changing geopolitical environment brings to the forefront the critical nature of cyberwarfare and espionage in undermining national security and economic stability. For instance, China has escalated its cyber operations against U.S. military targets, notably compromising Fortinet devices to gain extensive access to U.S. military systems, enabling potential actions against critical infrastructure near U.S. bases in places like Guam. Additionally, China has expanded its espionage activities across the South China Sea region, targeting Taiwan and major Southeast Asian countries, with a specialized focus on undermining Taiwanese critical infrastructure and defense sectors to collect strategic information that could be exploited during physical conflicts. Russia's cyber activities have been similarly aggressive, particularly targeting Ukrainian communities globally with influence operations aimed at fostering hostilities against Ukrainian refugees, especially in Poland and the Baltic states. Alongside these influence operations, Russia has sustained extensive phishing campaigns against Ukraine and NATO member states. Russian state actors launched operations where they impersonated Western diplomats and Ukrainian officials, aiming to infiltrate accounts to gather intelligence on Western strategies regarding Ukraine, including defense strategies and war crimes investigations.

The escalating threat of cyberwarfare poses significant challenges to democracies especially. From a strictly operational standpoint, centralized cybersecurity governance in authoritarian regimes such as China, Iran, North Korea, and Russia allows for swift decision-making and effective resource allocation, often enabling a quicker response to cyber threats. This centralization of course comes at the cost of diminished checks and balances, restricted civil liberties, and increased susceptibility to errors and abuses from a narrow decision-making base. In contrast, the decentralized cybersecurity governance structures in many democracies can delay the detection, response, and coordination needed to address cyberattacks effectively. Furthermore, the complexity and interconnectedness of technological infrastructures in highly developed countries increase their susceptibility to significant disruptions when critical systems are compromised. This complexity not only makes it difficult to secure systems comprehensively but also complicates the coordination of cyber defense efforts across the multiple entities involved in national security.

The U.S. Department of Homeland Security warns that the challenges posed by the increased connectivity of devices and individuals expand the global attack surface and position cyberspace as the most dynamic threat domain. It thereby underscores the need for a unified, well-resourced approach to cyber defense against a complex threat landscape, populated by both state and non-state actors engaging in novel cyber campaigns to undermine national security interests.
The integration of cybersecurity within national defense mechanisms is pivotal for the protection of sensitive data and critical infrastructure, and for ensuring the military's operational readiness in a digitally interconnected world. The establishment of entities such as the United States Cyber Command underscores this strategic priority, with a dedicated global team of cyber experts tasked with defending military networks and national interests.

In its 2023 Cyber Strategy, the United States officially denoted the role of cybersecurity in defense as extending to protecting classified, sensitive, and mission-critical information from unauthorized access, thereby safeguarding the nation's sovereignty and security interests against cyberattacks on critical infrastructure and government systems. It is also crucial for defending against state-sponsored cyberattacks and ensuring the security of vital sectors such as energy, transportation, and healthcare, which, if compromised, could lead to national crises. Moreover, cybersecurity aids in counterintelligence efforts by identifying espionage attempts and securing military and governmental communications, ensuring their confidentiality, integrity, and availability.

Democracy under Stress:
Disinformation and Cyber Threats in Electoral Processes

More than two billion voters are expected to head to the polls in elections across nations in 2024; the respective countries contribute to over 60 percent of the world's economic output. Looking at the number of elections this year, the range of targets is the largest it has been since the dawn of the digital age. Democratic election processes are increasingly endangered by the pervasiveness of multifaceted and evolving cyber threats and the omnipresence of disinformation campaigns. And with the high political stakes of the 2024 super-election-year, countries like Russia, Iran, and China, seeking to advance their strategic goals, have an especially high interest in influencing elections, as their outcome may determine the future foreign policy course of major competitors and rivals. In fact, ENISA's Threat Landscape Report 2023 names Foreign Information Manipulation and Interference as one of the prime cyber threats in 2023. This activity, according to the European External Action Service, is manipulative in character and conducted in an intentional and coordinated manner by both state and non-state actors. Threat actors aim to alter democratic elections by impacting citizens' ability to vote and the information they use to make choices. Highlighting the upcoming U.S. presidential election, Microsoft's Threat Analysis Center assessed that the "election 2024 may be the first presidential election during which multiple authoritarian actors simultaneously attempt to interfere with and influence an election outcome". CISA Director Jen Easterly stated in 2024 that "we should absolutely expect that foreign actors will attempt to influence and that they will interfere" in the elections but emphasized that the strides made in preventing interference would win out.

