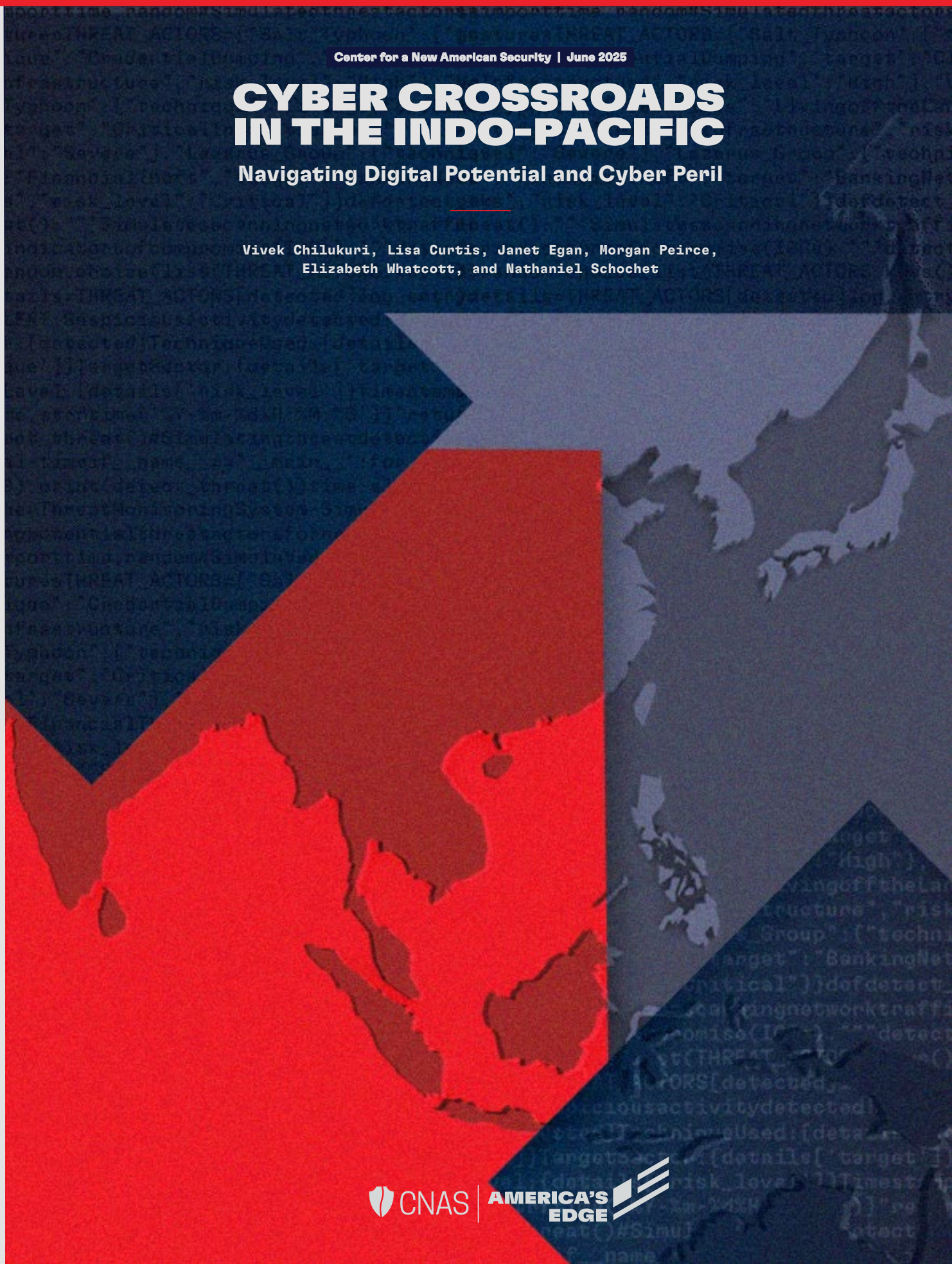
Center for a New American Security | June 2025

CYBER CROSSROADS IN THE INDO-PACIFIC

Navigating Digital Potential and Cyber Peril

Vivek Chilukuri, Lisa Curtis, Janet Egan, Morgan Peirce,
Elizabeth Whatcott, and Nathaniel Schochet



CNAS | AMERICA'S EDGE

About The Authors

Vivek Chilukuri is the senior fellow and program director of the Technology and National Security Program at the Center for a New American Security (CNAS). His work focuses on the responsible development and deployment of artificial intelligence; the U.S.-China technology competition; and the intersection of technology, democracy, and geopolitics. Before joining CNAS, Chilukuri served as a senior technology policy advisor, deputy chief of staff, and legislative director for Senator Michael Bennet (D-CO)—a member of the Senate Select Committee on Intelligence.

Lisa Curtis is the director of the Indo-Pacific Security Program at CNAS. With over 20 years of service in the U.S. government, her work centers on U.S. policy toward the Indo-Pacific and South Asia, with a particular focus on U.S.-India strategic relations, the Quad (the United States, Australia, India, and Japan), counterterrorism strategy in South and Central Asia, and China's role in the region. Curtis served as deputy assistant to the president and National Security Council senior director for South and Central Asia from 2017 to 2021.

Janet Egan is a senior fellow with the Technology and National Security Program at CNAS. Her research focuses on the national security implications of artificial intelligence (AI) and other emerging technologies, including how compute can be leveraged for the governance of advanced AI systems. Prior to joining CNAS, Egan was a director in the Australian Government Department of the Prime Minister and Cabinet.

Morgan Peirce is a research assistant for the Technology and National Security Program at CNAS, supporting the Center's research on quantum technology and cybersecurity. Before CNAS, Peirce was a fellow at the U.S. Indo-Pacific Command's Strategic Planning and Policy Directorate, where she focused on Northeast Asia.

Elizabeth Whatcott is a public policy coordinator at Meta and a former research assistant with the Technology and National Security Program at CNAS. Her work at CNAS included facilitating a series of cybersecurity roundtables in the Philippines and South Korea that informed the drafting of this report. After her time at CNAS, Whatcott joined the U.S. Department of Homeland Security as a Special Assistant to the Chief Information Officer and Chief Artificial Intelligence Officer.

Whatcott contributed to this report before she began her roles at both the U.S. Department of Homeland Security and Meta. This work represents her views and contributions, and not necessarily the views or positions of her past or current employers.

Nathaniel Schochet is a former program administrator for the Indo-Pacific Security Program at CNAS. He graduated in May 2020 from Hobart and William Smith Colleges, where he majored in Asian studies and minored in international relations. Schochet later completed a master's degree from the American University School of International Service in Washington, D.C., in May 2024.

About the Technology and National Security Program

The CNAS Technology and National Security Program produces cutting-edge policy research to secure America's edge in emerging technologies while managing potential risks to security and democratic values. The program produces bold, actionable recommendations to drive U.S. and allied leadership in responsible technology innovation, adoption, and governance. The Technology and National Security Program focuses on three high-impact technology areas: artificial intelligence, biotechnology, and quantum information sciences. It also conducts cross-cutting research to strengthen U.S. technology statecraft to promote secure, resilient, and rights respecting digital infrastructure and ecosystems abroad. A focus of the program is convening the technology and policy communities to bridge gaps and develop solutions.

About the Indo-Pacific Security Program

The CNAS Indo-Pacific Security Program explores opportunities and challenges for the United States in the region, with a special focus on the bilateral relationships and multilateral engagements that form an evolving security network to preserve freedom of the seaways, respect for national sovereignty, and peace and prosperity. It draws on a team with senior government, congressional, and nongovernment expertise in U.S. foreign policy, intelligence analysis, international security, and regional relationships. The Indo-Pacific Security Program analyzes trends and generates practical and creative policy solutions to issues related to sharpening the U.S. edge in the strategic competition with China, strengthening relationships with allies and partners like Australia, India, Japan, South Korea, and Taiwan, and addressing democracy and counterterrorism challenges in South and central Asia.

Acknowledgments

This report would not have been possible without the insights, feedback, and collaboration of several partnering organizations, outside experts, and CNAS colleagues. The authors would first like to thank the Prospect Foundation, the Japan Institute of International Affairs, the Stratbase ADR Institute for Strategic and International Studies, and the Asan Institute for Policy Studies for their close partnership in organizing the four cybersecurity workshops in Taipei, Tokyo, Manila, and Seoul, respectively. Their ability to convene high-level experts from government, industry, and academia in each location and substantively tailor the workshops was invaluable to this research. The authors would also like to extend their deep gratitude to Gary Corn, Chris Painter, Bart Hogeveen, Dr. Duyeon Kim, Mihoko Matsubara, Dr. Sherwin Ona, and Dr. Wei-Chung Teng for their invaluable feedback on earlier drafts of the report. The report would also not have been possible without the excellent research, editorial, and design contributions of current and former CNAS colleagues Maura McCarthy, Melody Cook, Emma Swislow, Caroline Steel, Jacob Stokes, Michael Depp, Evan Wright, Kareen Hart, Thomas Corel, and Julia Arnold. The workshops that informed this report were made possible with the generous support of the Microsoft Corporation. The writing and editing of this report were made possible with support to the CNAS Technology and National Security Program.

As a research and policy institution committed to the highest standards of organizational, intellectual, and personal integrity, CNAS maintains strict intellectual independence and sole editorial direction and control over its ideas, projects, publications, events, and other research activities. CNAS does not take institutional positions on policy issues and the content of CNAS publications reflects the views of their authors alone. In keeping with its mission and values, CNAS does not engage in lobbying activity and complies fully with all applicable federal, state, and local laws. CNAS will not engage in any representational activities or advocacy on behalf of any entities or interests and, to the extent that the Center accepts funding from non-U.S. sources, its activities will be limited to bona fide scholastic, academic, and research-related activities, consistent with applicable federal law. The Center publicly acknowledges on its website annually all donors who contribute.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Indo-Pacific faces a cyber crossroads. Down one path lies deeper military, intelligence, and economic ties between Washington and its key allies and partners in this strategically vital region. Down another, rising cyber threats from the People's Republic of China (PRC), North Korea, Russia, and a growing shadow industry of cybercriminals and hacktivists derail these ambitions by compromising critical infrastructure, weakening data security, and undermining democratic institutions. The outcome will depend on the choices Washington and its Indo-Pacific partners make—or fail to make—in the coming years.

The U.S.-China rivalry has long extended to the cyber domain, but in recent years, Beijing has increasingly exploited the gray zone of cyberspace to test, probe, and push other nations as part of a broader campaign to gain influence and shape regional norms and power structures.[1] In recent years, the PRC has sharply escalated its cyber aggression in a dangerous new game that combines traditional operations focused on espionage, intellectual property theft, and data exfiltration with newly assertive disinformation, influence operations, and pre-positioning in critical infrastructure. Adding to the uncertainty, rapid advances in artificial intelligence (AI) could further tilt the balance toward offense in cyberspace in unpredictable and potentially dangerous ways.

Against this backdrop, Indo-Pacific governments have taken historic steps to strengthen their resilience in a cyber landscape that has grown more varied, volatile, and dangerous than ever.

To assess how Washington and its Indo-Pacific partners are navigating this cyber crossroads, the Center for a New American Security's Technology and National Security Program and Indo-Pacific Security Program led a year-long research project that combined extensive desk research with in-person field research and expert workshops in Japan, South Korea, Taiwan, and the Philippines. This report draws on this research to offer in-depth assessments of the cyber landscapes in all four countries to identify key trends, challenges, and opportunities to strengthen cybersecurity and resilience in partnership with the United States.

The findings offer cause for both optimism and concern. On the one hand, Japan, South Korea, Taiwan, and the Philippines have all undergone notable shifts in elevating cybersecurity as foundational to national security. Japan's 2022 National Security Strategy made cybersecurity a pillar for the first time, and the government has passed reforms to facilitate information sharing with the United States and shift toward active cyber defense.[2] South Korea updated its National Cybersecurity Strategy to adopt a Defend Forward cyber posture, mirroring the U.S. shift in 2018.[3] Taiwan established a National Institute of Cybersecurity within its Ministry of Digital Affairs, and the Executive Yuan approved a four-year plan to boost digital resilience.[4] The Philippines finalized a five-year National Cybersecurity Plan.[5]

For its part, the United States has elevated cybersecurity in its foreign policy with expanded information sharing, capacity building, and diplomacy anchored in a new Bureau of Cyberspace and Digital Policy within the U.S. Department of State. Recent years have seen Washington both strengthen its proactive cyber capacities and embrace a "name and shame" approach to call out malign cyber operations from foreign adversaries like Russia and the PRC.

Still, these laudable efforts to bolster cyber policies, personnel, and partnerships have failed to keep pace with rising threats. Washington's finger-wagging

statements and targeted sanctions in the wake of cyber incidents have failed to stem rising threats. To confront growing cyber dangers across the Indo-Pacific, the United States and its partners need a more assertive and coordinated approach that intensifies efforts on two fronts: (1) building capacity within each country to strengthen cybersecurity and resilience, and (2) strengthening cooperation to enable more integrated, proactive cyber defense, collective signaling, and cost inflicting on malign cyber actors.

To that end, this report offers recommendations to government leaders in the United States, along with both country-specific and cross-cutting recommendations for government leaders in Japan, South Korea, Taiwan, and the Philippines. Although many of the recommendations directed toward the four countries could fairly apply to the United States, strengthening domestic cybersecurity and resilience is beyond the scope of this report.

For the United States:

- **Launch a "Cyber Shield" for Indo-Pacific treaty allies** to strengthen joint resolve, response, and resources to defend against malign state cyber actors.
- **Significantly expand military cyber engagement and capacity building** by the five component commands in the Indo-Pacific area of responsibility with priority regional allies and partners, for instance, through regular joint tabletop cyber exercises.
- **Clarify legal and policy frameworks to facilitate expanded Hunt Forward and Defend Forward operations in the Indo-Pacific.** In the four countries examined in this report, the legal basis for expanding proactive cyber defense operations remains ambiguous at best.
- **Preserve and strengthen the State Department's Bureau of Cyberspace and Digital Policy (CDP).** CDP has been highly effective at elevating cybersecurity and digital issues in U.S. foreign policy, both with foreign partners and within the department itself. The Trump administration should strengthen the CDP by expanding the Cyber Capacity Building Fund, ensuring sufficient staff, designating CDP as the principal coordinator for all civilian cyber engagement and capacity building with allies and partners, and rationalizing cyber dialogues.
- **Develop a unified strategy for promoting secure and resilient information and communications technology (ICT) infrastructure in the Indo-Pacific** drawing on the full range of U.S. government tools.
- **Pursue agreements to expand the Cyber Trust Mark with Indo-Pacific partners,** mirroring the January 2024 agreement with the European Union.
- **Encourage Japan's participation in AUKUS Pillar II,** which creates a framework for improved intelligence sharing and cyber cooperation.
- **Scale joint military cybersecurity cooperation with Taiwan,** including Hunt Forward operations, consistent with new authorities in the FY 2024 National Defense Authorization Act.
- **Prioritize the provision of defense cybersecurity capabilities through the new Taiwan Security Cooperation Initiative,** which authorizes the U.S. Department of Defense to provide up to $300 million in total assistance.

For Japan, South Korea, Taiwan, and the Philippines:

- **Mandate adoption of cybersecurity best practices across government**, such as multifactor authentication and prohibitions on the use of personal devices for official business.
- **Prioritize cybersecurity in increased defense spending** with investments to modernize legacy IT infrastructure, boost threat detection and offensive capabilities, and acquire cutting-edge AI and cloud-based cyber defenses.
- **Deepen partnerships with local and foreign technology companies to benefit from broader threat data and best-in-class capabilities.**

- **Clarify legal and policy frameworks to allow forward-deployed teams from U.S. Cyber Command**, enabling more Hunt Forward and Defend Forward operations.
- **Designate a single point of entry to route intergovernmental cyber coordination.**
- **Develop an integrated strategy to counter malign foreign influence** that combines intelligence, cyber, diplomatic, and economic tools to better identify, deter, disrupt, and respond to adversary influence operations.
- **Establish clear and uniform skills and competencies for cybersecurity roles in government, aligning wherever possible with private sector certifications.**
- **Leverage AI tools to boost productivity of limited cybersecurity professionals.**
- **Develop a strategy to transition from compromised ICT hardware, software, and infrastructure from vendors linked to foreign adversaries.**
- **Encourage businesses to adopt Secure by Design and Secure by Default principles.**
- **Boost public awareness about the ties between escalating cyberattacks and national security.**

Strengthening cybersecurity across the Indo-Pacific is a generational effort that will require sustained investment, prioritization, and partnership from leaders across both government and industry. None of this will be easy, but it is essential to realizing a future for the Indo-Pacific defined not by fears of digital vulnerability, but common aspirations for greater connectivity, collaboration, and partnership. That future remains up for grabs.

INTRODUCTION

The Indo-Pacific faces a cyber crossroads. Home to half the world's population, the region continues to digitize faster than any other, with billions of people, devices, and businesses connecting online for the first time. Policymakers from Washington to Seoul see vast potential from the region's growing connectivity and technology adoption, but they also see growing peril from cyber threats.

The Indo-Pacific is home to two of the world's most aggressive and capable cyber nations, the People's Republic of China (PRC) and North Korea. Pyongyang continues to wield cyber operations to steal intellectual property (IP) and fund its illicit weapons programs, including through brazen attacks against cryptocurrency platforms in recent years.[6] For its part, Beijing has embraced a far more aggressive cyber posture, breaching and pre-positioning in critical infrastructure while intensifying its cyber espionage and disinformation campaigns against Indo-Pacific democracies.[7] Although Russia's cyber aggression has focused principally on Europe and North America, it has also conducted malign cyber operations in the Indo-Pacific, for instance, ahead of the 2020 Olympics in Tokyo.[8] A proliferating shadow industry of scammers, cybercriminals, and hacktivists for hire only adds to the danger, while fast-developing capabilities from artificial intelligence (AI) risk upsetting the offense-defense balance in cyberspace in unpredictable ways.

Against this backdrop, leaders across the region recognize that stronger cybersecurity is essential to realizing a future for the Indo-Pacific defined not by fears of digital vulnerability, but shared aspirations for greater connectivity, prosperity, and partnership. To that end, governments across the region have elevated cybersecurity with a raft of new laws, agencies, investments, and initiatives. It would be a mistake, however,

to view this flurry of activity as sufficient. If the United States, which boasts the greatest resources and cyber capabilities of any nation, continues to struggle against the PRC's cyber aggression, the outlook is decidedly grimmer in nations like the Philippines, which has roughly 200 highly certified cybersecurity professionals in a country of 118 million.[9] Even wealthier countries like Japan and South Korea have considerable work ahead to boost cyber security and resilience, from mainstreaming best practices like multifactor authentication (MFA) to updating regulations that privilege domestic vendors at the expense of cutting-edge technologies.