A primary digital threat to the democratic integrity of elections is the strategic use of disinformation. The WEF's Global Risks Report 2024 named misinformation and disinformation as the most severe global risk anticipated over the next two years. Disinformation refers to false information deliberately created and disseminated with the intent to deceive or mislead. It is often used in political contexts to influence public opinion, manipulate social attitudes, or sway electoral outcomes. Disinformation campaigns are strategically designed, utilizing crafted messages that exploit existing biases or societal divisions, and are distributed through various media channels to achieve a specific malicious objective.

Disinformation adds another layer to the pervasiveness of digital threats to elections because even if election systems are robust, disinformation and public distrust can still lead to unrest, as evidenced by the post-election violence in the United States and Brazil.

While discussions on disinformation often focus on external state actors, there are also domestic sources or multiplicators of disinformation, as foreign-origin disinformation is distributed and amplified by domestic actors. In the EU, for instance, a 2021 study on disinformation and propaganda requested by the INGE committee of the European Parliament has pointed out how national political disinformation, conspiracy theories, and propaganda can be traced within the EU.

The challenge of combating disinformation is exacerbated by its ability to blend seamlessly into the regular information flow, often making it indistinguishable from legitimate news. The actors behind these campaigns exploit the anonymity of the internet and the global reach of digital platforms to spread their messages widely and quickly, often without easy traceability. Disinformation campaigns have evolved with technological advancements, particularly with the advent of generative AI. These campaigns now have the capacity to create and disseminate fake news and deepfakes on an unprecedented scale. According to the Google Cloud Cybersecurity Forecast 2024, such information operations can severely erode public trust in news and information, challenging the foundation of democratic engagement and the perceived legitimacy of election outcomes.

The utilization of digital channels for these campaigns not only spreads falsehoods at an alarming rate but also introduces a nuanced layer of cyber risk, as they can be intricately linked to various cyberattacks, blurring the lines between misinformation and cyberwarfare. The Russian war on Ukraine represents a prominent case of an extensive cyberwar, where traditional warfare is strategically aligned with a diverse range of cyberattacks and disinformation campaigns, designed to spread intimidation and disruption. In February 2024, the French agency VIGINUM revealed the discovery of a pro-Russian propaganda network to present the so-called "special military operation" in a positive way and denigrate Ukraine and its leaders, by repeatedly presenting inaccurate or misleading narratives. To reach a wide audience in France and several other Western Countries, the network employed several techniques including massive automation and search engine optimization, a VIGINUM technical report on the matter assessed. The disclosure of this discovery to the public by Minister for Europe and Foreign Affairs Stéphane Séjourné was aimed at alerting the French public ahead of the European Election in June 2024 to the threat of disinformation disseminated by Russian actors.

Next to disinformation, cyber threats to electoral systems present a multifaceted challenge, encompassing everything from the probing and compromising of networks that manage voter registration data and vote tallies to sophisticated hack-and-leak operations. These operations, notably executed by state actors in international elections, involve stealing and exposing sensitive information about candidates and political figures, casting a shadow over the electoral process. The prevalence of high-profile hack-and-leak operations, such as the exposure of the Clinton Campaign's emails before the 2016 U.S. elections and the 2017 #MacronLeaks, has prompted the European Commission to recognize such activities as impermissible manipulative behavior in its 2022 Code of Practice on Disinformation.

The manipulation or compromise of voter registration databases can lead to disenfranchisement or fraudulent registrations. Hacking or tampering with electronic voting machines could directly manipulate vote counts, and malware or ransomware attacks could disrupt the voting process. Additionally, election management systems are at risk, where manipulation could result in the misallocation of resources or inaccurate reporting of results. In March 2024, the United Kingdom called out a pattern of malicious cyber activity by Chinese state-affiliated organizations and individuals targeting the UK Electoral Commission – which oversees elections and regulates political finance in the UK – between 2021 and 2022, as well as UK parliamentarians. "While these attempts to interfere with UK democracy have not been successful," said Foreign Secretary Lord Cameron as quoted in a government press release, "we will remain vigilant and resilient to the threats we face", in response sanctioning a front company and two members of a Chinese state-affiliated group.