Washington has a direct interest in prioritizing stronger cybersecurity with Indo-Pacific allies and partners. U.S. aspirations to deepen commercial, military, and intelligence partnerships across the region will run headfirst into the reality of Beijing's growing cyber aggression, along with uneven cyber personnel, policies, and practices in key Indo-Pacific partners and allies. Left unchecked, the diffusion of compromised, Chinese-linked digital infrastructure and technologies will also impede future U.S. cooperation in the region. Beijing understands the strategic value of creating and exploiting cyber vulnerability in the Indo-Pacific to limit such cooperation, even if it comes at great expense to the countries themselves. U.S. businesses and military bases across the region also remain exposed when host governments fail to keep pace with evolving cyber threats. Moreover, cyber threats do not respect national boundaries, and recent history is replete with examples of cyber operations initially targeted abroad—like the 2017 WannaCry incident—eventually harming U.S. interests. Proactive U.S. leadership and stronger cyber partnerships are essential to advancing an open, secure, and prosperous Indo-Pacific.

The United States brings unrivaled capabilities to any cyber partnership, including powerful military, diplomatic, and economic leverage, exquisite global intelligence collection, and formidable offensive capabilities within U.S. Cyber Command. Since 2018, U.S. Cyber Command has embraced a Defend Forward strategic posture, which allows for proactive cyber operations to eliminate threats at their source. The shift stemmed from a recognition that traditional cyber defenses had proven insufficient to check adversary operations and had surrendered valuable intelligence to malign state actors actively seeking to breach U.S. and allied systems. In recent years, U.S. Cyber Command has expanded Hunt Forward operations (HFOs), in which teams from the Cyber National Mission Force deploy to a partner country—at their request—to conduct joint forensic analysis of their at-risk networks to hunt for cyber threats and signs of penetration.[10] HFOs in Ukraine prove that these deployments not only protect partner networks but yield critical insights about adversary tactics and techniques to better defend the homeland. Testimony from the former head of U.S. Cyber Command, General Timothy Haugh, confirms that so far these teams have deployed 22 times to 17 countries across the globe.[11] The United States has yet to realize the full potential of proactive cyber operations under Defend Forward that benefit from access to allied and partner networks, as well as expanded HFOs in key Indo-Pacific allies and partners. Achieving this, however, will require sustained efforts to build capacity and clarify legal and policy frameworks in partner countries.

The United States brings unrivaled capabilities to any cyber partnership, including powerful military, diplomatic, and economic leverage, exquisite global intelligence collection, and formidable offensive capabilities within U.S. Cyber Command.

For all these reasons, the Center for a New American Security's (CNAS) Technology and National Security Program and Indo-Pacific Security Program conducted a year-long project to assess the fast-changing cyber landscape in the Indo-Pacific. As part of the project, the programs organized four in-depth workshops with local partners in Tokyo, Seoul, Taipei, and Manila to drill down on key cybersecurity trends, policy gaps, and implementation challenges to strengthen cybersecurity in a newly dangerous period. Although each country has its own unique context, the four workshops surfaced through lines that point to shared challenges—and opportunities—to strengthen cybersecurity and resilience both through actions within each country and through deeper partnerships with the United States, industry, and other Indo-Pacific governments.

In the next section, the report provides background on different threat actors in the region, including the PRC, North Korea, Russia, and nonstate actors. The report then provides four in-depth studies of the cyber landscape in Japan, South Korea, Taiwan, and the Philippines. For consistency, the report surveys each's country's cyber landscape across four areas:

- **Policy:** cyber, legal, and regulatory frameworks
- **People:** cyber workforce and literacy
- **Partnerships:** public-private, bilateral, and regional cyber cooperation
- **Progress:** implementation successes and challenges and remaining gaps

Finally, the report outlines recommendations for government leaders in the United States and the four covered countries to strengthen cybersecurity and set the course for a more secure, prosperous, and cyber-resilient Indo-Pacific.

CYBER LANDSCAPE IN THE INDO-PACIFIC

No region has more digital potential and cyber peril than the Indo-Pacific. The region is an economic powerhouse, representing 40 percent of global gross domestic product (GDP) and nearly 30 percent of global trade in goods and services.[12] The Indo-Pacific also drives two-thirds of global economic growth with half the world's population.[13] One reason for this economic dynamism is the Indo-Pacific's enthusiastic embrace of technology and digitalization. No region in the world can match its rate of internet adoption and digital connectivity between people and businesses.[14] And it has room to grow, especially in Southeast Asia, where fewer than one in five small and medium enterprises (SMEs) are digitally connected.[15]

According to a 2023 report from Temasek, Google, and Bain and Company, Southeast Asia's digital economy has grown at a 27 percent compound annual rate since 2021, far outpacing growth in the broader economy.[16] In most countries, growth in the digital economy could outpace the broader economy anywhere from 66 percent (the Philippines) to 283 percent (Thailand), owing to a rising population, wealth, and urbanization.[17] By 2030, Southeast Asia's digital economy could reach up to $1 trillion in gross merchandise value.[18] India's digital economy alone could reach $1 trillion in the coming years.[19]

However, the region's expanding digital infrastructure also expands the attack surface for malign state-sponsored and nonstate actors. Inadequate cybersecurity already costs the region upward of $300 billion annually in economic losses, to say nothing of the foreign direct investment, commercial and

***

military technology transfers, intelligence sharing, and other valuable transactions forgone over concerns about cyber vulnerability.[20]

Compounding the challenge, the Indo-Pacific has emerged as the central theater in the U.S.-China competition. This rivalry has long extended to the cyber domain, but in recent years, Beijing has intensified malign cyber operations, combining traditional goals of espionage, IP theft, and data exfiltration with new campaigns for disinformation, influence operations, and pre-positioning in critical infrastructure—enhancing Beijing's ability to shape regional cyber norms and power structures as a result.[21]

Looking ahead, the challenge for the Indo-Pacific is to realize the vast potential of increased digitalization and connectivity across the region while building a more resilient and secure cyber domain, even as threats from state-sponsored actors, nonstate actors, and emerging technologies continue to evolve.

The remainder of this section outlines the primary cybersecurity threats in the Indo-Pacific—specifically, nation-state actors, cybercriminals, hacktivists, and disinformation.

State-Sponsored Actors

State-sponsored groups are among the most sophisticated cyber threat actors in the Indo-Pacific.[22] These entities, often directly employed or indirectly supported by national governments, conduct cyber operations to advance strategic, economic, and geopolitical objectives. Cyber operations backed by nation-states tend to employ advanced persistent threat (APT) tactics, which focus more sophisticated cyber techniques on a single target over an extended period. Access to state resources allows these nation-state actors to support sustained cyber intrusions to facilitate long-term objectives like espionage, IP theft, or disruption in the case of future conflict.[23] Among the most prominent and active nation-state cyber actors in the region—and globally—are the PRC and North Korea.[24] Since 2005, these two nations, along with Russia, have sponsored 77 percent of all known state-backed cyber operations.[25]

THE PEOPLE'S REPUBLIC OF CHINA

The PRC strives to become a "cyber superpower," and it is well on its way.[26] The PRC operates a hacking program larger than every major nation combined.[27] Between 2005 and 2023, the PRC conducted or sponsored at least 247 known cyber operations.[28] According to the U.S. intelligence community, the PRC is "the broadest, most active, and persistent cyber espionage threat."[29] Multiple APT groups active in the Indo-Pacific have been linked to Beijing, including APT30—a group that specifically

A People's Republic of China (PRC) Coast Guard ship fires a water cannon at the Unaizah, *a Philippine Navy chartered vessel, conducting a routine resupply mission to troops stationed at Second Thomas Shoal on March 5, 2024, in the South China Sea. After a similar incident between the PRC Coast Guard and a Philippine vessel in August 2024, PRC-linked cyberattacks targeted entities around the South China Sea, including the Philippines. (Ezra Acayan/Getty Images)*

targets members of the Association of Southeast Asian Nations (ASEAN) and has even infiltrated air-gapped networks—those physically separated from the broader internet—demonstrating its sophistication.[30] In 2019, the Australian Signals Directorate held the PRC's Ministry of State Security responsible for compromising the network of the national parliament, underscoring Beijing's capability and intent to collect sensitive data.[31]

In July 2021, the Biden administration stood with several allies to accuse the PRC of employing "criminal contract hackers" to conduct its malign cyber activities across the globe.[32] That same year, the New Zealand government claimed that another Chinese state-backed group, APT40, hacked its parliament.[33] In 2023, Microsoft named the Chinese-linked groups, Volt Typhoon and Flax Typhoon, for penetrating Taiwanese and American infrastructure to pre-position for a future conflict, using "living-off-the-land" (LoTL) techniques that exploit tools within the penetrated system to sustain themselves and hinder detection.[34] The following year, the United States and the United Kingdom sanctioned a company linked to another Chinese state-backed hacking group, APT31, which allegedly targeted millions of Americans and Britons in a vast, multiyear espionage campaign.[35] The PRC has repeatedly denied involvement in state-sponsored cyberattacks.

The gray zone quality of cyberspace appeals to the PRC, as it allows Beijing to behave more aggressively and with less pushback than it could in conventional domains. Beijing also benefits from the general difficulty of attributing cyberattacks, especially for Indo-Pacific nations that often are less cyber capable and more beholden to Beijing's economic leverage. The intangible, abstract nature of cyberattacks can also mute public and international reaction, further incentivizing Beijing to push the envelope. A Chinese spy plane crossing into Japanese airspace, for example, drives headlines and public reaction in a visceral way that cyber intrusions rarely do.

According to the U.S. intelligence community, the PRC is "the broadest, most active, and persistent cyber espionage threat."

For all these reasons, Beijing has increasingly incorporated cyber operations into an integrated strategy to advance its broader geostrategic interests, which are to sustain domestic economic growth, secure the Chinese Communist Party's (CCP's) political control, and surpass the United States as the preeminent global economic, military, and technology power. Given powerful U.S. technological advantages, including formidable offensive cyber capabilities, a perception of cyber vulnerability in Beijing may also motivate its more assertive cyber operations—embracing the

On January 31, 2024, top U.S. cybersecurity officials discussed the growing threat of PRC cyber operations that conduct espionage, disinformation, and pre-positioning operations against the United States. (Kevin Dietsch/Getty Images)

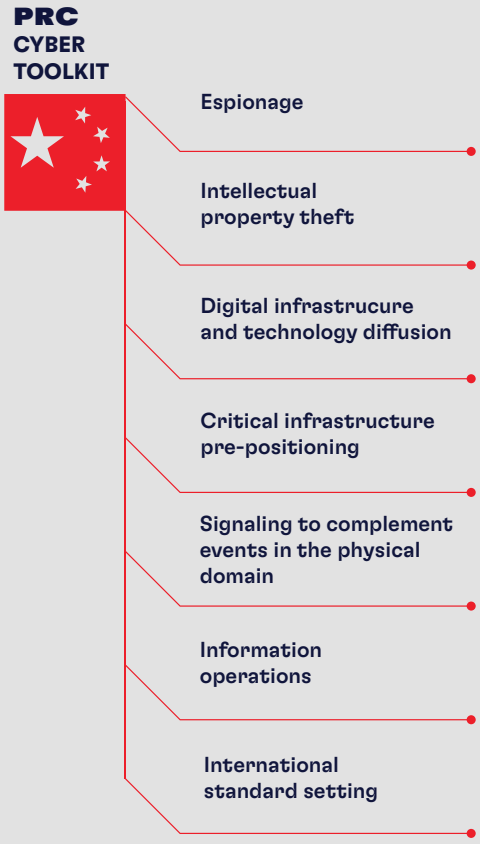
notion that the best defense is strong offense. To that end, Beijing conducts cyber operations for IP theft, espionage, intimidation, influence operations, and more recently, pre-positioning in critical infrastructure to disrupt key public services, sow chaos, and impede adversary mobilization in a potential future conflict.[36] In a secret meeting held in Geneva in December 2024, Chinese officials acknowledged their role in expanded cyber operations penetrating U.S. critical infrastructure and explicitly linked the escalation to growing U.S. support for Taiwan.[37]

Beijing is far ahead of most nations—including the United States—in integrating the various tools, tactics, and outcomes of cyber operations into a unified strategy to advance national interests. Whereas many Indo-Pacific nations continue to view "traditional" cyberattacks against civilian infrastructure as separate from conventional military operations, foreign influence operations, and economic competitiveness, Beijing's behavior suggests an appreciation for how different cyber tactics can complement each other and advance goals beyond the cyber domain. Penetrating the networks of U.S. ports and electricity grids, for instance, could impede military mobilization in the case of a cross-Strait crisis. Exfiltrating sensitive data from the Japanese Foreign Ministry could then inform targeted influence operations to undermine the government. Several examples underscore how Beijing uses cyber operations to advance real-world objectives, from increasing diplomatic pressure, undermining foreign democracies, or pilfering valuable trade secrets and technology.

Similarly, there is evidence that the PRC uses cyber operations to reinforce events in the physical domain. For example, the PRC's malicious cyber activity increases sharply during maritime flareups with the Philippines over the disputed Second Thomas Shoal in the South China Sea.[38] Similar cyberattacks have accompanied maritime disputes between the PRC and Vietnam.[39] Ahead of Taiwan's elections in January 2024, Chinese-linked cyberattacks increased almost 850 percent compared to the same period the prior year.[40]

Beijing also uses the cyber domain to make the world safe for the CCP by attempting to surveil and silence critics at home and abroad, undermine democratic governance, and burnish its authoritarian model by comparison.[41] Beyond Beijing's Great Firewall, which tightly controls the domestic information ecosystem, Chinese cyber actors monitor CCP critics across the Indo-Pacific—including dissidents and journalists—to repress free speech.[42] There is evidence of PRC-linked, large-scale Distributed Denial-of-Service (DDoS) attacks against apps favored by prodemocracy activists in Hong Kong, such as Telegram and FireChat.[43] Similarly, PRC-linked hackers reportedly used malware and phishing to target the Uyghur diaspora, the Dalai Lama, and members of the Tibetan parliament.[44] In leaked documents, I-Soon, a private Chinese cybersecurity firm, claimed it targeted and monitored ethnic minorities, foreign universities, and governments in the Indo-Pacific.[45] The documents listed China's Ministry of

Figure 1: People's Republic of China (PRC) Cyber Toolkit



The PRC wields an expanded range of cyber operations to advance its interests, complementing traditional espionage and data exfiltration with information operations and pre-positioning in critical infrastructure.

Chinese Communist Party General Secretary Xi Jinping delivers a keynote speech at the opening ceremony of the Second World Internet Conference in east China's Zhejiang province on December 16, 2015. In his speech, Xi outlined his vision of "cyber sovereignty"—a concept that has drawn criticism from researchers for promoting strong state control over the internet and advancing authoritarian norms in global cyberspace governance. (STR/AFP via Getty Images)

State Security, Ministry of Public Security, and the People's Liberation Army (PLA) as some of I-Soon's biggest clients.[46] Every year around the anniversary of the Tiananmen Square protests, activists and international organizations have endured a surge of malicious, PRC-linked cyber activity.[47] The PRC continues to deny involvement in these attacks.

A longtime goal of Chinese cyberactivity is IP theft. International partners have repeatedly criticized the PLA and Ministry of State Security for its cyber-enabled theft of trade secrets for the PRC's commercial and strategic benefit. In October 2023, the Five Eyes Alliance issued a rare public warning about Chinese IP theft. At the time, the director-general of Australia's Security and Intelligence Organisation deemed it "the most sustained scaled and sophisticated theft of intellectual property and expertise in human history."[48]

In late 2024, the U.S. government uncovered perhaps the most far-reaching, sophisticated, and aggressive PRC cyber operation to date, dubbed "Salt Typhoon." The attack infiltrated at least nine U.S. infrastructure and telecommunications companies to record and geolocate millions of calls placed by Americans.[49] U.S. officials also believe the attack gave the Chinese hackers access to the phone calls and text messages of senior U.S. elected officials, including President Donald Trump and Vice President J.D. Vance. Senator Mark Warner, Vice Chair of the Senate Select Committee on Intelligence, called it "the worst telecom hack in our nation's history."[50]

The United States is not alone. Kazutaka Nakamizo, the deputy director of Japan's National Center of Incident Readiness and Strategy for Cybersecurity (NISC), described how PRC-backed hackers had increased attacks against internet and telecommunications providers, among other critical infrastructure operators.[51]

These operations reflect a troubling shift in the PRC's cyber posture from a traditional focus on espionage and data exfiltration to pre-positioning in critical infrastructure across the Indo-Pacific for leverage in a future conflict.[52] In January 2024, former U.S. FBI Director Christopher Wray testified that hackers linked to the PRC were preparing to "wreak havoc and cause real-world harm to American citizens and communities" by burrowing into critical infrastructure, including electrical grids, transportation systems, water treatment plants, and pipelines for oil and gas.[53] The former head of U.S. Cyber Command, General Timothy Haugh, described how recent operations by groups like Volt Typhoon contrast with prior intrusions: "One of the reasons we believe it is pre-positioning is—there are not tools being put down and there's not data being extracted."[54] He pointed to Volt Typhoon's infiltration of a water system in Guam, a U.S. territory in the Pacific, that would play a vital role in any future military confrontation with the PRC.[55]

Important but less understood are the PRC's ambitions to shape global cyber governance and standards-setting bodies to align with Beijing's vision of "cyber sovereignty."[56] CCP General Secretary Xi Jinping laid out this vision at the 2015 World Internet Conference, describing cyber sovereignty to mean "respecting each country's right to choose its own internet development path, its own internet management model, and its own public policies on the internet."[57] Behind the gauzy language is an effort to establish a normative predicate for strong government control over the internet, laying the ground

for a future of several, tightly controlled national internets. This starkly contrasts with the longtime U.S. commitment to an open, global internet free of censorship. Indeed, the PRC's cyber operations point to a bald discrepancy between its actual conduct and notional commitments to responsible state behavior in cyberspace—for instance, not engaging in commercial espionage and opposing the militarization of cyberspace.[58]

At the same time, the PRC is actively exporting digital infrastructure and services through its Digital Silk Road initiative, where Beijing and Chinese companies collaborate to deploy subsea fiberoptic cables, 5G networks, satellite communications, e-commerce platforms, and more, in key emerging markets, often accompanied by memoranda of understanding with nations like Vietnam, Myanmar, and Indonesia to align on underlying technical standards.[59] The expansion of China's digital infrastructure in the form of Huawei-built 5G networks and submarine cables also expands China's economic and political leverage, along with its ability to harvest sensitive data. Similarly, the expansion of Chinese-linked technology platforms, like TikTok, pose not only concerns for data security but potential influence operations.