Moreover, phishing and social engineering tactics pose significant threats, as targeted attacks on election officials or political parties can lead to the compromise of sensitive information and data breaches or the introduction of malware, further undermining the integrity and security of the electoral process. The integrity of election systems is at stake when hackers target the electronic infrastructure that underpins the democratic process, including voting machines and voter databases. Even without successful tampering of vote counts, the mere act of compromising these systems has the potential to significantly erode public confidence in the election outcomes.

The role of AI in exacerbating the threat landscape cannot be overstated. From spreading disinformation to creating deepfakes and manipulating social media algorithms, the misuse of AI technologies represents a multifaceted challenge to election integrity. The potential for AI to automate the generation and dissemination of disinformation at scale, target voters with personalized misinformation, and exploit data privacy vulnerabilities underscores the evolving nature of threats to democratic processes. The 2022 "Facing Reality?" report from the Europol Innovation Lab found that advancements in technologies like deepfakes can lead to undermined public trust in authorities and official facts as the volume of deepfakes increases.

To strengthen electoral integrity and combat disinformation, both national governments and international bodies have implemented a range of regulatory approaches. For instance, Finland has proactively engaged with media organizations to boost public education on media literacy, equipping citizens with the skills needed to discern reliable information from disinformation. Singapore enacted the Protection from Online Falsehoods and Manipulation Act (POFMA), empowering government authorities to directly counteract online misinformation and disinformation by mandating corrections, removing content, or blocking accounts spreading harmful falsehoods. On a broader scale, the European Union's Code of Practice on Disinformation involves major online platforms committing to measures like increasing transparency in political advertising and systematically dismantling fake accounts. Additionally, the G7 Rapid Response Mechanism facilitates real-time information sharing among member countries, enhancing the collective ability to respond swiftly to disinformation threats.

Organizations like CISA in the United States, the Federal Office for Information Security (BSI) in Germany, and ENISA in the EU are at the forefront of these efforts, offering resources like the Cybersecurity Toolkit to Protect Elections and initiatives to combat online disinformation through open data. For instance, a cooperation of the European member states, the European Commission, and ENISA published a new cybersecurity compendium on how to protect the integrity of elections in March 2024. It aims to support elections management bodies, national electoral authorities, and cybersecurity bodies involved in increasing electoral resilience in the member states by providing guidelines and practical measures based on relevant experiences and best practices identified by its contributors.

The Intersection of Cybersecurity and AI

AI has emerged as a transformative force in cybersecurity, significantly enhancing the efficacy of security measures. The value of AI in this sector and its pivotal role in shaping future cybersecurity landscapes are underscored by a significant financial trajectory, with projections indicating that the global market for AI-powered cybersecurity solutions is set to expand from approximately $15 billion in 2021 to an estimated $135 billion by 2030, according to a report on Artificial Intelligence in Cybersecurity Market Analysis by Acumen in 2022.

AI can enhance cybersecurity efforts through sophisticated detection capabilities that surpass human accuracy, as analyzed by Morgan Stanley in 2023, detecting actual attacks more accurately than humans and significantly reducing false-positive results, referring to instances where a security system mistakenly identifies a benign activity as a threat or risk, and ensuring that responses are prioritized based on the severity of real-world risks. Its prowess in identifying the hallmarks of phishing within emails and messages, alongside its capability to simulate and thus expose potential vulnerabilities through social engineering attack simulations, provides a proactive shield against cyber threats. The rapid analysis of massive datasets by AI ensures that threats are not only swiftly identified but also that containment measures can be promptly enacted, showcasing AI's indispensable role in timely threat mitigation.