[These activities] point to the PRC's increased willingness to spy, steal, scare, and even sabotage competitors.

Taken together, these activities form part of a broader Chinese strategy to challenge the existing international order and assert Beijing's influence.[60] They also point to the PRC's increasing willingness to wield cyber power to spy, steal, scare, and even sabotage competitors. Facing serious pressures from an economic slowdown, aging population, and rising geopolitical tensions with many Indo-Pacific neighbors, the PRC has become increasingly aggressive in how it uses cyber and other means to achieve its goals.[61]

NORTH KOREA

North Korea is among the world's poorest, most isolated, and cyber-aggressive nations. These traits are inextricably linked: North Korea's cyber operations are fundamental to its strategy to both mitigate the effects of international sanctions, finance weapons of mass destruction (WMD) and ballistic missile development, and weaken its neighbor to the south.[62] Understood this way, North Korean cyber operations differ from other state actors in the Indo-Pacific in their focus on global financial theft and regional targeting of South Korea, although the government also uses cyber operations for more traditional espionage, statecraft, and exfiltration of commercial and military technologies it could not otherwise acquire.

Even as its population lacks basic necessities, North Korea has made substantial investments in its cyber capabilities. It ranks fourth for state-sponsored cyberattacks, conducting at least 89 since 2003.[63] More than half of its cyberattacks target South Korea and the United States.[64] More than most state actors, North Korea uses cyber operations to illicitly acquire funds through ransomware, social engineering, and malware attacks on cryptocurrency exchanges.[65]

According to UN experts, North Korean cyberattacks generated more than $3 billion over six years, enabling the government to increase its funding of WMD and ballistic missile development.[66] The U.S. government estimates that revenue from cyber operations fund approximately half of North Korea's weapons program.[67] Recent North Korean malicious cyber activities targeted the United States and South Korean health sectors, alongside broader critical infrastructure, using ransomware to elicit payments in cryptocurrency in return for restoring access to data.[68]

The country's cyber operations are often executed by entities, such as the Lazarus Group and APT38, which are linked to North Korea's Reconnaissance General Bureau.[69] The U.S. government charged the Lazarus Group with perpetrating the 2014 malware attack on Sony Pictures and the 2017 WannaCry ransomware attack, which impacted organizations both in the Indo-Pacific and across the globe.[70] The North Korean government has denied these accusations. In February 2025, the Lazarus Group stole $1.5 billion from the cryptocurrency exchange, Bybit, one of the largest ever financial thefts.[71] As long as North Korea can bypass sanctions and raise significant funds through cyber operations, strong incentives will remain to continue its cyber aggression.[72]

The PRC has been a key enabler of North Korea's malicious cyber activity. A significant share of North Korea's internet traffic transits through the PRC, whose government reportedly turns a blind eye to North Korean cyber actors operating within its borders.[73] There are also reports of North Korean government hackers going to the PRC for cyber training, while Chinese front companies play an active role in helping North Korean IT workers bypass sanctions and launder online currencies.[74] Cooperation with the PRC is thus essential to managing the North Korean cyber threat, but growing tensions with Washington sharply limit Beijing's interest in playing a constructive role, and may indeed increase incentives for just the opposite.[75]

North Korea's cyber operations are fundamental to its strategy to both mitigate the effects of international sanctions, finance weapons of mass destruction and ballistic missile development, and weaken its neighbor to the south.

RUSSIA

Russia ranks second only to the PRC for conducting cyberattacks around the world.[76] It presents a dangerous combination of sophisticated cyber capabilities and a high propensity to wield them in conspicuous, aggressive, and boundary-pushing ways.

Underscoring Russia's cyber reach and recklessness was its global cyber operation in 2017, targeting devices like routers and switches as points of entry for malicious activity, including espionage, IP extraction, and persistent access to lay the groundwork for future operations.[77] Although Russia's cyber operations have primarily focused on Europe and the United States, it remains a key if underappreciated cyber actor in the region. Several Indo-Pacific nations have fallen into Russia's digital crosshairs, enduring operations from threat actors linked to the Main Intelligence Directorate (GRU), the country's foreign military intelligence service.[78]

In 2018, *The Washington Post* reported that, according to U.S. intelligence, Russian military spies had hacked hundreds of computers ahead of the 2018 Winter Olympics in South Korea in a "false flag" operation that made it appear as if the attack came from North Korea. The GRU-linked operation was likely to protest its ban from the games over allegations of doping.[79] For similar reasons, the Russia-sponsored actor known as Fancy Bear (alternatively, APT28 or Strontium) targeted over 16 organizations with cyber operations ahead of the 2020 Tokyo Olympics.[80] The same group has also targeted defense officials in Japan and South Korea.[81]

Although Russia-sponsored cyber operations are less prevalent in the Indo-Pacific compared to those linked to the PRC or North Korea, leaders across the region have paid close attention to the Kremlin's offensive cyber operations in Ukraine. The war in Ukraine underscored Russia's willingness to use cyber operations to reinforce military objectives and cause direct physical destruction. According to the cybersecurity firm Mandiant, hackers affiliated with Russia's GRU military intelligence agency used a cyberattack to cause a widespread power blackout coinciding with the start of a missile strike against Ukrainian critical infrastructure.[82] To date, the GRU hacker unit, known as Sandworm, is the only group to have successfully triggered a blackout through a cyberattack.

Russia's actions in Ukraine serve as a warning to governments in the region contending with Beijing's aggressive pre-positioning, and as a demonstration of Russia's capabilities should its regional focus shift.

Cybercriminals

Cybercrime is among the fastest-growing threats in the Indo-Pacific, fueled by rapid digitalization, low cyber hygiene, and widespread availability of malicious cyber tools.[83] The combination of rapid growth and weak cybersecurity across the region creates powerful incentives for cybercrime.

Cybercriminals, typically motivated by financial gain, exploit both cyber and social vulnerabilities using tactics, such as ransomware attacks, phishing campaigns, and data exfiltration. In some cases, governments have allegedly hired cyber criminals to attack foreign companies, either independently or in concert with state-sponsored actors. The Biden administration blamed China's Ministry of State Security for hiring cybercriminals to spy on U.S.

companies for commercial advantage, and European intelligence agencies have observed hackers conducting operations in close parallel with those initiated by Chinese authorities.[84]

In ransomware attacks, a cybercriminal denies a user access to their files until they pay a ransom to the attacker. In a malware attack, the attacker uses malicious software to execute unauthorized actions on the victim's system without their knowledge. In practice, these categories often overlap, with cyber attackers often employing malware to access a system to spy, steal, sabotage, or extract ransom. These criminal attacks can have national consequences. For example, in June 2024, cybercriminals successfully compromised Indonesia's national data center and shut down access to several government services, including immigration, effectively halting entry into the country.[85] The attackers demanded $8 million in ransom, leveraging the widespread impacts for financial gain.[86]

Access to cybercrime tools has never been easier, supported by growing availability and professionalism of cybercrime-as-a-service.[87] Executing a successful cyberattack is no longer restricted to those with specialized cyber capabilities and expertise. Malicious actors can pay as little as $40 per month on the dark web to have ransomware operated on their behalf.[88] Cheaper, scalable tactics make attacks on smaller businesses and individuals more profitable, expanding the pool of potential targets beyond large companies and organizations.[89] The United Nations Office on Drugs and Crime estimates that cyber scams targeting victims in East and Southeast Asia generated financial losses between $18 billion and $37 billion in 2023 alone.[90] The region has also seen a rise of "scam compounds" that exploit a combination of forced labor, weak local governance, and corruption to establish enterprise-level scamming operations in border regions between China, Myanmar, Cambodia, and Thailand.[91] Advances in AI will likely increase cybercrime threats in the Indo-Pacific by enabling more automatic, sophisticated, and targeted phishing attempts in native languages.[92]

Hacktivists

Hacktivists are politically motivated cyber actors who use hacking techniques to promote social, ideological, or political causes.[93] Their activity in the Indo-Pacific is growing. In corrupt or weakly governed states, hacktivists and cybercriminals often flourish. Unlike nation-state actors or cybercriminals, hacktivists are driven primarily by ideological goals rather than financial gain or state-set objectives (although the line between state-backed actors and nationalistic hacktivists is often blurred). Their tactics depend on their objectives, but they often take the form of Denial-of-Service attacks to shut down a site or service, data leaks to cause reputational damage, and website defacements as a form of protest. For example, in 2022, Malaysian hacktivists defaced at least 70 Indian government and private sector websites following perceived anti-Muslim remarks by a member of India's ruling party.[94] In November 2024, the office of the South Korean president described an increased tempo of cyberattacks from pro-Russian hacktivists following the deployment of North Korean troops to Ukraine.[95]

State-sponsored actors, cybercriminals, and hacktivists are not always clearly distinct groups.[96] In some cases, nation-states may explicitly or implicitly enable criminal or hacktivist groups to target geopolitical rivals, for instance, by purchasing exfiltrated data, promising immunity from enforcement, or even recommending targets. Nationalist cybercriminals may structure their operations to avoid domestic impacts or choose targets that support national objectives. Hacktivists with nationalistic aims may also act against other nations they perceive as hostile, even without buy-in from their own government—serving as rogue, ideologically motivated cyber actors.

Disinformation

Disinformation campaigns have become a potent tool for shaping narratives, influencing public opinion, and undermining democratic processes across the Indo-Pacific. Disinformation is the deliberate spread of false or misleading information with malicious intent. Misinformation, by contrast, is the unintentional dissemination of inaccurate or false information.[97] Often supported by cyber means, disinformation can significantly affect political stability, social cohesion, and trust in democratic institutions and norms.[98]

Several Indo-Pacific nations have accused the PRC of sophisticated disinformation campaigns to undermine their democratic institutions. For instance, the

PRC has sought to reshape narratives around contentious issues, such as the South China Sea disputes, Taiwan's sovereignty, and Hong Kong's prodemocracy protests.[99] Additionally, through purchasing local media outlets in the region, the PRC has used commercial ownership to further control media coverage.[100] By manipulating social media and other online platforms, Chinese state-linked actors have worked to create and spread narratives that align with Beijing's strategic interests.[101] Last August, New Zealand's Security Intelligence Service assessed the PRC was conducting influence campaigns against the country, with a focus on targeting local ethnic Chinese communities and individuals with links to the PRC.[102]

Advances in AI are likely to amplify the PRC's disinformation campaigns by boosting volume, targeting, and culturally tailored content.[103] These disinformation campaigns are challenging longstanding global norms by normalizing authoritarian rule and promoting state sovereignty at the expense of individual rights and freedoms.[104]

Russia has also used cyber operations for audacious foreign influence campaigns to undermine democratic governance. The most infamous case was Russia's efforts to influence the 2016 U.S. presidential election through the state-linked Internet Research Agency, although similar influence operations have continued to sow discord and undermine Western support for Ukraine.[105] As Russia faces growing international sanctions and diplomatic isolation, it has escalated its disinformation campaign through state-backed third parties like the Social Design Agency (SDA).[106] For the Kremlin, these campaigns are cost-effective ways to sow discord and undermine adversary governments, exploiting their relatively open societies and social media platforms. According to documents leaked from the Kremlin and published by VSquare, the SDA manufactured nearly 34 million social media comments in just the first quarter of 2024.[107] In 2022, the Australian domestic spy agency reportedly investigated at least one significant effort to boost pro-Russian figures in Australian elections.[108] Although there is not yet evidence of Russian influence operations in the Indo-Pacific on the scale of its efforts in the 2016 U.S. presidential election, there is reason for concern.

The Kremlin's capabilities and experience in cyber-enabled disinformation, willingness to wield these tactics, and assessment that they are both cheap and effective, all suggest that Russia could easily ramp up such campaigns. Indeed, Russia's most effective use of cyber operations since its invasion has been influence operations to undermine support for Ukraine in the Global South.[109]

Growing ties with the PRC also influence Russia's cyber activities in the region, aligning them around a shared interest in challenging U.S. influence and promoting a multipolar world order. As Beijing increases its influence operations in the region and deepens ties with Moscow, it is not hard to envision pathways for Russia—working independently or in concert with the PRC—to escalate disinformation campaigns targeting Indo-Pacific democracies beyond the United States and Australia.

***

COMMON CYBER CHALLENGES AND OPPORTUNITIES

Although the contour of the cyber landscape in Japan, South Korea, Taiwan, and the Philippines depends on their particular context, workshops led by CNAS researchers surfaced common themes and challenges in their efforts to strengthen cybersecurity and resilience. These themes encompass four broad categories: policy, people, partnerships, and progress. This section will briefly describe these areas, while the following sections will provide a more in-depth analysis for each country.

Policy: Legal and Regulatory Frameworks

Legal and regulatory frameworks are essential for a nation's ability to protect its digital assets and respond to cyber threats effectively. These frameworks matter because they signal the prioritization of cybersecurity for domestic and international actors; establish consistent standards; provide guidance to industry on security standards and compliance; create enforceable mechanisms for protecting critical infrastructure; and provide mechanisms for holding accountable and thus deterring malicious actors.

Without robust cyber frameworks, nations face several risks: the technology sector may lack adequate incentives to prioritize security, allowing inconsistent security practices to create vulnerabilities for malicious actors to exploit; businesses lack clear guidance on security requirements or incident reporting obligations; government agencies struggle to coordinate responses to major incidents; and nations have limited means to respond to cyber criminals and state-sponsored threats. For example, when frameworks fail to specify incident reporting requirements, attacks often go unreported, hindering mitigation efforts and governments' understanding of the nature and extent of the threat. Regulations that privilege domestic technology vendors, however well-intentioned, may in practice deny government agencies, private businesses, and critical infrastructure operators best-in-class cybersecurity solutions.

Across the Indo-Pacific, governments have made notable strides in developing and strengthening their policy and legal frameworks. Many countries have introduced national cybersecurity strategies and regulations, creating the foundation for protecting critical infrastructure and improving cyber resilience. However, work remains to achieve shared cyber objectives, such as intelligence sharing and cross-border incident response.

People: Workforce, Cyber Literacy, and Awareness

Cybersecurity starts with people, including trained cybersecurity professionals, white hat hackers, and cyber-conscious consumers, employees, managers, and policymakers. No technology or policy can replace the indispensable role of a skilled cyber workforce and broad cyber literacy.

Across the Indo-Pacific, the cybersecurity workforce gap grew by 23 percent between 2022 and 2023. In Japan, it grew by a staggering 98 percent.[110] Left unaddressed, this gap will compound as more work falls on fewer trained professionals, leading to burnout, early retirements, or career transitions. Every nation in the Indo-Pacific, along with the United States, faces significant challenges to build a sufficiently robust cyber workforce, literacy, and societal awareness. At the same time, rapid digitalization has outpaced community cyber awareness, leaving people and businesses vulnerable.

As accelerating digitization intertwines the networks of governments, industry, and consumers, robust cyber partnerships become increasingly vital.

In the four countries studied in this report, the cyber workforce gap has left government and industry vulnerable and struggling with timely incident detection and response.[111] Workshops led by CNAS researchers also found that governments struggle to compete with the private sector over a limited talent pool—and in the case of the Philippines, with the allure of higher paid opportunities abroad. The workshops also revealed that the workforce shortage has hindered regional cyber partnerships, as governments struggle to recruit and retain the experts needed to advance engagement.[112]

Partnerships: Public-Private and International Collaboration

As accelerating digitalization intertwines the networks of governments, industry, and consumers, robust cyber partnerships become increasingly vital. Partnerships between government and industry are particularly critical: the private sector, which is often on the front lines of cyber defense, holds critical data, best-in-class technology, and operational expertise that governments may lack, while governments have access to classified cyber threat data and insights, as well as the policy levers to improve cybersecurity standards, information sharing, and resources across sectors. Although the workshops revealed strong agreement on the importance of public-private partnerships, they also confirmed that uneven implementation and technology adoption remain a challenge. Specifically, the workshops underscored the need to move from high-level frameworks and rhetorical commitments toward tangible outcomes, such as mechanisms for incident reporting, threat sharing, IT modernization, and workforce training.[113]

In most cases, workshops led by CNAS researchers also revealed an urgent need to strengthen trust between government and industry.[114] Businesses are often reluctant to report incidents and share detailed post-attack forensics, owing to either a lack of formal mechanisms to do so, fear that reporting would risk their public reputation and potential liability, or concern that government counterparts would not adequately secure sensitive, proprietary information. Governments, for their part, need to grow more comfortable disclosing threats against their own infrastructure and personnel, and cyber intelligence, while breaking down bureaucratic cultures that disincentivize collaboration and information sharing within government. They must also prioritize replacing vulnerable, legacy IT infrastructure with cutting-edge technology solutions, including cloud services, and AI-enabled cyber defenses. Governments can also strengthen and clarify procedures for securing sensitive data shared by businesses for cyber incident reporting. (Of course, these dynamics all exist in the United States as well.) The four case studies in the next section further explore differences in how Japan, South Korea, Taiwan, and the Philippines approach public-private partnerships to identify best practices that Indo-Pacific governments could adopt and scale.

Cyber threats do not respect sovereign borders, which makes international partnerships essential.[115] Here, the Indo-Pacific has shown leadership. Governments in the region established the ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE) to expand training opportunities and support.[116] ASEAN has also committed to develop a regional cybersecurity strategy and establish an ASEAN Computer Emergency Response Team (CERT) to facilitate intergovernmental communications, threat-sharing, and response.[117] Ambitions to deepen regional cyber partnerships, however, must contend with nascent, uneven, and under-resourced domestic

cyber capabilities and institutions. This points to an opportunity for more mature cyber actors, such as the United States, Australia, and Singapore, to fill the gap by expanding their cybersecurity capacity building, training, and engagement regionwide.[118]

Progress: Implementation, Challenges, and Recommendations

There is no shortage of new cyber policies, agencies, investments, and initiatives across the Indo-Pacific. The common challenge is implementation—closing the gap between rhetoric and reality. Insufficient funding, bureaucratic inertia, flagging political will, and a lack of technical expertise can all sap progress. Workshop participants consistently emphasized the need for continuous follow-through, regular assessments, and clear accountability structures to ensure that governments and industry not only establish cybersecurity policies but adapt them continuously as threats evolve.[119] The four subsequent case studies explore not only the stated cyber objectives and initiatives of each country but also assess their progress in implementation.

***

JAPAN

Japan is one of America's most vital allies, not only in the Indo-Pacific, but across the globe. Following the Second World War, the U.S.-Japan relationship flourished into a comprehensive strategic partnership. The Treaty of Mutual Cooperation and Security between the United States and Japan, signed in 1960, bound the nations to mutual defense and allowed for the continued presence of U.S. military personnel and assets in the country. Today, over 55,000 U.S. military personnel are stationed in Japan, and bilateral defense cooperation has deepened significantly. Japan now acquires more than 90 percent of its defense imports from the United States, and Washington has both deployed and sold cutting-edge military assets to Japan, such as the F-35 Joint Strike Fighter.[120]

U.S.-Japan economic ties also run deep. American companies in every sector, from retail to finance to technology, have significant operations in Japan. For its part, Japan has also invested over $480 billion in the United States, and Japanese companies support over 860,000 American jobs.[121] As Washington seeks to reorient toward the Indo-Pacific to meet an increasingly assertive PRC, Japan's importance has only grown. At the same time, uneven cybersecurity has emerged as a significant barrier to deeper bilateral ties.

Despite Japan's technological prowess, cybersecurity has historically lagged. For years, Japan's pacifist postwar constitution impeded the adoption of active cyber defenses, as well as the collection and sharing of threat intelligence. Stovepiped cybersecurity capabilities across the government have compounded the challenge. In a 2018 episode that was both embarrassing and revealing, Japan's minister overseeing

cybersecurity admitted he had never used a computer.[122] A 2021 study from the International Institute of Strategic Studies criticized Japan's small cyber force, limited cyber defense funding, lack of national cyber leadership, and shortage of cyber expertise.[123]

In 2022, Admiral Dennis Blair, former U.S. director of national intelligence, bluntly described Japan's cyber capabilities as "minor league." The sharp remarks from a senior U.S. official, known as the "Blair Shock," helped galvanize action from the Diet (Japan's national legislature).[124] Blair's comments reflect renewed pressure on Japan to bolster its cybersecurity and resilience to meet rising threats. Washington understands that stronger Japanese cybersecurity is essential to realizing shared aspirations for greater bilateral intelligence sharing, security cooperation, and technology partnerships, which have assumed new urgency given rising tensions with the PRC.[125]

Arguably, no factor was more important in spurring changes in Japan's cyber posture than Russia's 2022 invasion of Ukraine. Brazen Russian cyberattacks against Ukrainian critical infrastructure, combined with broad information operations targeting not only Ukraine but its supporters worldwide, underscored the hybrid nature of modern warfare and the risk to nations unprepared to wage it.

All of this led to a historic shift in Tokyo's security posture. Japan's 2022 National Security Strategy (NSS) made cybersecurity a pillar for the first time and expanded the mission of its Cyber Command.[126] The government also pledged to increase its cybersecurity spending tenfold over five years, while increasing the number of "cyber warriors" in Japan's Self-Defense Forces (JSDF) to 4,000.[127] This is the floor of what is required in an increasingly dangerous landscape of cyber threats.

Threats

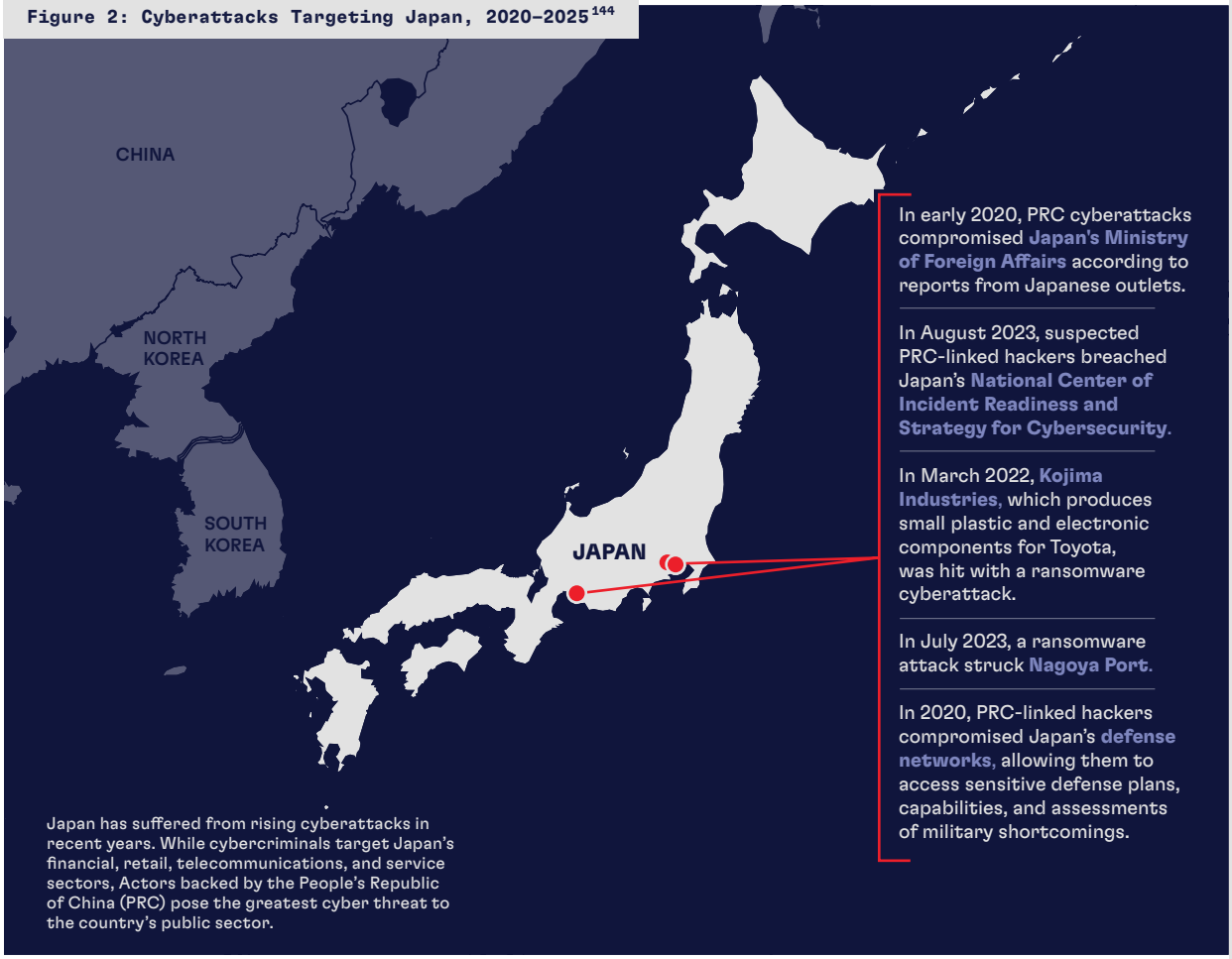
Japan has suffered from rising cyberattacks in recent years, which have laid bare the nation's digital vulnerabilities.[128] A survey from ISC2, an association of cybersecurity professionals, found that 63 percent of its Japanese members believed the threat landscape had become "more challenging than it's been in the past five years."[129] According to Japan's National Police Agency (NPA), cases of suspicious internet access in Japan by foreign nations more than doubled between 2019 and 2023.[130] The financial, retail, telecommunications, and services sectors remain the most attacked, with cybercriminals focusing their efforts on SMEs, which are more vulnerable.[131] Participants at the workshop in Tokyo noted that while APT attacks represent just a fraction of all cyber incidents in the country, they command the vast majority of government officials' time for response and mitigation.[132]

PRC-sponsored threat actors remain the greatest danger, increasingly targeting Japan with APT attacks that allow attackers to gain access to a network and remain undetected for extended periods to exfiltrate sensitive data. Japanese outlets have reported that, in early 2020, Chinese cyberattacks compromised Japan's Ministry of Foreign Affairs (MoFA) and leaked classified diplomatic information overseas. However, senior government officials have not confirmed either the nature of the leak or exposure of classified information.[133] In August 2023, hackers allegedly linked to Beijing breached Japan's cybersecurity agency, the National Center of Incident Readiness and Strategy for Cybersecurity (NISC), potentially accessing sensitive data stored on its networks over a nine-month period before their discovery.[134]

Japan also faces threats from hacktivists, malware attacks, and foreign-based cyber criminals.[135] In 2021, pro-Russian hacker groups, including NoName057(16) and the Cyber Army of Russia, launched DDoS attacks against Japan's ruling Liberal Democratic Party and local government websites, forcing several offline. These attacks coincided with a scheduled joint military exercise between Japan and the United States.[136] The following year, a Russian hacktivist group hit 20 Japanese government websites across four ministries using DDoS attacks.[137] Some experts speculated that the attack was Russian retaliation following Japan's support for Ukraine.[138]

A 2023 report from the IT security company TrendMicro found that Japan had the most malware detections compared to the United States, Italy, Brazil, and India, with a significant portion originating from foreign governments.[139] In particular, North Korea–sponsored threat actors have targeted ransomware attacks against Japanese financial and cryptocurrency institutions to raise funds for the Kim Jong Un regime. From 2017 to 2023, Japan lost $720 million worth of cryptocurrency to hackers affiliated

Figure 2: Cyberattacks Targeting Japan, 2020–2025[144]



with North Korea, equivalent to around 30 percent of cryptocurrency losses to Pyongyang worldwide over this period.[140]

Japanese industry and critical infrastructure operators have also faced increased cyber threats. In March 2022, a ransomware attack on Kojima Industries, a key supplier for Toyota, shut down 14 factories for 24 hours.[141] In July 2023, another ransomware attack struck the port at Nagoya, affecting an estimated 15,000 containers and related businesses.[142] Lockbit, a Russia-based cybercrime operation, claimed responsibility.[143]

Stakeholders

The increasingly dangerous cyber landscape has spurred several new Japanese government agencies and offices:

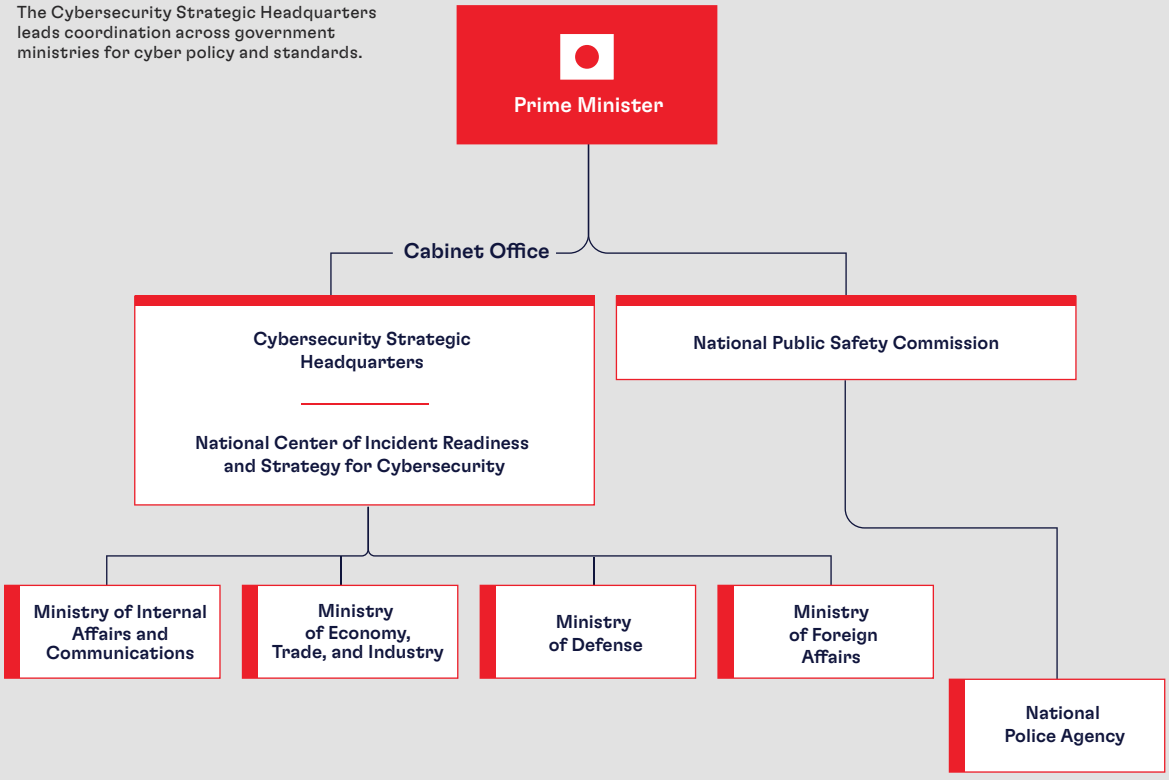
- **CYBERSECURITY STRATEGIC HEADQUARTERS (CSSH):** leads coordination across government ministries for cyber policy and standards from the Cabinet Secretariat of the Prime Minister's Office (Kantei).
- **NATIONAL CENTER OF INCIDENT READINESS AND STRATEGY FOR CYBERSECURITY (NISC)**: acts as the CSSH's operational arm and works directly with ministries to implement the National Cyber Strategy. It also serves as the main point of contact for international collaboration.[145]
- **MINISTRY OF INTERNAL AFFAIRS AND COMMUNICATIONS (MIC)**: promotes the security and resilience of Japanese telecommunications and local municipal governments.

- **MINISTRY OF ECONOMY, TRADE, AND INDUSTRY (METI)**: maintains a cybersecurity division that publishes electricity, energy, and manufacturing guidelines for both the public and private sectors.[146]
- **MINISTRY OF DEFENSE (MOD)**: oversees the JSDF, which has created cybersecurity divisions and expanded cybersecurity training.
- **NATIONAL POLICE AGENCY (NPA)**: oversees investigations and responses related to cybercrime. In April 2022, the NPA launched a 200-member cybercrime investigation team.[147]
- **MINISTRY OF FOREIGN AFFAIRS (MOFA)**: manages bilateral, regional, and international cyber diplomacy and partnerships. Japan's cyber diplomacy has focused on promoting the rule of law in cyberspace, developing confidence-building measures, and cyber capacity building.[148]

Industry also plays a critical role in defending Japan's cyberspace, although government statistics suggest that domestic companies have been slow in integrating cybersecurity best practices.[150] Even as companies like NTT—the major Japanese telecommunications firm—become leaders in Japanese cyber defense, many firms continue to outsource cybersecurity rather than adopt expertise among their own staff.[151] Japan's concern with "*anzen daiichi*," or "safety first," practices that do not tolerate mistakes, along with the difficulty of adopting digital infrastructure and software that can handle the Japanese language's different writing systems, can at times inhibit the adoption of more cutting-edge (ICT) platforms.[152]

Figure 3: Japan's Cybersecurity Agencies[149]

The Cybersecurity Strategic Headquarters leads coordination across government ministries for cyber policy and standards.



Policy

Japan's cyber policies do not lack for volume or ambition. Japan's challenge remains matching new policy frameworks for cybersecurity with sufficient resources and follow-through, along with enacting constitutional reforms to improve threat intelligence collection and sharing and to enable active cyber defense, a term of art for proactive cyber operations to disrupt threats at their source. For instance, Article 9 of Japan's constitution prohibits maintaining military personnel and the offensive use of forces. Under Japanese law, taking action to disrupt malicious cyber activity is only permissible after an "emergency or military attack" has occurred. Another legal hurdle is Article 21, which restricts the government's ability to gather and share domestic signals intelligence to identify and monitor cyber threats. Such intelligence sharing is vital to bilateral and multilateral cybersecurity cooperation.[153]

Japan's cybersecurity policies date back to the First National Strategy on Information Security in 2006. The strategy established an Information Security Policy Council to oversee cyber policies and coordination; identified critical infrastructure sectors for cyber protection; and proposed various efforts to boost incident response, public-private collaboration, and public cyber awareness. The strategy, however, suffered from weak enforcement, a narrow focus on critical infrastructure at the expense of the broader economy, and vague guidelines for implementation. It also focused on more conventional threats like cybercrime without sufficiently addressing more sophisticated, state-based techniques, such as APT attacks attributed to Chinese-linked actor MirrorFace.[154]

Since 2013, Japan has introduced or revised major cybersecurity-related policies at least six times:

- **2013 CYBERSECURITY STRATEGY**: expanded the critical sectors requiring heightened cybersecurity, such as transportation and health care, strengthened coordination between government agencies and NISC, and elevated the cyber domain for national security, and MoD's role accordingly.[155]

- **2014 CYBERSECURITY BASIC ACT**: clarified and rationalized civilian roles in cybersecurity across government to better resemble the governance models of allies such as the United States.[156] The act also converted the Information Security Policy Council into the CSSH and clarified its role and responsibilities.

- **2015 CYBERSECURITY STRATEGY**: further broadened the strategy's scope beyond critical infrastructure to reflect Japan's rapidly digitizing economy to areas such as cloud computing and connected devices, while calling for common cyber standards, stronger reporting, and improved coordination within government.[157]

- **2018 CYBERSECURITY STRATEGY**: elevated preparation for large-scale attacks ahead of the Tokyo 2020 Olympics, specifically noting the risk of state-sponsored APT attacks and emphasizing greater resilience in key government agencies and critical infrastructure. Notably, the 2018 strategy made the first reference to Japan's deterrence capabilities in cyberspace.[158]

- **2021 CYBERSECURITY STRATEGY**: continued the shift toward elevating the cyber domain in national security and named the PRC, Russia, and North Korea as key threat actors. The strategy also emphasized the need to counter digital surveillance and repression in cyberspace. It also began the historic shift to active cyber defense.

- **2022 NATIONAL SECURITY STRATEGY**: embraced active cyber defense, elevated cybersecurity as a key pillar in Japan's NSS for the first time and set an ambition for the country to become a "Global Cyber Leader."[159]

The 2022 NSS was a watershed in Japan's security posture, calling for a defense budget equal to 2 percent of the GDP by FY 2027. The shift responded directly to the deteriorating security environment in the Indo-Pacific, driven by the PRC's growing military threats against Taiwan, increased efforts to contest Japan's administration of the Senkaku Islands, and maritime aggression in the South China Sea. Russia's war in Ukraine also heavily influenced the 2022 NSS by underscoring the dangers of hybrid war and exposing the vulnerability of Japan's existing security posture, policies, and institutions.[160] Russia's enhanced defense collaboration with the PRC compounded these concerns, along with escalating missile and nuclear threats from North Korea.[161]

The 2022 NSS also called on the government to enhance information warfare capabilities and engage in active cyber defense.[162] It explicitly called for Japan to develop cyber response capabilities "equal to or surpassing the level of leading Western countries," as well as for a new body to wage information warfare.[163] Beyond this, the NSS directed MoFA and MoD to integrate AI tools to enhance intelligence analysis and monitoring of the information domain. Accordingly, the government has increased the budget for information warfare within MoFA, MoD, and NPA.[164] As of March 2025, the JSDF continues to refine its doctrine for cyberspace, and its cyber command and control remains underdeveloped.[165]

Another major shift in Japan's cybersecurity policy came in May 2024, when the Diet modernized the country's security clearance mechanism to better align with equivalent systems in the United States and other security partners.[166] The new Economic and Security Information Act builds on the 2014 Act on the Protection of Specially Designated Secrets, which only covered sensitive government information, to include sensitive information related to economic security, cybersecurity, technology, critical infrastructure, and supply chains.