AI has a transformative impact on cybersecurity decision-making processes. By mimicking human cognitive functions and computing capabilities, AI systems streamline the analysis and prioritization of data, thereby enhancing the detection and classification of cybersecurity threats. This is especially crucial in expansive network environments, where AI's ability to correlate and analyze data from diverse sources plays a critical role in threat intelligence and network surveillance. Real-time monitoring of network activity through AI technologies offers another layer of defense, with the capability to identify and act upon illegal connections, anomalous data transfers, and other signs of potential security breaches. The automation and adaptability facilitated by AI extend across various components of the cybersecurity framework, including IoT devices, cloud services, and network infrastructures, enabling continuous updates and improvements to security protocols. AI's application in network surveillance and threat detection provides a nuanced understanding of security incidents, offering descriptive analytics that clarify the events leading to breaches and enabling AI-powered diagnostics to delve into the causes behind such incidents. Predictive analytics play a crucial role in forecasting the impacts of system vulnerabilities, while prescriptive analytics guide the formulation of strategic responses to neutralize threats effectively.

Moreover, AI has, according to a 2023 Morgan Stanley article on the new era of AI and cybersecurity "potential to be a game-changing tool in penetration testing". By leveraging AI tools to probe their own systems for weaknesses, organizations can pre-emptively address vulnerabilities before they can be exploited by cyber adversaries, marking a proactive stride toward more secure digital environments.

Despite the numerous benefits AI brings to cybersecurity, it also introduces new challenges. Cybercriminals have quickly adopted AI technologies to develop more sophisticated methods of attack, leveraging its capabilities to enhance their malicious endeavors significantly.

Generative AI has become a powerful tool in the arsenal of cybercriminals, enabling them to create deepfakes with alarming accuracy and efficiency. By manipulating text, images, and sound, these AI-driven deceptions can mimic individuals or scenarios convincingly, making them potent instruments for misinformation campaigns, social engineering, and extortion. The distribution of such content across social platforms can sow discord and undermine trust at unprecedented scales.

In the domain of password security, AI's impact is equally profound. Enhanced algorithms have bolstered the ability of hackers to crack passwords more swiftly and accurately, streamlining the process of unauthorized access and making it a more attractive and fruitful endeavor for cybercriminals. A group of researchers discovered that AI-driven attacks can accurately steal passwords by analyzing the sounds of keystrokes, achieving up to 95 percent accuracy without relying on complex language models.

AI's influence extends to the automation of social engineering attacks, where it enables the crafting of highly personalized and sophisticated messages designed to deceive. By automating and refining these processes, cybercriminals can launch a higher volume of attacks with increased efficacy, encompassing a broad spectrum of fraudulent activities from phishing to intricate business email compromise scams.

Data poisoning – "a type of cyberattack in which an adversary intentionally compromises a training dataset used by an AI or machine learning model to influence or manipulate the operation of that model" – represents another critical threat posed by AI. This subversion leads to flawed decision-making by the AI, with the potential for significant damage before the issue is identified and rectified. The challenge of detecting and addressing data poisoning underscores the vulnerabilities inherent in relying on AI for security measures.

Furthermore, the use of AI in disseminating malware through commonly downloaded programs illustrates a sophisticated mechanism of attack. By embedding malware that activates after a delay, attackers can exploit AI to gather critical user data and uncover system vulnerabilities. This intelligent malware, capable of learning from both its successes and failures, represents a formidable challenge as it can adapt to defensive measures and initiate novel attacks, often in a covert manner that blends into the targeted organization's security environment.

AI is just one of the many emerging technologies that will shape future security strategies. Looking ahead, the advent of quantum computing and other advanced technologies presents new challenges and opportunities, necessitating a continual evolution and adaptation of cybersecurity measures to stay ahead of potential threats. Quantum computing introduces a transformative potential for enhancing security measures due to its ability to process complex computations exponentially faster than traditional computers. This capability is pivotal for developing advanced cryptographic technologies, which can fortify the encryption of sensitive data and secure communications against increasingly sophisticated cyber threats. However, quantum computing also poses a profound risk as it could potentially break the current encryption standards that underpin much of digital security today. Recognizing this dual-edged nature, governments and international organizations are investing in quantum-resistant cryptography. Furthermore, as part of a broader strategic approach, collaboration in research and sharing of quantum-safe practices are encouraged through international cybersecurity forums and alliances.

Building Resilience:
Innovation and Regulation in Building Effective Cyber Resilience

ACyber resilience has become a cornerstone of strategic planning for organizations, recognizing that cyber threats are an inevitable aspect of the digital age. Cyber resilience focused on maintaining operational continuity and ensuring a swift recovery from cyber incidents through the adoption of a comprehensive cyber resilience framework. Differing from traditional cybersecurity, which is aimed at preventing and protecting against attacks, cyber resilience operates on the understanding that attacks are unavoidable. As such, it includes a robust set of plans for incident management, business continuity, risk mitigation, and the training of personnel.

The WEF's Global Cybersecurity Outlook Report 2024 assesses that in 2023, the cybersecurity sector expanded at a rate four times faster than the global economy and surpassed the tech industry's growth, indicating a surge in innovation and opportunities. Despite this progress, a lack of cyber security remains a significant risk, as highlighted in the WEF's Global Risks Report 2024. This goes for both the immediate and long-term future, especially for governments and the private sector, where cyber insecurity ranks as the third most severe short-term threat.

Moreover, the WEF's Global Cybersecurity Outlook 2024 points out that many organizations lack the robustness to be considered truly cyber-resilient. In addition, there is a growing disparity between large, resource-rich organizations and smaller enterprises. Advanced tools and skilled talent are often more available to larger entities. Additionally, securing aging systems and legacy technology remains a significant hurdle for many, further complicated by a widening skills gap in the cybersecurity workforce.

A robust cyber resilience strategy is designed to proactively counter and manage cyber risks, ensuring operational continuity and building trust among stakeholders. Developing cyber resilience encompasses several key steps. It begins with prioritizing cyber risk within the broader organizational risk management framework, ensuring that cyber threats are regularly assessed and addressed. Cultivating a culture of resilience is critical, involving regular training, awareness programs, and ensuring buy-in across all levels of the organization. Establishing robust cyber governance is essential, with leadership playing a pivotal role in supporting and promoting cyber resilience strategies. Moreover, fostering systemic resilience through collaboration, understanding supply chain risks, and aligning with regulatory requirements enhances an organization's defensive posture. Implementing cybersecurity by design, where security measures are integrated from the initial stages of product and system development, is also vital. This comprehensive approach not only mitigates risks but also positions organizations to respond effectively to cyber incidents, maintaining operational continuity and safeguarding stakeholder trust.

However, innovation alone is not sufficient. Regulation plays a crucial role in establishing minimum cybersecurity standards, protecting consumer data, and ensuring that organizations implement necessary security measures. Effective regulation requires a delicate balance, encouraging innovation and protecting public and private interests without stifling technological advancement.

The regulatory landscape is rapidly evolving to address the increasing frequency and sophistication of cyberattacks. With regulations like the Network and Information Systems Directive (NIS2), the Digital Operational Resilience Act (DORA), and the Cyber Resilience Act (CRA), the EU exemplifies this trend by setting stringent cybersecurity obligations for essential entities and financial services and imposing requirements on the suppliers of products with digital components. For example, the CRA applies mandatory security requirements to all products connected directly or indirectly to another device or network from baby-monitors to smart-watches, as many digitally connected products have shown inadequate levels of cybersecurity. The CRA introduced a framework of cybersecurity requirements governing the planning, design, development, and maintenance of such products, with obligations to be met at every stage of the value chain.

By adhering to these regulatory requirements, organizations not only ensure compliance but also strengthen their resilience against cyberattacks. Regulations also promote a culture of accountability and continuous improvement, as organizations are encouraged to regularly update their cybersecurity practices in line with evolving standards and threats. This symbiosis between regulation and organizational practice fosters a more secure and resilient digital ecosystem.

In the United States, federal and state-level initiatives are enhancing cybersecurity disclosures and standards, such as the recently revised New York State Department of Financial Services (NYDFS) Cybersecurity Regulation (23 NYCRR Part 500), requiring financial services companies operating in New York to develop and implement an effective cybersecurity program, to assess their cybersecurity risk and develop a plan to proactively address them. The amendment brings substantial updates to NYDFS's cybersecurity requirements, emphasizing the essential need for organizations to enhance their cybersecurity programs to strengthen protections for both businesses and consumers.