In May 2025, the Japanese cabinet approved two bills to strengthen active cyber defense and reporting for potential cyber operations targeting critical infrastructure. The active cyber defense bill has three key elements. First, it authorizes the government to monitor limited information about communications between Japan and abroad when there are suspicions of cyberattacks. Second, it requires critical infrastructure operators to report cyberattacks to the government, which in turn will counsel on mitigation and response. Third, it clarifies that the police and the JSDF can conduct active defense measures to penetrate and neutralize attackers at the source, with permission from an independent committee.[167] Now, the focus turns to implementation.

People

Japan has the most cybersecurity professionals in the Indo-Pacific but also the largest cyber workforce gap.[168] Between 2022 and 2023, the gap grew by 98 percent.[169] The country's aging population compounds the problem with an older, less technologically literate workforce, and a smaller pool of students and early-career professionals.

The government has launched several initiatives to address this. METI established the Industrial Cybersecurity Center of Excellence in 2017, which offers a year-long training program for professionals in critical infrastructure sectors.[170] Since its inception, the initiative has trained at least 350 graduates.[171] Japan's Information Technology Promotion Agency has also created the Digital Skills Standards, which serves as a framework to guide the country's digital transformation.[172] NISC has also increased recruitment of white hat hackers to identify potential cyber risks.[173]

The JSDF also faces a shortage of cyber professionals. In 2012, the JSDF had only 100 people in its cyber defense unit.[174] A new regional cyber defense unit in 2019 added another 60 personnel, situated within the Western Army of the Japan Ground Self-Defense Force.[175] After the 2022 NSS, the government directed the MoD to boost its total "cyber warriors" to 4,000 and provide cybersecurity training to at least 16,000 JSDF personnel within five years.[176] To that end, the JSDF plans to create a specialized test for officer candidates, which represents one in five JSDF members, in its cyber unit starting in FY 2025.[177]

According to a Japanese defense official, as of April 2024, the MoD had recruited 2,230 members of its new cyber unit, but recruitment of cyber professionals remains a challenge.[178] One reason for the recruiting challenge is uncompetitive compensation: a private sector cybersecurity specialist in Japan can expect annual salaries of up to 100 million yen, while a general SDF officer can earn just 2.9 million yen.[179] The JSDF has proposed new allowances for special duties such as cyberspace within the FY 2025 budget, but it will take time for corrections based on government versus private pay imbalances.[180] Even if the JSDF reaches its 4,000-person target, its "cyber warriors" will remain far lower than the 6,800 cyber specialists reportedly tied to North Korea, or China's cyberattack force of 30,000.[181]

The Japan Directorate for Signals Intelligence also remains small and underfunded, leaving it heavily reliant on the U.S. National Security Agency.[182] The directorate has been providing intelligence support to cyber operations since 2012, but only had about 1,700 personnel as of 2018.[183] Over the years, Tokyo

has generally invested funding into new weapons platforms instead of its cyber capabilities, although the JSDF's FY 2024 budget provisioned nearly $12 billion for the expansion of the Japan Ground Self Defense Force System, Signal and Cyber School.[184]

Partnerships

A hallmark of Japan's cyber policy is international partnerships. Tokyo has set an explicit goal to become a global leader in cyber diplomacy, with a focus on promoting norms of responsible state behavior consistent with its broader international engagement around technology and digital issues.[185] Priorities of Japan's cyber diplomacy include capacity building abroad and promoting confidence-building measures and the rule of law in cyberspace.[186] To that end, Japan actively participates in international and regional cyber partnerships. Tokyo participates in the G7 Cyber Expert Group and is a party to the Convention on Cybercrime.

Japan's cyber diplomacy has been especially active in the Indo-Pacific, with a focus on establishing CERTs. Japan launched its own CERT (JPCERT) in 1996, and Tokyo has since been instrumental in establishing the ASEAN-CERT and launching the ASEAN-Japan Cybersecurity Capacity Building Centre in Bangkok, which helps standardize incident reporting frameworks regionwide.[187]

Japan also maintains several cyber dialogues, including with Australia, the EU, France, India, the United Kingdom, South Korea, and Israel.[188] In a March 2024 meeting, Japan and India's foreign ministers also agreed to enhance cooperation in cyberspace. The following month, Japan, the United States, and the Philippines agreed to form a defense network against cyberattacks at their first-ever trilateral summit.[189] The United States, Japan, India, and Australia have also established the Quad Cybersecurity Partnership to promote joint cyber principles, an outcome of which is accelerating cybersecurity capacity-building projects in the Philippines and India.[190]

Beyond the Indo-Pacific, Japan is one of the few Asian nations that has active cyber cooperation with NATO, participating in its annual cyber exercises since 2021.[191] Japan actively participates in the United Nations' cyber-related forums, including the Group of Governmental Experts, and the Open-Ended Working Group.[192]

Japan's most important cyber partnership is with the United States. For years, Washington has provided regular signals intelligence, capacity building, technical assistance, and diplomatic engagement to support Tokyo's shift to active cyber defense and align with cyber standards and practices of other leading economies. Although U.S.-Japan cyber cooperation has remained strong for over a decade, the deteriorating security environment in the Indo-Pacific has elevated it in the bilateral agenda.

The CNAS Technology and National Security Program and Indo-Pacific Security Program host a private roundtable on cybersecurity in the Indo-Pacific with the Japan Institute for International Affairs on April 19, 2024. (Michael Depp/CNAS)

During the most recent 2+2 meeting in July 2024, both governments emphasized the foundational importance of cyber and information security for the alliance and committed to zero trust architecture to build resilience in information and communications technology.[193] Bilateral cyber cooperation has also advanced through the U.S.-Japan Dialogue on Digital Economy. In the 2022 session, both countries agreed to expand cooperation on a host of cyber-related issues, from adopting AI and the cloud, to organizing cybersecurity capacity building for ICT infrastructure in third countries.[194]

Cyber cooperation has also advanced in the military domain, with the U.S. Department of Defense (DoD) and Japanese MoD establishing a U.S.-Japan Cyber Defense Policy Working Group in October 2013, driving cooperation around information security, defensive cyber operations, and aligning the two countries' respective cyberspace missions given different capabilities and legal contexts.[195]

Although the U.S.-Japan Treaty of Mutual Cooperation and Security provides some legal basis for the forward deployment of U.S. cyber and intelligence officials to support HFOs within the country, political and legal sensitivities have likely limited their scope. To date, U.S. Cyber Command has focused more on training and consultation with Japanese peers. Absent legal and constitutional reforms, the United States also faces limits on the scope of its active cyber defense operations on Japanese networks.

Tokyo has set an explicit goal to become a global leader in cyber diplomacy.

The U.S. private sector is poised to play a significant role in expanding Japan's cyber capabilities, practices, and personnel. In March 2024, Google announced a regional cybersecurity research hub based in Tokyo.[196] The following month, Microsoft launched a $2.9 billion investment in AI and cloud infrastructure in Japan over a two-year period, with efforts to partner with Japan's CSSH to boost cybersecurity resilience, training, and technology solutions.[197] Not to be outdone, AWS rolled out an investment of over $15 billion through 2027 to expand its cloud computing infrastructure across the country, and the company claims to have trained over 400,000 people in Japan with cloud skills since 2017.[198]

Partnerships with leading technology companies will be vital as Tokyo begins to grapple with the implications of advanced AI models on the offense-defense balance in cyberspace. In Japan's FY 2023 budget, the MoFA pledged to use AI to enhance monitoring of the information space and to strengthen intelligence analysis. For its part, the MoD also committed to introducing an AI-powered information gathering and analysis system for information warfare.[199] Time will tell if Tokyo can close the gap between its policy ambition and real-world capability.

Progress and Recommendations

Japan has undertaken the greatest shift in its security posture since the Second World War, including a historic shift toward active cyber defense. The elevation of cybersecurity as a pillar of the 2022 NSS was also critical to signaling to the national security enterprise, private sector, and international partners that the government recognizes cybersecurity as foundational to national security. Now the question is whether the cyber domain will receive commensurate investment and prioritization as more traditional security priorities. The rubber will meet the road as Japan strives to spend 2 percent of its annual GDP on defense—the equivalent of $320 billion.

A priority for the Trump administration will be maintaining momentum with Japanese Prime Minister Ishiba Shigeru through deeper bilateral cybersecurity cooperation while sustaining constructive pressure to match Japan's new cyber policies and promises with follow-through and investment. The administration should unequivocally convey that cybersecurity ranks among the greatest barriers to expanding bilateral cooperation.

To address these issues, the report offers the following recommendations to leaders in the Japanese government:

Prioritize cybersecurity investments as Japan boosts defense spending to 2 percent of GDP by 2027, consistent with the 2022 NSS. Specifically, Tokyo should prioritize investments to replace at-risk legacy software and IT infrastructure in government, especially in security-relevant agencies; modernize

threat detection and active defense capabilities within the Japan Directorate for Signals Intelligence and the JSDF; and boost compensation to meet the MoD target to train 4,000 "cyber warriors."

Swiftly implement the legislation passed in May 2025 that enables active cyber defense and strengthens reporting requirements. Implementation for key provisions of the new laws will unfold over the next two and a half years, including standing up a cabinet-level body to review and approve cyber operations and the development of legal agreements between the government and telecommunications operators.[200]

Prioritize implementation of the May 2024 reforms to Japan's security clearance system. Sufficient staff, resources, and political prioritization will be essential to timely implementation of the reforms, including completion of background checks, which will facilitate the sharing of classified information between Japan and key allies like the United States.

Create a cyber visa for high-skilled foreign workers to address workforce shortage. The combination of Japan's aging population, reluctance to expand immigration, and growing competition for technology talent will complicate urgent efforts to bridge the cyber workforce gap. Tokyo should consider a special visa with other inducements for top foreign cyber talent.

Empower NISC to require and enforce the adoption of modern cybersecurity technologies and best practices across both the public and private sectors.[201]

Establish pathways between the government and private sector to share sensitive information on cyber threats. The May 2024 reforms improved information-sharing between the Japanese government and foreign counterparts, but gaps remain in the government's ability to share sensitive information with the Japanese private sector. At a workshop hosted by CNAS researchers in Tokyo, participants noted the lack of familiarity among Japanese businesses with handling sensitive information, inhibiting cooperation with the government.[202]

Expand cyber capacity building in the Indo-Pacific, partnering with the United States, Australia, and Singapore wherever possible to maximize resources and limit redundancy.

Prioritize deployment of secure, resilient telecommunications networks in the Indo-Pacific through MoFA overseas assistance. Japan is one of the Indo-Pacific's most generous providers of Official Development Assistance.[203] In 2022, it also created a distinct category of Official Security Assistance to provide nonlethal capabilities to partners to strengthen their "security and deterrence capabilities."[204] Japan is both a more trusted interlocutor than the United States in many Indo-Pacific capitals and a global technology and telecommunications leader. Tokyo has an opportunity to expand its leadership in guiding rapid digitization across the region toward secure, trusted networks for subsea cable infrastructure, 5G, and Open Radio Access Network (RAN) telecommunications networks, and data centers to counter China's Digital Silk Road.

***

SOUTH KOREA

Alongside Japan, South Korea is among America's closest allies in the Indo-Pacific. The 1953 U.S.-Republic of Korea (ROK) Mutual Defense Treaty binds the nations together, and the United States maintains a significant military presence in the country to uphold its commitments and deter aggression—principally from North Korea. As South Korea flourished as a global economic and technology leader in the postwar period, the bilateral alliance matured into a comprehensive partnership spanning trade, space, energy, and more.[205] The presence of significant U.S. military personnel and infrastructure, business operations, and investment gives Washington no shortage of reasons to prioritize South Korea's cybersecurity and resilience.

Rising threats from North Korea have long driven South Korea's cybersecurity policy, with new reforms and investments following high-profile attacks. Although the constant threat from the north spurs vigilance, it may also have led Seoul to over-attribute cyber operations to North Korea—potentially obscuring a rise in PRC-linked operations.[206]

South Korea's position as a global technology leader presents both advantages and disadvantages for its cybersecurity. On the one hand, South Korea's highly educated talent pool means it faces a manageable cyber workforce shortage compared to the other countries examined in this report. Between 2022 and 2023, the cyber workforce gap in South Korea grew just 6 percent, compared to 98 percent in Japan.[207] On the other hand, rapid digitalization has enabled a significant rise in botnet attacks that exploit vulnerabilities in connected devices. World-leading companies like Samsung Electronics and SK Hynix underscore the country's technology leadership, but a desire to protect that leadership has also led Seoul to embrace regulations that privilege domestic technology firms and can sometimes come at the expense of best-in-class cybersecurity solutions.

Threats

Malign cyber operations targeting South Korea are on the rise. Cyberattacks against South Korea's public institutions surged in 2023, with an average of 1.62 million attempted attacks per day.[208] Korea's National Intelligence Service (NIS) reported a 36 percent rise in cyber operations linked to foreign actors.[209] In 2024, the Korea Internet and Security Agency (KISA) reported another 35 percent increase in cyber incidents, driven by 58 percent increase in server hacking and a 23 percent rise in DDoS attacks.[210] Although reported ransomware attacks saw a 31 percent decline over this period, they remain a significant threat.[211] In the first half of 2024, ransomware attackers infected up to 41 percent of backup data with malware.[212] These attacks disproportionately impact South Korean SMEs, which accounted for nearly 94 percent of all reported ransomware attacks between 2023 and 2024.[213]

More broadly, participants at a workshop in Seoul hosted by CNAS researchers described considerable work ahead for South Korea to improve cyber awareness and hygiene—across both the public and private sectors. Best practices such as MFA, burner phones for travel to high-risk destinations like the PRC, and restrictions on the use of personal devices for official business remain alarmingly sparse. They also noted that businesses struggle with paltry cybersecurity budgets compared to U.S. peers and received insufficient government support.[214]

The proliferation of connected devices in South Korea has also multiplied attack vectors for malicious actors. Once compromised, hackers can use connected devices for credential theft, spam, man-in-the-middle attacks, or to weaponize their computing power through botnets for DDoS attacks. South Korea's cybersecurity agencies have identified growth in internet of things (IoT) botnets in 2023, increasing the frequency and severity of such attacks. In addition, South Korea's high internet penetration and bandwidth have made it an attractive target for malicious cyber actors who use the country's robust digital infrastructure to launch attacks on targets in other countries.[215] In response, South Korea's cybersecurity ministries have called for stronger authentication mechanisms, higher security for public Wi-Fi, and improvements to the IoT security certification system.[216]

State-sponsored actors linked to North Korea and the PRC remain the country's principal cyber threat. In recent years, these actors have deployed AI-enabled tools and exploited zero-day vulnerabilities to target critical infrastructure, government institutions, and SMEs. Between January and September 2023, South Korea experienced 17,000 cyberattacks attempting to steal diplomatic intelligence, with over 8,000 cyberattacks targeting South Korea's MoFA.[217]

NORTH KOREA

Seoul has named North Korea its most significant cyber threat.[218] According to South Korea's NIS, 80 percent of cyberattacks against South Korea's public sector in 2023 came from North Korea–backed actors.[219] These attacks typically target government agencies, defense contractors, and financial institutions, incurring at least $650 million in total damages.[220]

Prominent North Korea–linked threat actors include the Lazarus Group, Andariel, and Kimsuky Group, whose sophistication and coordination have increased with time. In 2022, Microsoft reported that the Lazarus Group created fake profiles claiming to be recruiters on LinkedIn, luring targets onto WhatsApp to install malware.[221] The group also infiltrated a defense company's network and gained unauthorized access to sensitive data using malware, despite the company's efforts to separate internal and external networks. The same year, Andariel exfiltrated data from a defense company contractor by installing malware on its servers.[222]

Between 2022 and 2023, South Korea observed coordinated attacks between North Korean cyber groups for the first time. According to the NPA, Lazarus Group, Andariel, and Kimsuky Group hacked into 10 of the nation's 83 defense companies either directly or through subcontractors.[223] Each cyber group used a distinct technique, demonstrating a high level of technical expertise and coordination to maximize disruption.

In 2023, South Korea observed coordinated attacks between North Korean cyber groups for the first time.

North Korean cyber groups have placed greater focus on exploiting zero-day vulnerabilities within South Korean systems. Analysis by KISA finds that the Lazarus Group continuously steals and analyzes source code to find zero-day vulnerabilities in South Korean software, analyzing it for a year, on average, before attempting to infiltrate the target's network.[224] The group is also becoming more adept at using publicly available information, like social media, to better target attacks. In 2024, the Lazarus Group successfully conducted phishing attacks against South Korean workers by impersonating employees of a Chinese virtual asset investing company.[225]

THE PEOPLE'S REPUBLIC OF CHINA

In 2023, the NIS attributed only 5 percent of cyber operations from foreign sources to China.[226] At the same time, the Korean spy agency noted that attacks from China tended to inflict more severe damage despite being less frequent, accounting for 21 percent of all "cybersecurity incidents of high significance" that year. The NIS also characterized these attacks as a "slow and stealthy infiltration," but declined to attribute responsibility to the government, preferring instead to point out its origins in China.[227]

Even as Seoul remains reluctant to attribute rising cyber operations to Beijing, the People's Liberation Army's (PLA) cyber espionage group, TAG-74, continues to target South Korean academic institutions and government entities.[228] In 2023, the NIS

confirmed that PRC-sponsored actors attempted to breach South Korea's national satellite communication network.[229] Although officials detected the breach quickly, the hacker still gained access to the network management system, underscoring its vulnerabilities.[230] The incident prompted NIS, KISA, and the Ministry of Science and ICT (MSIT) to strengthen security systems for space and aviation infrastructure.[231]

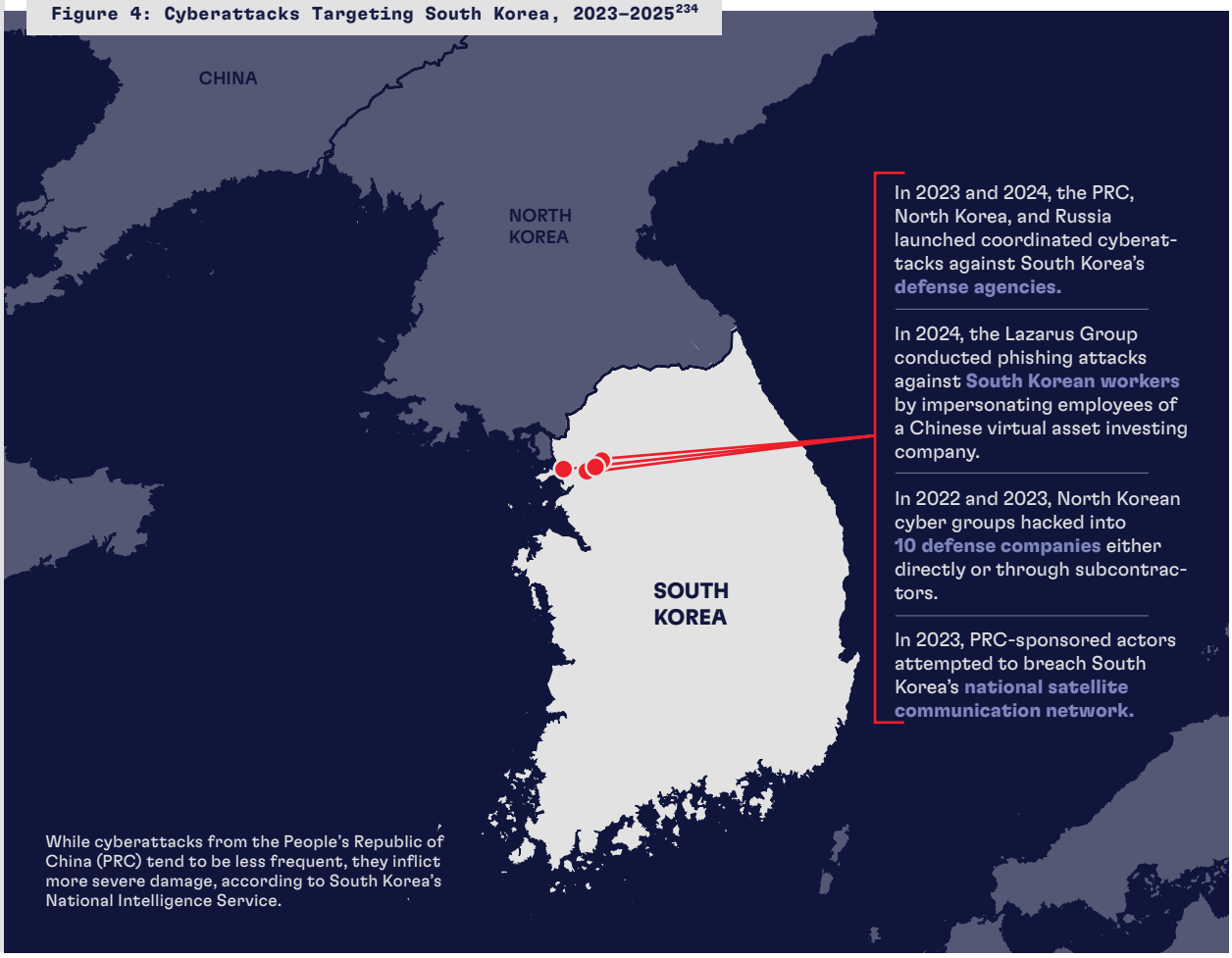
The recent growth of South Korean defense exports has also presented a ripe target. In 2023 and 2024, NIS observed coordinated attacks from the PRC, North Korea, and Russia against South Korea's defense agencies, including the Agency of Defense Development, the Korea Institute for Defense Analysis, and the Defense Counterintelligence Command, indicating a troubling level of malign collaboration to undermine South Korea's defense sector.[232] As South Korea deploys networked weapons systems, such as the KF-21 Boramae fighter, protecting data links and software will be essential to defend against PRC infiltration.[233]

Stakeholders

Although most of South Korea's ministries have cybersecurity roles and responsibilities, key agencies include:

- **The National Security Office (NSO)**: a "control tower" housed within the president's office that coordinates government-wide cyber responses and reviews policy directions.[235]
  - **The Secretary to the President for Cybersecurity at the NSO**: drafts the nation's

Figure 4: Cyberattacks Targeting South Korea, 2023–2025[234]



strategic cybersecurity policies and supervises South Korea's primary cybersecurity agency, the NIS.

  - —**National Intelligence Service (NIS)**: leads South Korea's cyber crisis management efforts, conducts cyber intelligence activities, and responds to domestic cyber incidents.
  - —**National Cybersecurity Center (NCSC)**: supports monitoring, detecting, and responding to domestic cyber threats.[236]

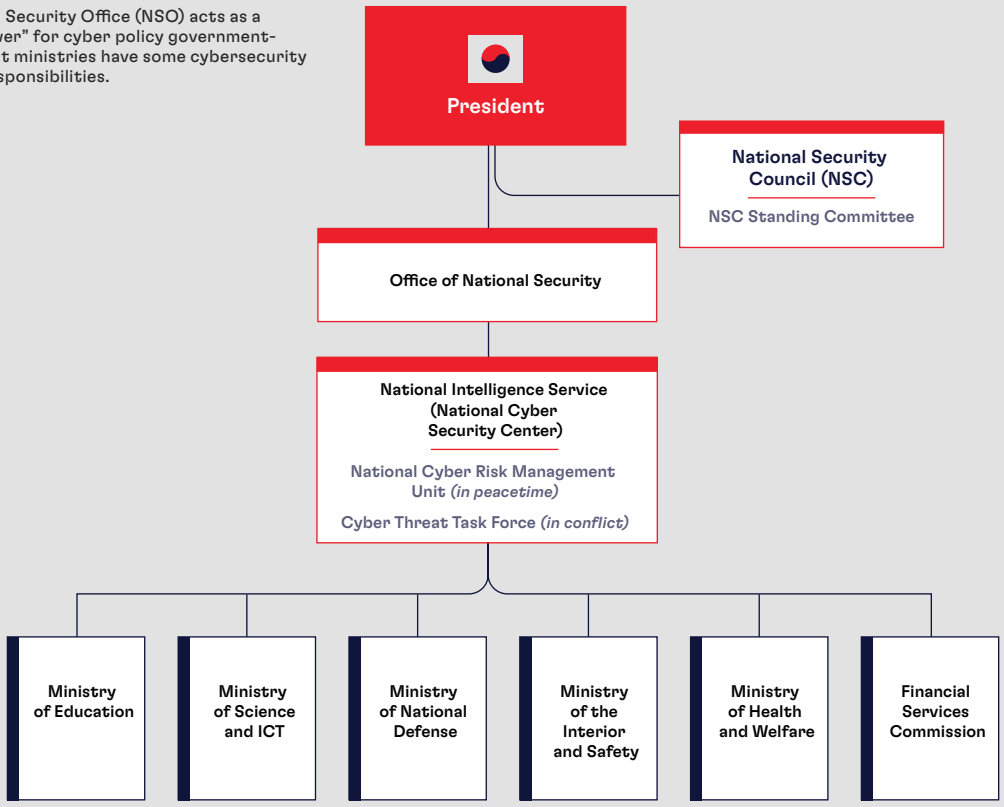
- **The Ministry of Science and Information Communications Technology (MSIT)**: oversees information security policies and frameworks concerning the private sector.
- **Korea Internet and Security Agency (KISA)**: partners with MSIT to prevent and respond to cyberattacks against the private sector and support South Korea's cybersecurity industry. KISA runs private-public partnerships for cybersecurity, including the Cyber Security Big Data Center and the K-Cyber Security Alliance.
- **The Ministry of National Defense**: manages South Korea's military-related security threats and operates the ROK Joint Chiefs of Staff Cyber Operations Command.[237]
- **The Ministry of Foreign Affairs (MoFA)**: leads bilateral and multilateral cyber dialogues.

Policy

Major cyberattacks from North Korea have prompted the South Korean government to reconceptualize cybersecurity as a fundamental component of national

Figure 5: Cybersecurity Roles in the South Korean Government[238]

The National Security Office (NSO) acts as a "control tower" for cyber policy government-wide, as most ministries have some cybersecurity roles and responsibilities.



security.[239] A 2009 North Korean cyberattack that shut down government websites, as well as a 2013 attack on major banks and broadcasting agencies, helped reshape Seoul's view of cybersecurity.[240] In response, the government implemented policies to streamline cyber threat detection and responses, increase public-private partnerships, and bolster offensive cyber capabilities.[241]

- **2024 National Cybersecurity Strategy**: adopts an offensive cybersecurity posture, further aligning with the U.S. Defend Forward approach.[242] The 2024 strategy also enhances the role of South Korea's military and intelligence agencies in preemptive cyber operations, threat detection, and information sharing, while establishing a rapid response system for critical infrastructure.[243] However, the government has not provided unambiguous legal authority for South Korean military and intelligence agencies to conduct these operations.[244]
- **National Intelligence Service Korea Act**: elevates cybersecurity as a core responsibility of the NIS and improves information sharing and coordination across government.[245]
- **Cloud Security Assurance Program (CSAP)**: requires foreign cloud service providers (CSPs) to create a unique, Korea-specific product for government agencies, affiliated public institutions, educational institutions, and public hospitals. KISA oversees the certification process for CSPs, which includes a requirement for localized infrastructure, personnel, and data.[246] While the government amended the program in 2023 to ease certain requirements, in practice, it has impeded adoption of some best-in-class solutions that derive real-time insights from global threat data and AI-enabled capabilities.[247]
- **Information and Communications Network Act (ICNA)**: governs information and communications networks, particularly within the private sector. The law requires companies with more than one million users or 10 billion KRW ($7 million) in profits to implement network separation. The government amended the ICNA in 2024 to mandate incident reporting within 24 hours and authorize fines to spur compliance.[248]
- **Personal Information Protection Act (PIPA)**: defines sensitive personal information, regulates its collection and use, and requires any government agencies or company responsible for controlling or processing personal information to designate a chief privacy officer.[249]

The 2024 National Cybersecurity Strategy was a watershed in South Korea's cybersecurity policy framework, but strategies are not legally binding, and the country still lacks a unified cybersecurity law (no different from the United States).[250] The 2024 strategy made passing a comprehensive "Cybersecurity Act" a strategic objective to "establish a national response system" and unified governance structure for cybersecurity through a better national "control tower."[251] There have been multiple attempts to advance related legislation in the National Assembly, including reforms introduced in June 2020, November 2021, and December 2024.[252] As of April 2025, none have passed. [253] The political crisis in Seoul following former President Yoon's declaration of martial law in December 2024 will likely further delay consideration of cybersecurity legislation.[254]

People

South Korea's cyber workforce shortage is more manageable than other countries examined in this report. A KISA survey of the country's cybersecurity industry found the number of cybersecurity professionals is keeping pace with the growth of the country's cybersecurity industry, growing by almost 30 percent between 2021 and 2022. However, most companies surveyed still identified hiring and retaining qualified personnel as the most significant barrier to technology development.[255]

The gap is more dire in government. To close it, MSIT set a goal to train 100,000 cybersecurity professionals through public-private-military cooperation as part of its 2022 Republic of Korea Digital Strategy.[256] Seoul has especially struggled to keep the Cyber Operations Command (COC) properly staffed, as graduates from the Ministry of National Defense Cyber Specialist Officer System program increasingly leave the military for the private sector.[257] The program provides select students with full scholarships for four years, after which they are commissioned as

cyber operations officers in the military for a mandatory seven years.[258] In 2016, 96 percent of program graduates were commissioned as cyber operations officers, while in 2023, the number collapsed to just 17 percent.[259] The drop came from the vast majority of graduates choosing to repay the four-year government scholarship and avoid mandatory service in favor of higher paying jobs in the private sector.[260] In addition, most graduates who complete their full mandatory service chose to leave the military for the private sector instead of applying for long-term service.[261]

Partnerships

South Korea proactively embraces alliances and partnerships to enhance its cyber resiliency and promote democratic principles in cyberspace. The country places particular importance on partnership with the United States. As with Japan and the Philippines, the mutual defense treaty with the United States provides some legal basis for the presence of U.S. cyber personnel, and both countries have increasingly emphasized cyber cooperation to address rising state-sponsored threats.

In 2023, Seoul and Washington jointly announced the Strategic Cybersecurity Cooperation Framework, which emphasized active cooperation between the U.S. Cybersecurity and Infrastructure Security Agency (CISA) and KISA, as well as integration of the cyber domains in the 1953 Mutual Defense Treaty.[262] The framework reaffirms bilateral cooperation in cyberspace, including deterring malicious actors, information sharing, collaboration in international forums, and active participation in cyber military exercises.[263]

These cyber military exercises are jointly led by U.S. Cyber Command and South Korea's Ministry of National Defense's Cyber Operational Command and include the annual Ulchi Freedom Shield exercise and the Freedom Shield exercise.[264] In 2022, South Korea also joined the U.S.-led multinational exercise Cyber Flag for the first time.[265] The 2024 exercise, held in Virginia, involved 18 nations and incorporated offensive cyber operations, marking a strategic shift in the exercise's scope that previously only focused on defensive cyber operations.[266]

South Korea has also worked to operationalize the nascent U.S.-Japan-South Korea trilateral relationship through participation in the inaugural June 2024 Freedom Edge exercise, which combined the U.S.–South Korea Freedom Shield and U.S.-Japan Keen Edge to strengthen defensive cyber capabilities.[267] The second iteration was held in November 2024.[268] South Korea has also formalized a strategic cyber partnership with the United Kingdom.[269]

South Korea is expanding cybersecurity engagement through multilateral organizations. In 2022, South Korea became a member of the International Counter Ransomware Initiative. In May 2024, the ROK MoFA sought to use its month-long chairmanship of the United Nations Security Council to elevate illegal cyberattacks as a global priority. [270] South Korea is also an active participant in the United Nations' Open-Ended Working Group on Information and Communications Technologies.[271]

Domestically, South Korea has prioritized partnership with industry. MSIT, the agency overseeing cyber incident reporting, can stand up public-private joint investigation groups to analyze major security breaches in ICT networks.[272] KISA focuses on fostering cybersecurity partnerships with industry and provides them with cybersecurity tools to combat attacks, including antivirus and web vulnerability identification programs.[273] KISA also runs 10 Regional Information Security Support Centers nationwide to provide SMEs with tailored cybersecurity services.[274]

U.S. cybersecurity companies are active in South Korea. In 2016, U.S. cyber intelligence company Fortinet part`nered with KISA to improve incident analysis and identification of threats, such as botnets, malicious domains and URLs, malware samples, and zero-day vulnerabilities.[275] In 2024, the cybersecurity company Palo Alto Networks launched a cloud-based tool for analyzing cyber threats.[276] In a major breakthrough for the ability of U.S. companies to partner with the Korean government, Microsoft announced in December 2024 that it had become the first hyperscaler to achieve certification under CSAP, allowing government agencies to use Azure cloud services.[277] Google Cloud announced its certification two months later.[278]

Progress and Recommendations

South Korea has made considerable progress in strengthening its cybersecurity posture, underscored by the 2024 National Cybersecurity Strategy. Remaining challenges include a cyber workforce shortage, interagency coordination, limited adoption of cybersecurity best practices across government and industry, and regulations that inhibit partnerships with foreign companies to adopt cutting-edge cybersecurity technologies. While the CSAP certification for Microsoft and Google is a welcome step to improve Seoul's access to world-leading cloud and AI-enabled defenses, Seoul should pursue additional reforms to encourage diverse industry partnerships across the cybersecurity ecosystem. As cyber threats targeting South Korea grow more sophisticated, addressing these vulnerabilities must be a top priority for the Lee administration.

To address these issues, the report offers the following recommendations to leaders in the South Korean government:

Designate a top cyber official in the president's office to lead coordination across government. Responsibility for cyber policy development, incident detection, and response falls across several agencies, including the COC, MSIT, NIS, and KISA. The government should designate a Blue House official responsible for coordinating policy and improving information sharing across these bodies to limit gaps. This should complement legislation to establish a unified, national "control tower" for cybersecurity incident detection and response, consistent with the 2024 National Cybersecurity Strategy.

Enact clear legal authorities for active cyber defense. Although the 2024 National Cybersecurity Strategy emphasizes a more offensive posture in cyber space, the government did not complement it with clear legal authorities to enable the COC and others to develop and deploy offensive cyber capabilities.

Mature offensive cyber capabilities through public investment and partnership with the United States. Seoul should ensure the COC has sufficient resources and personnel to develop its offensive cyber capabilities to strengthen deterrence and Defend Forward Operations (DFOs). It should expand joint exercises with U.S. Cyber Command to hone offensive capabilities and doctrine.

Integrate cybersecurity training for mandatory military service. South Korea's Military Service Act requires mandatory military service for able-bodied men aged 18 to 28. Mandating cybersecurity training would boost the country's long-term cyber resilience and workforce, including for the COC. For implementation, the government should consider partnering with Israel to learn from its example of integrating cybersecurity into its mandatory military service, which has significantly boosted the pipeline of cyber talent for government and industry.

Increase salaries for commissioned cyber officers to reduce incentives to seek private sector jobs after the four-year scholarship from the Ministry of National Defense Cyber Specialist Officer System.

Reform regulations that privilege domestic technology vendors, such as CSAP, to facilitate access to best-in-class modern cybersecurity solutions for the public sector. CSAP's three-tier system reflects an outdated understanding of cybersecurity best practices that fails to appreciate the growing potential of AI-enabled cyber defenses with access to international data on threat actor tactics, techniques, and procedures (TTPs). CSAP's broad requirement for data localization epitomizes this view. The law's requirement to use domestic encryption algorithms may boost domestic cyber firms but needlessly deprives the country of superior options. The medium- and high-level certifications are also over-inclusive; Seoul should only require data localization and physical separation for the most national security–sensitive data. It should drop these requirements for most other contexts.

***

TAIWAN

Unlike Japan, South Korea, and the Philippines, Taiwan is not a formal ally of the United States. The two countries do not have a mutual defense treaty, and the United States does not maintain official diplomatic relations—even if it maintains a robust diplomatic presence in Taipei and encourages strong commercial, technology, and people-to-people ties. The United States has long maintained a "one China policy" that opposes "unilateral changes to the status quo" from either Taiwan or the PRC.[279] The 1979 Taiwan Relations Act informs the U.S. position of "strategic ambiguity," committing Washington to both treat any non-peaceful attempts at unification as a security threat and to supply defensive arms to Taiwan.[280]

Despite this ambiguity, Washington has a vital interest in ensuring Taiwan's security as it faces escalating aggression from the PRC in air, sea, and cyberspace. Washington's willingness to defend Taiwan has become a proxy for its willingness to check the PRC's aggression and defend democracy. More concretely, Taiwan fabricates 90 percent of the world's advanced chips, which are indispensable to the U.S. military and economy. The loss of access to these chips, whether from physical or cyberattacks, would inflict profound harm on the U.S. economy and national security.