Many emerging economies are also establishing foundational cybersecurity strategies that emphasize national coordination and international collaboration. For instance, countries like India and Brazil have adopted national cybersecurity policies that include frameworks for public-private partnerships, aimed at enhancing the technical and strategic capabilities of both sectors in managing cyber risks. India's National Cyber Security Policy, for example, seeks to create a secure cyber ecosystem with resilient cyber protection mechanisms and a robust incident response strategy. This policy emphasizes building indigenous capabilities in cybersecurity technologies and fostering innovation through startups and academic institutions. Similarly, Brazil has implemented the Brazilian National Strategy for Cybersecurity, which outlines strategic objectives that include strengthening governance mechanisms, protecting critical infrastructure, and enhancing legal frameworks to address cybercrimes effectively. Moreover, in Africa, where cybersecurity infrastructure is still developing, countries like Kenya have launched comprehensive national cybersecurity strategies which focus on establishing robust governance frameworks. These include specific measures for protecting critical information infrastructures, boosting cybersecurity awareness, and collaboration with international bodies to leverage global cybersecurity initiatives.

With the evolving regulatory environment, the challenge of navigating conflicting regulations across different jurisdictions is increasing, with 34 percent of business executives highlighting it as a major compliance hurdle, according to the Global Security Outlook 2024. This underscores the critical need for alignment and cooperation across borders, ensuring a unified and robust defense against cyber threats, while at the same time creating a business-friendly environment.

International Cooperation in Defense and Crisis Reaction

The inherently borderless nature of cyber threats coupled with their increasing sophistication emphasizes the critical need for international cooperation among states, international and regional organizations, and other entities. In its Global Cybersecurity Outlook 2024, the World Economic Forum urges that forging a secure cyber environment necessitates collaboration not only among national and international bodies but also includes organizations, suppliers, insurers, and regulatory entities. This collective effort relies heavily on the seamless sharing of information and intelligence as well as mutual assistance, all of which are underpinned by aligned policy goals and robust bilateral and multilateral relations.

Recognizing this need, the United Nations' Global Cybersecurity Index, delineated by the International Telecommunication Union (ITU) in 2024, has outlined a comprehensive framework encompassing five foundational elements for cooperation in cybersecurity.

Intra-State Cooperation stands at the forefront of this framework, emphasizing the critical role of cohesive collaboration within countries. By bringing together various governmental sectors, agencies, and departments, nations can forge a united front against cyber threats. This internal alignment is crucial for sharing intelligence, pooling resources, and strategizing effectively to bolster national cybersecurity defenses.

Multilateral Agreements serve as the bedrock of international cybersecurity cooperation, providing a structured platform for countries to collaborate in combating cyber threats. These agreements facilitate the exchange of critical information, mutual support in incident management, and the co-creation of strategies to deter cyber adversaries. Through these collaborative efforts, nations can transcend geographical and political boundaries to address the global nature of cyber threats.

International Fora offer valuable spaces for dialogue and consensus-building among nations on cybersecurity norms and policies. These forums, including specialized groups within the United Nations and other global platforms, are instrumental in fostering international cooperation. They allow countries to share experiences, negotiate norms, and collectively enhance the global cybersecurity posture.

Public-Private Partnerships recognize the indispensable role of the private sector in cybersecurity. By fostering collaboration between governmental bodies and industry leaders, these partnerships harness a wealth of expertise and resources to develop cutting-edge cybersecurity solutions, share timely threat intelligence, and respond effectively to cyber incidents. This synergy between the public and private sectors is crucial for advancing cybersecurity innovation and resilience.

Inter-Agency Partnerships, the fifth pillar, focus on harmonizing efforts across various international organizations and agencies. Such partnerships ensure that policies, strategies, and actions are aligned and mutually reinforcing, thereby amplifying the global response to cyber threats. These collaborations are vital for creating a coherent and united international stance on cybersecurity.

At the center of international cyber cooperation stands information sharing. This involves creating standard operating procedures for exchanging information, establishing secure lines of communication, and aligning technical cyber incident information with military intelligence threat assessments. This kind of collaboration aims to define what type of information needs to be shared, who needs to receive it, and ensure it is released in a timely and appropriate manner.