For these reasons, Washington should pay close attention to rising cyberattacks against Taiwan. Indeed, the democratic island arguably faces the most intense cyber aggression of any nation in the Indo-Pacific, owing to rising tensions with Beijing following the 2024 election of the Democratic Progressive Party's (DPP) President Lai Ching-te, who the PRC perceives as pro-independence. While Taiwan's longtime technology leadership makes it well poised to adapt to Beijing's growing cyber aggression, the island will remain outmatched without close partnership from the United States, other allies and partners, and foreign technology firms.

Geopolitics have complicated Taiwan's efforts to forge international cyber partnerships. Many foreign governments and firms remain wary of angering a far wealthier and more powerful China by openly supporting the democratic island's cyber defenses. For this reason, even as Taipei has moved to expand its cyber engagement abroad, it has also worked to modernize its cybersecurity bureaucracy, policy, workforce, and technology through partnerships with foreign firms.

Threats

Recent years have seen a surge in cyberattacks against Taiwan.[281] In 2024, Taiwan's government websites and platforms experienced an average of 2.4 million attempted intrusions per day, more than double the previous year.[282] According to industry reports, cyberattacks increased nearly 850 percent ahead of Taiwan's January 2024 presidential election, compared to the same period the prior year.[283] The cybersecurity firm Trellix has identified increasingly sophisticated attack methods focused principally on "defense evasion, discovery, and command control." Phishing, malware, website defacement, and DDoS attacks were also common.

STATE-SPONSORED ACTORS

Rising cyberattacks mirror rising tensions with Beijing, which in recent years has escalated its cyber aggression alongside military, economic, and diplomatic pressure. More than other domains, the

abstract nature of cyberthreats to the broader public, combined with technical challenges of timely attribution, makes the cyber domain well-suited for Beijing's campaign to maximize gray zone pressure against the democratic island. The PRC has similarly exploited the inherent ambiguity of both the cyber domain and Taiwan's status to push the envelope and effectively use the democratic island as its testbed for cyberattacks. This allows Beijing to hone its TTPs, and escalate nontraditional aggression against Taiwan.[284]

To that end, the PRC has combined espionage and infiltration techniques with newly brazen disinformation and influence campaigns as part of a broader effort to coerce, intimidate, divide, and demoralize Taiwan and its democratic institutions. According to a cybersecurity expert at Google, there are over 100 hacking groups in China alone that have gone "after everything" from Taiwan's defense to commercial sectors.[285]

In 2024, Taiwan's government websites and platforms experienced an average of 2.4 million attempted intrusions per day, more than double the previous year.

According to a report from Recorded Future, a cyber threat intelligence firm, the likely PRC-linked hacking group known as RedJuliett targeted "government, education, technology, and diplomatic organizations" in Taiwan for six months between 2023 and 2024 as part of a state-backed cyber espionage campaign by exploiting vulnerabilities in public-facing devices and applications.[286] These ongoing state-backed campaigns aim to monitor and exfiltrate sensitive information to inform Beijing's cross-Strait policy.[287] In March 2024, the Taiwanese Ministry of National Defense (MND) confirmed a successful hack of Chunghwa Telecom that exfiltrated sensitive data, including documents from the Taiwanese armed forces, coast guard, and MoFA, which were later sold on the dark web. Taiwan's MND has not formally attributed the attack.[288]

Taiwan also faces significant APT attacks.[289] In August 2023, Microsoft reported that Flax Typhoon, a PRC-backed group active since mid-2021, was targeting "dozens" of organizations in Taiwan for espionage.[290] According to Microsoft, Flax Typhoon used LoTL techniques to target "government agencies and education, critical manufacturing, and information technology organizations" across the country. Flax Typhoon has also reportedly conducted APT attacks against the Taiwanese government, education, and critical manufacturing organizations as part of a broader espionage campaign. Volt Typhoon, another prominent cyber group linked to the Chinese government, has also used APT attacks and LoTL tactics to target critical infrastructure.[291]

Taiwan's semiconductor industry is especially vulnerable. Most of these chips come from a single company, the Taiwan Semiconductor Manufacturing Corporation (TSMC), raising the danger that a single successful cyberattack could upend the global chip supply chain.[292] There is precedent for concern. In January 2024, one of Taiwan's biggest semiconductor manufacturers, Foxsemicon Integrated, fell victim to a ransomware attack in which hackers claimed to have obtained personnel data belonging to employees and customers and demanded a $1 million ransom.[293]

Although the PRC is the principal source of cyberattacks against Taiwan, the island also faces state-backed actors linked to North Korea that target its financial institutions for revenue. In 2017, a North Korean hacking unit allegedly stole $60 million from a Taiwanese bank.[294] A federal grand jury in the United States indicted a North Korean man in 2024 for infiltrating the computer systems of a Taiwanese defense companies, among other victims, to steal "technical and design information about military weapons and vehicles, such as tanks, fighter jets, rockets, and torpedoes."[295]

HACKTIVISTS

Taiwan also faces attacks from Chinese hacktivists, who conduct less sophisticated DDoS attacks—typically coinciding with cross-Strait tensions—to signal displeasure with Taiwanese or U.S.-Taiwan policy.[296] For example, hacktivists forced several Taiwanese government websites offline following U.S. Speaker of the House Nancy Pelosi's visit to Taiwan in August 2022. Chinese hacktivists also had control of electronic billboards and displays across Taiwan, including in local 7-Eleven stores, to broadcast brazenly critical messages of the Speaker and her visit.[297] These messages read, "Nancy Pelosi, you

warmonger, get out of Taiwan!" and "The old witch's ill-intended visit to Taiwan is a serious provocation to the sovereignty of the Motherland … Greater China will ultimately be unified!"[298] APT27_Attack, a Chinese hacktivist group, claimed responsibility.[299]

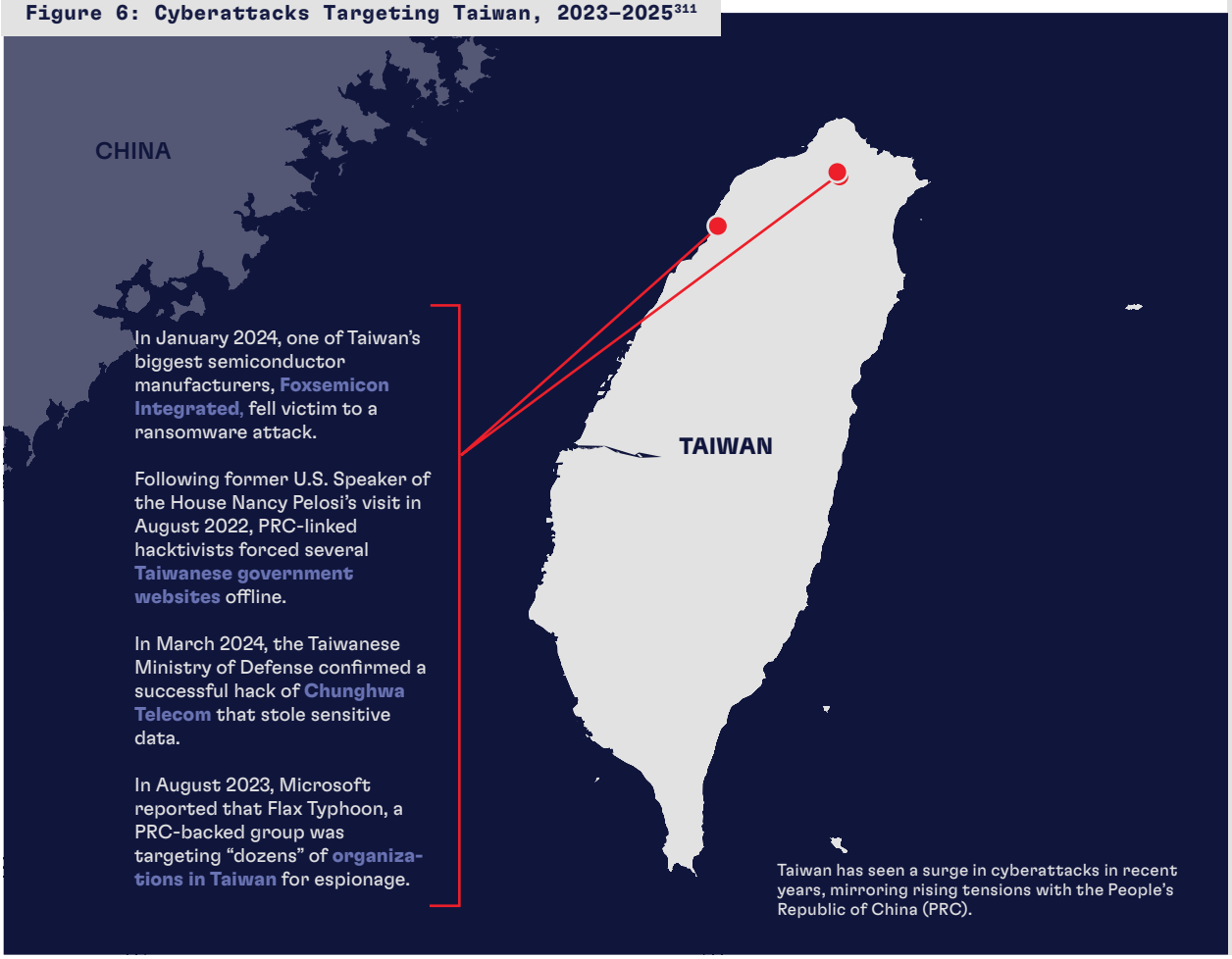
DISINFORMATION

The unusual geopolitical stakes of Taiwan's domestic politics attract significant disinformation campaigns. These mostly come from the PRC, which seeks to bend Taipei to its will in its campaign for reunification.

According to a 2022 Digital Society Project report, Taiwan was the world's most common target of foreign disinformation for nearly the last decade.[300] These disinformation threats were especially acute ahead of Taiwan's 2024 presidential election.[301] Chinese state-linked cyber actors executed sophisticated social media campaigns to undermine DPP candidates, amplify false narratives, and exacerbate political divisions.[302]

The most infamous case was the production and dissemination of a 300-page ebook, "The Secret History of Tsai Ing-wen," which reinforced false narratives about the former president as corrupt and promiscuous to erode trust in her and the DPP ahead of the election.[303] The effort was likely linked to Spamouflage, a Beijing-backed digital propaganda group (also known as Dragonbridge and Storm-1376).[304] Spamouflage allegedly used AI to generate fake accounts, audio clips, and even "news anchors" to amplify the ebook and its false messages on social media platforms and Taiwanese blogs. According to Microsoft, this was the first instance of a nation-state using AI-generated material to influence a foreign election.[305] On election day, an audio clip also went viral, falsely showing Terry Gou, a former presidential

Figure 6: Cyberattacks Targeting Taiwan, 2023–2025[311]



candidate, endorsing the more pro-PRC Kuomintang candidate.[306]

During this period, TikTok emerged as a font of disinformation.[307] As of May 2024, a quarter of Taiwan's 23 million residents used TikTok. In the 2024 presidential election, TikTok videos questioning the election's legitimacy spread quickly, overwhelming Taiwan's FactCheck Center.[308] Although Taipei issued an executive order banning the app on government devices, it remains legal on private devices.[309]

Despite a deluge of disinformation, the Taiwanese government and civil society have helped to minimize its impact by working proactively to build public awareness and preview, identify, debunk, and discredit the PRC's foreign influence operations.[310]

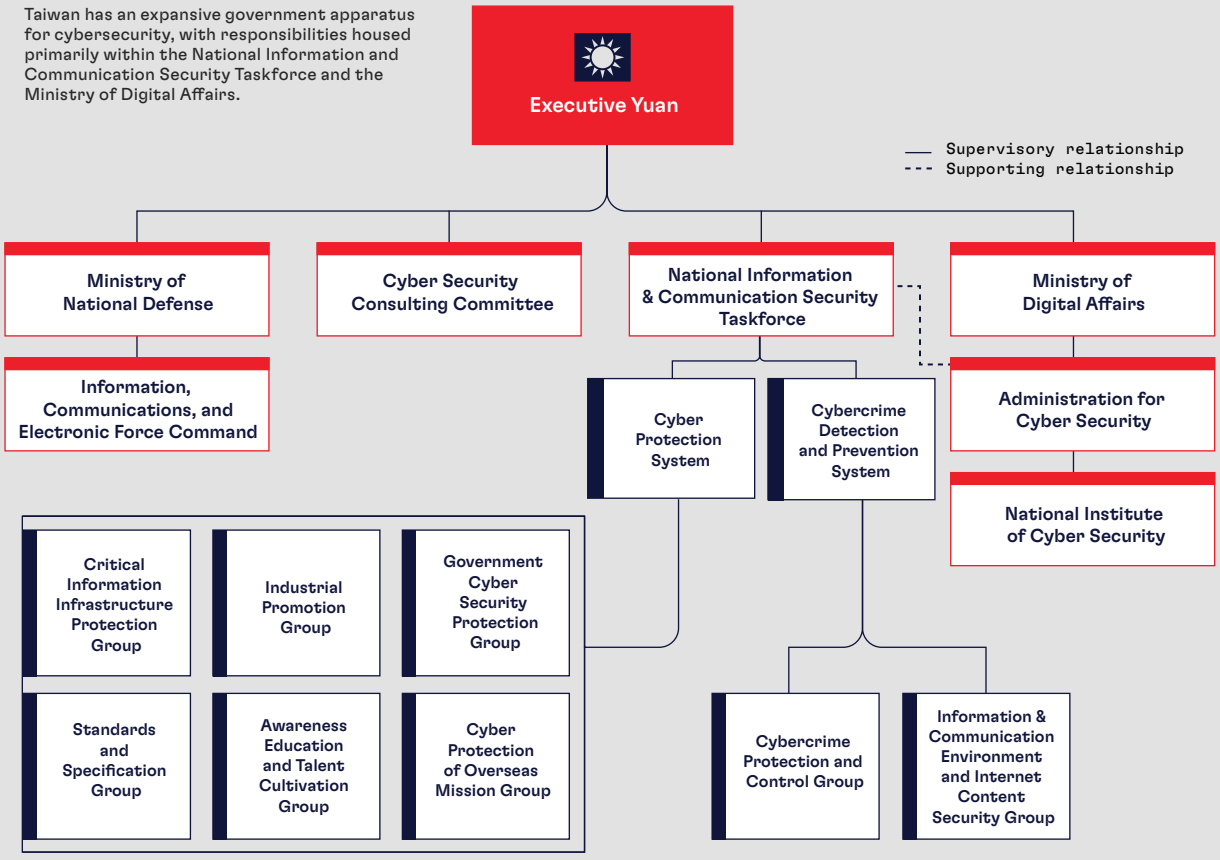
Stakeholders

In recent years, Taiwan has recognized its cyber vulnerability and empowered government agencies to combat cyber threats.

- **Ministry of Digital Affairs (MoDA)**: established in January 2022, leads the management of policy and regulation of the nation's digital infrastructure, with specific mandates to boost digital connectivity. MoDA also deepens digital applications to improve government efficiency, leads Taiwan's international engagement on digital policy, and boosts cybersecurity.[312]
- **Administration of Cyber Security (ACS)**: plans and implements Taiwan's national cybersecurity policies and regulations. These include implementing incident detection mechanisms and

Figure 7: Taiwan's Cybersecurity Agencies[318]

Taiwan has an expansive government apparatus for cybersecurity, with responsibilities housed primarily within the National Information and Communication Security Taskforce and the Ministry of Digital Affairs.



defense mechanisms for critical infrastructure, auditing cybersecurity efforts at government agencies and public entities, coordinating government cybersecurity efforts, and promoting international cooperation on cybersecurity.[313]

- **National Institute of Cyber Security (NICS)**: established in February 2023, advances Taiwan's cybersecurity through research and development and implementation of ACS plans. The NICS differs from the other bodies through its emphasis on cybersecurity research and technical assistance.[314] The NICS's Talent Empowerment Center focuses on recruiting and training cyber personnel.[315]
- **National Information and Communication Security Taskforce (NICST)**: advances national cybersecurity policies by advising on national cybersecurity policy and plans and coordinating interministry cybersecurity affairs.[316]
- **The Taiwan Academic Cybersecurity Center (TACC)**: established in April 2024, conducts forward-looking cybersecurity research including AI in cybersecurity, postquantum cryptography, zero trust architecture, secure satellite communications and 5G. It is a National Science and Technology Council flagship project.
- **Information, Communication and Electronic Force Command (ICEF)**: created in 2017 as a fourth service branch under the Ministry of National Defense to unify communications, cyber, and electronic warfare capabilities.[317]

Taiwan is home to a robust ecosystem of civil society organizations (CSOs), which play a vital role in combating misinformation in Taiwan. Prominent entities include Doublethink Lab, an organization that investigates PRC disinformation campaigns, and Cofacts, an open source, citizen-driven collaborative fact-checking platform.[319]

The private sector also plays a significant role in safeguarding Taiwan's digital infrastructure. Although most cybersecurity firms operating in Taiwan have headquarters abroad, CHT Security, a subsidiary of Chunghwa Telecom, is a leading domestic player. Trend Micro, a Japanese company founded by Taiwanese entrepreneurs in the United States, also hosts an office in Taipei. Cisco has operated in Taiwan for nearly three decades, and in June 2024, it announced its intention to establish a cybersecurity center in Taiwan to boost threat intelligence and cybersecurity training in partnership with local tech associations.[320] AWS has also announced a new "Infrastructure Region" in Taiwan by early 2025 to meet the growing demand for cloud services across the Indo-Pacific.[321] TSMC has also contributed to cybersecurity by helping develop some of the first standards for semiconductor equipment.[322]

Policy

Taiwan has answered an increasingly dangerous cyber landscape with several new policies and initiatives. In December 2020, the Executive Yuan designated cybersecurity as one of "Six Core Strategic Industries" signaling to both domestic and foreign firms the nation's prioritization of the sector as an engine of economic growth.[323] The creation of MoDA in 2022, and NICS the following year, added greater institutional muscle to Taiwan's cyber policies and implementation. The Executive Yuan's NICST has launched four-year plans for cybersecurity since 2011, with the most recent 2021–2024 plan focusing on building Taiwan's active defense capabilities in cyberspace.[324] In addition, with the creation of the ICEF in 2017, Taiwan honed its offensive cyber capabilities to counter the PRC's gray zone cyber campaigns and to enhance early warning of PLA activities.[325]

- **Personal Data Protection Act**: passed in 2010, regulates the collection and use of personal data. Among other requirements, the law stipulates that custodians of personal data must take preventive measures to safeguard it from theft, disclosure, alteration, and destruction.[326] The law does not mandate certain security practices, leaving these decisions to private entities.[327] Although the law outlines a fiduciary duty for a company to protect data in its custody, it does not strictly hold those companies liable for breaches.[328]