Another critical mechanism is the creation of specialized committees and working groups, such as an EU–NATO Cyber Research and Technology Innovation Committee. This committee addresses the technology gap between public and private sectors and among member states by identifying innovative tools relevant to enhancing cyber defense capabilities. It also looks into fast-developing technological areas like cloud computing and automated information sharing, which are crucial for cyber resilience and defense.

International cooperation in cyber defense and crisis reaction has seen significant advancements through strategic partnerships and initiatives, with recent examples showcasing the global commitment to bolstering cyber resilience. One such instance of strengthening cyber defense cooperation is the enhanced partnership between the United States and the European Union. In 2024, U.S. Secretary of Homeland Security Alejandro N. Mayorkas and European Commissioner for Internal Market Thierry Breton reaffirmed their commitment to cyber resilience. This partnership involves comparing and aligning cyber incident reporting requirements, enhanced cooperation between cybersecurity agencies, and the creation of a transatlantic working group of open-source security experts, among other initiatives.

The NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE) is another example for international cooperation in the cyber domain. The Centre includes membership from 37 nations and focuses on research, training, and exercises in cyber defense. Its activities, such as the publication of the Tallinn Manual and the annual International Conference on Cyber Conflict (CyCon), underscore the collective effort to address cyber challenges through multidisciplinary collaboration among nations, NATO, academia, and the private sector.

Another example is the Cyber Expert Group of the G7. Founded in 2015, it helps to coordinates cybersecurity policy and strategy across G7 countries and acts as a vehicle for information sharing, cooperation, and incident response. This includes annual incident response tests and quadrennial cross-border cyber exercises.

However, international cooperation in cyber defense and crisis reaction faces a complex set of challenges that hinder the effectiveness of collective efforts to secure cyberspace. The intricacies of these challenges span legal, political, technological, and operational domains, reflecting the multifaceted nature of cybersecurity itself.

One significant barrier to enhanced international cooperation is the diversity of legal and regulatory frameworks across nations as mentioned above. These differences create a fragmented landscape that complicates the exchange of critical cybersecurity information and joint response efforts. For instance, what is considered permissible cyber activity or data sharing in one country may be illegal or restricted in another, leading to hesitancy and barriers to international collaboration.

Political and trust issues further exacerbate the situation. Trust is a cornerstone of any effective international partnership, especially in areas as sensitive as cybersecurity. However, geopolitical tensions and historical mistrust among nations can undermine efforts to establish a unified front against cyber threats. The absence of trust slows down the development of cooperative initiatives and can lead to reluctance in sharing vital intelligence that could preempt or mitigate cyber incidents.

The varied levels of cybersecurity maturity among countries also pose a significant challenge. There is a wide gap between nations with advanced cyber capabilities and those still developing their cyber infrastructure and defenses. This disparity affects the ability of countries to engage in and contribute to international cyber defense efforts equally. Advanced nations may find themselves in a position where they are disproportionately supporting the cybersecurity needs of less developed partners, which can strain resources and dilute focus on addressing shared threats.

The rapidly evolving nature of the cyber threat landscape itself presents another hurdle. Cyber threats are becoming increasingly sophisticated, requiring constant vigilance and adaptation of defense strategies. The dynamic nature of cyber threats makes it difficult for international agreements and cooperative frameworks to stay current and effective. This necessitates a level of agility and flexibility in international cooperation that is often hard to achieve through formal structures.

Operational coordination challenges, including differences in time zones, languages, and national procedures, further complicate international cyber defense efforts. Efficient real-time collaboration and information sharing require sophisticated mechanisms and technologies that can bridge these operational gaps. Yet, developing and implementing such solutions on an international scale is daunting and requires significant investment and commitment.

Overall, to adequately address the changing landscape of cyber threats, more collaboration is necessary – between all relevant stakeholders. By sharing resources, intelligence, and best practices, countries and organizations need to build a more resilient cyber environment capable of withstanding and recovering from attacks, ultimately safeguarding critical infrastructures and the global digital economy.

50 years Aspen Institute Germany

Security Network Munich