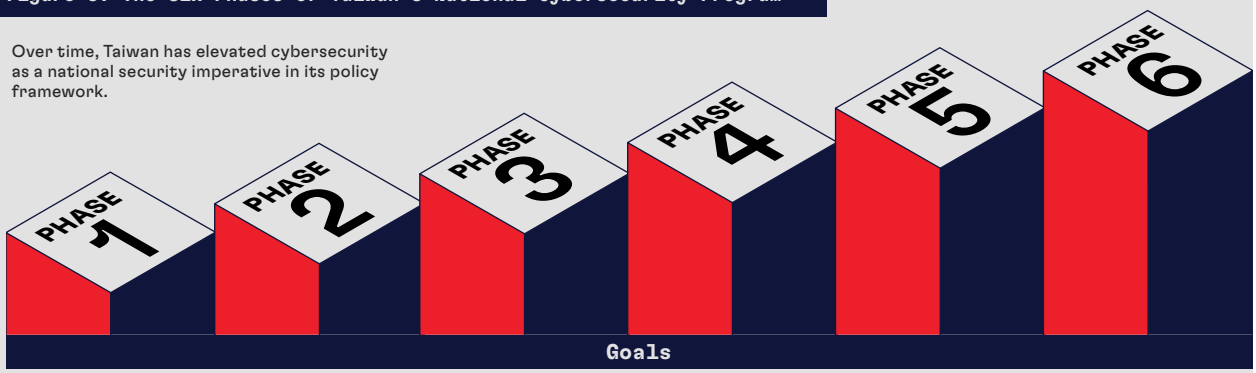
- **Cybersecurity Management Act (CMA)**: enacted in 2018, serves as Taiwan's foundational cybersecurity law covering government agencies, state-owned enterprises, state-sponsored foundations, and some nongovernment entities, such as critical infrastructure operators.[329] Under the law, these covered entities must develop and follow cybersecurity plans, along with incident reporting and response mechanisms.[330] The law requires cyber incident responses within an hour, with mitigation efforts required between 36 and 72 hours, depending on the seriousness of the attack.[331]
- **National Cyber Security Strategy Phase Six Development Program (2021–2024)**: aims to build an active defense network, promote private-public cooperation, cultivate autonomous development capabilities, and recruit top global talent.[332]

Despite progress, key gaps remain in Taiwan's cybersecurity policies. CMA's jurisdiction does not include most private entities, which leaves significant cyber vulnerabilities and fails to reflect the interconnected threat landscape. Taiwanese law also does not mandate that private companies designate a chief information security officer (CISO), except for certain critical industries like finance. With that said, Taiwan's lead agency for regulating the financial sector does require any company listed on the country's major stock exchanges to designate a CISO.[333]

Initial phases focused on establishing NICST and core cyber bureaucracy, infrastructure, and policy across government, developing technical standards,

Figure 8: The Six Phases of Taiwan's National Cybersecurity Program[334]

Over time, Taiwan has elevated cybersecurity as a national security imperative in its policy framework.



2001–2004	2005–2008	2009–2012	2013–2016	2017–2020	2021–2024
Build Taiwan's cybersecurity defense foundation.	**Extend defenses and create 24/7 monitoring.**	**Improve incident responses and reporting mechanisms.**	**Strengthen cybersecurity governance and intelligence-sharing.**	**Elevate cybersecurity to the level of national security.**	**Establish an active defense posture in cyberspace.**
Key Actions					
Establish the National Information and Communication Security Taskforce and the National Center for Cyber Security Technology.	Create the National Security Operation Center to provide 24-hour cyber monitoring and defense.	Build full-cycle incident response mechanisms.	Establish the National Center for Cyber Security Technology to advance development and adoption of cybersecurity technology.	Create a national cybersecurity joint defense system.	Integrate capabilities to eliminate cyber threats at their source.
Develop information security management systems for critical infrastructure.	Appoint chief information security officers in ministries.	Promote international cybersecurity standard certifications (ISO 27001) among Taiwan's government agencies.	Establish the Institute of Watch Internet Network (iWIN) to enhance internet content security.	Cultivate high quality cybersecurity talent.	Increase cyber defense capacity through public-private cooperation.

introducing CISOs in key government agencies, improving incident response, boosting private sector collaboration and information sharing, and supporting public and private cybersecurity research, and talent cultivation. In the fifth phase, NICST explicitly elevated cybersecurity as a national security imperative and aimed for a "national cybersecurity joint defense system." The most recent program also proposed a National Cyber Security Program of Taiwan (2021–2024) that envisions a "resilient, secure, smart country" with a focus on attracting top foreign talent, building an active cyber defense base, securing critical infrastructure, and expanding cybersecurity awareness.[335]

People

Despite growing threats, Taiwan continues to struggle with a shortage of cyber personnel. This shortage is downstream of Taiwan's broader deficit of high-skilled workers, which is projected to hit 120,000 by 2028, according to comments by a government minister in an interview with the *Taipei Times*. Taiwan's low birth rate and aging population further constrict the talent pipeline. The cybersecurity industry must also compete with Taiwan's world-renowned chip industry, which also faces a growing deficit of trained engineers.

Taiwan has struggled to cultivate cyber talent. A broad lack of awareness across government, industry, and society has generated confusion about necessary competencies for cybersecurity professionals, discouraging new entrants and needlessly shrinking the talent pipeline. Mirroring this ambiguity, the CMA fails to define criteria for CISOs. which complicates hiring them because agencies and firms worry about whether their selections are compliant. Participants in the Taipei workshop organized by CNAS researchers also noted a relative lack of interest in cybersecurity careers among students and younger workers, compared to more exciting fields like AI and semiconductors.[336] Competition over a shrinking youth labor pool, especially in the private sector, compounds the challenge.

The cybersecurity workforce gap is especially acute in government. According to the National Audit Office's 2020 Central Government Final Account Review Report, 35 percent of "level A" to "level C" government agencies lacked information security personnel. In Taiwan, government agencies are categorized into levels A through E based on their cybersecurity responsibilities.[337] According to Claire Wang, a Taiwanese legislator, the requirement for 2,300 government agencies and many private firms to appoint a CISO has contributed to the workforce shortage, leaving a demand for nearly 10,000 trained cyber personnel. The Executive Yuan's goal of training 350 cybersecurity experts by 2024 will still leave a significant shortage.[338]

Government and industry have taken steps to address the workforce gap, although it will require more ambitious efforts. The government has proposed to make the country a regional "cybersecurity research and training hub" to expand the domestic talent pipeline and attract top cyber talent from around the world. MoDA also launched a Cybersecurity Center of Excellence with a Cybersecurity Talent Training Division.[339] The effort focuses on practical skills through exercise-based training.[340] The Ministry of Education's Information Security Incubation Program also trains high school, college, and graduate students to "meet the manpower needs of information security" and build a talent pipeline for industry.[341] Google has launched an effort to train up to 2,000 workers by 2025 in partnership with MoDA and the National Taipei University of Technology through free online certification courses.[342] Cisco's new cybersecurity center in Taiwan will also prioritize workforce development and training.[343]

The cybersecurity industry must also compete with Taiwan's world-renowned chip industry, which also faces a growing deficit of trained engineers.

A bright spot for Taiwan is its relative success in promoting cyber awareness through active public campaigns. Taiwan's Ministry of Education, for instance, established a website for cybersecurity education.[344] Taiwan offers an instructive model to the world for taking a proactive approach to countering disinformation and building resilience by drawing on credible voices in government, civil society, and even

private citizens. Ahead of the January 2024 election, Taiwanese senior government officials and CSOs actively prepared the public for disinformation, and groups like the Taiwan FactCheck Center debunked false claims as they arose.[345]

Partnerships

Taiwan is actively encouraging cybersecurity partnerships in the private sector through leveraging hyperscale cloud services, such as Microsoft, Google, and Amazon, to increase redundancy and strengthen national digital resilience. Experts anticipate that Taiwan's cyberspace will be heavily contested and potentially denied during a conflict with the PRC, impacting the situational awareness and ability to exercise command and control of Taiwan's armed forces.[346] Learning from Ukraine's experience following Russia's invasion, Taiwan began a four-year, $40 million initiative to migrate key government services to the cloud. As Taiwan migrates these government services to the cloud, it is balancing risks to data sovereignty through offshore encrypted backups, local control over encryption keys, and compliance with Taiwan's data privacy rules.[347] Taiwan is also actively encouraging cloud providers to partner locally with satellite providers to develop systems capable of switching to satellite communications in emergency situations.[348] To address its cyber workforce gap, Taipei has also actively courted international firms, and Cisco, Google, and Microsoft have all announced plans to expand opportunities for cybersecurity training and internships.[349]

Beyond encouraging partnerships with the private sector, Taipei recognizes the urgency of partnering with cyber-leading nations to mitigate the dangerous asymmetry it faces against a sophisticated threat actor like the PRC. President Lai himself called for international collaboration to "combat disinformation [and] strengthen democratic resilience" in his May 2024 inaugural address.[350] Taipei has long sought bilateral and multilateral cyber partnerships, although its contested status has complicated this effort by limiting participation in many international forums.

The effort has yielded some success. Several countries have prioritized cybersecurity cooperation with the island given its critical role in the global chips supply chain.[351] Taiwan and the United States created the Global Cooperation and Training Framework (GCTF) in 2015 to boost the participation of Taiwanese officials, businesses, and civil society leaders in multilateral exchanges and trainings. Australia, Japan, and Canada later joined the effort. Several of the GCTF's recent convenings have focused on cybersecurity, including a December 2023 workshop in Delhi with participants from Taiwan, India, and the United States.[352] Taiwan also has representatives on the Asia Pacific CERT.[353]

The United States remains Taiwan's most important cyber partner. As awareness of Beijing's cyber threat has grown in both capitals, so has the U.S.-Taiwan cyber partnership. Taiwan-U.S. defense cooperation has focused on hardening Taiwan military networks against PRC intrusion and disruption. As the Taiwanese armed forces introduce advanced platforms that rely on networked software systems, such as the F-16V fighter jets, ensuring data links and mission computers are secure from jamming or intrusion will be critical.[354] To this end, the United States approved a $75 million sale in 2024 for an "advanced tactical data link system" to "secure the flow of tactical information" and enhance "communications and networks security."[355]

Taipei recognizes the urgency of partnering with cyber-leading nations to mitigate the dangerous asymmetry it faces against a sophisticated threat actor like the PRC.

In addition, the United States and Taiwan have held joint cyber exercises since 2019 to strengthen interoperability and assess cyber readiness by simulating real-world cyberattacks.[356] That same year, the United States and Taiwan established the Talent Circulation Alliance (TCA), a public-private partnership to promote talent cultivation and exchange between the two countries and other like-minded nations.[357] In December 2021, the two governments created the U.S.-Taiwan Technology Trade and Investment Collaboration (TTIC) framework to support the joint development of commercial programs and to bolster critical technology supply chains, including for cybersecurity.

Experts speak about Taiwan's cybersecurity landscape at the CNAS-Prospect Foundation workshop in Taipei, hosted by the CNAS Technology and National Security Program and Indo-Pacific Security Program. (Michael Depp/CNAS)

In September 2023, the Director of the U.S. National Institute of Standards and Technology led a delegation of 13 U.S. cybersecurity firms to Taiwan to promote two-way trade and investment between the United States and Taiwan.[358] As part of the visit, the United States and Taiwan agreed to increase cyber collaboration by building a joint cybersecurity supply chain under the TTIC.[359]

The U.S. Congress also took a major step to boost U.S. support for Taiwan's cybersecurity. The FY 2024 National Defense Authorization Act (NDAA), for instance, included a provision authorizing the DoD to cooperate on:

> *defensive military cybersecurity activities with the military forces of Taiwan ... to (1) defend military networks, infrastructure, and systems; (2) counter malicious cyber activity that has compromised such military networks, infrastructure, and systems; (3) leverage United States commercial and military cybersecurity technology and services to harden and defend such military networks, infrastructure, and systems; and (4) conduct combined cybersecurity training activities and exercises.*[360]

The provision seems to authorize HFOs by U.S. Cyber Command. Taiwanese law neither explicitly authorizes nor prohibits HFOs or the use of Taiwanese networks for U.S. DFOs, but Taipei has quietly welcomed U.S. cyber cooperation even if both parties keep such assistance discrete, given political sensitivities. In the FY 2025 NDAA, Congress authorized the DoD to provide up to $300 million in material and other assistance to Taiwan, including "defensive cyber capabilities or support," through a new Taiwan Security Cooperation Initiative.[361]

Progress and Recommendations

The flood of cyberattacks and disinformation ahead of the January 2024 elections brought global attention to the cyber threats Taiwan faces, highlighting Beijing's growing fusion of traditional cyberattacks with influence operations, as well as Taiwan's democratic resilience.

Taiwan's relationship with the United States is shifting as the Trump administration looks for Taipei to invest more in self-defense and address trade imbalances. These new realities give Taiwan the opportunity to demonstrate to the United States its strategic importance in the cyber domain as the front line against PRC cyber aggression, a test bed for the PRC's TTPs, and a model of whole-of-society resilience to disinformation.

To address these issues, the report offers the following recommendations to leaders in the Taiwanese government:

Prioritize cybersecurity investments as Taipei seeks to raise defense spending to at least 3 percent of its GDP.[362] Taiwan should not only spend more on its defense; it should spend strategically in areas beyond traditional platforms like fighter jets and missile systems. Specifically, it should invest in secure communications infrastructure, cloud and AI-enabled cyber defenses, and robust command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) networks.[363] Investments in data integration and interoperable digital systems are also essential for networking Taiwan's defense assets and boosting resilience, as well as boosting interoperability with the United States and other allies.

Pursue "digital embassies" abroad to house sensitive government data for resilience in the case of a cross-Strait crisis. Inspired by Estonia's early work and Ukraine's actions to offshore critical data following the Russian invasion, Taiwan could partner with the United States and other governments to house sensitive data abroad to boost resilience. Audrey Tang, Taiwan's first minister of digital affairs, proposed this idea in 2023.[364]

Expand and further leverage the GCTF. Since Taiwan and the United States launched the framework in 2015, Japan, Australia, and Canada have joined as official partners. Taipei should work with GCTF nations to secure formal partnership from other key Indo-Pacific nations, such as India, South Korea, and New Zealand. It should also increase the pace of workshops and other engagement around disinformation and democratic resilience to share Taiwan's experience.

Create a cyber visa for high-skilled foreign workers to address workforce shortage. Taiwan has an aging population with a falling number of STEM students. There is also fierce competition for domestic talent from the country's fast-growing semiconductor sector, which will only grow with surging AI demand. Existing government efforts to expand the domestic talent pipeline will prove insufficient given these structural realities. To close the cyber workforce gap, Taipei should consider a special visa for top cyber talent. This will not be easy given backlash against the government's efforts to introduce 100,000 Indian migrant workers in 2023, but demographic realities leave few compelling options.[365]

Partner with international low Earth orbit (LEO) space companies to develop resilient telecommunications. After the Russian invasion crippled conventional networks, Ukraine has relied on Starlink for telecommunications—underscoring both the promise and limits of LEO satellite-based connectivity. Taiwan should cultivate multiple international partners to ensure diverse, resilient communications in the case of a cross-Strait crisis. The U.S. Space Force is also developing its own LEO constellations and should consider developing an agreement with the Taiwanese MND to make it available during a cross-Strait crisis.[366]

Expand the CMA to include jurisdiction over medium to large enterprises and consider requiring specific best practices for incident detection and response.

***

THE PHILIPPINES

The Philippines is one of the United States' closest allies and security partners in the Indo-Pacific. and security partners in the Indo-Pacific, anchored in the 1951 U.S.-Philippine Mutual Defense Treaty. The United States is also among the largest foreign investors in the Philippines and the country's third-largest trading partner.[367] The two countries have conducted a major annual joint military exercise, Balikatan, for nearly 40 years.[368] After a period of hedging under former President Rodrigo Duterte, the Philippines has more explicitly aligned with the United States under President Ferdinand "Bongbong" Marcos Jr. in response to the PRC's rising maritime aggression. Washington should embrace this shift and expand security cooperation broadly, including in the cyber domain.

The United States has a direct interest in strengthening cybersecurity in the Philippines, not only to safeguard existing economic and military ties, but also to pave the way for even closer defense, intelligence, and technology cooperation to counter the PRC's rising aggression. An important but less understood American interest in strengthening Philippine cybersecurity is the country's significant Business Process Outsourcing (BPO) industry, 85 percent of which comes from U.S. companies. This means vast U.S. corporate and personal data is stored within the country—often within vulnerable, on-premise databases—further raising the stakes of stronger cyber defenses.[369]

The Philippines has considerable work ahead. Of the four countries studied in this report, the Philippines is the most vulnerable. Rapid expansion of its digital footprint has dramatically increased the attack surface for opportunistic state and nonstate actors. A 2023 Cisco study estimates that just 1 percent of Philippine organizations are prepared to defend themselves against cyberattacks.[370] Although the government recognizes the danger and has made laudable reforms and investments, the pace of change has not kept up with fast-evolving dangers—especially in updating IT infrastructure and closing massive cyber workforce gaps.

Of the four countries studied in this report, the Philippines is the most vulnerable.

Although the Philippines has improved its cybersecurity posture, notably through the introduction of the 2023 National Cybersecurity Plan and establishing of a new Cyber Command within the Philippine Armed Forces, it continues to lag several ASEAN peers. Between 2020 and 2024, the Philippines' Global Cybersecurity Index score improved from 77 to 93, but it still ranked lower than Singapore, Indonesia, Malaysia, Thailand, and Vietnam.[371] Strengthening cybersecurity and resilience will only grow in importance as Manila works to enhance defense cooperation with the United States and position itself as a global hub for the BPO industry.

Threats

Like the other three countries examined in this report, the Philippines has endured rising cyber

threats in recent years. The Philippines' rapidly expanding digital economy has also expanded cybersecurity vulnerabilities. While the country doubled its digital economy during the COVID-19 pandemic to $17 billion, ransomware attacks in the Philippines also doubled between 2022 and 2023.[372]

Between 2021 and early 2023, the government suffered multiple high-level breaches, including from cyber criminals and state-sponsored actors, resulting in sensitive data leaks.[373] During this period, the Philippine National CERT addressed 3,470 cybersecurity incidents, with malware and malicious code comprising 49 percent, followed by data leakage and compromised websites, which accounted for a 12 percent share each. Over 60 percent of known incidents during this period targeted the government's emergency response systems.[374]

THE PEOPLE'S REPUBLIC OF CHINA

PRC-linked groups have become the Philippines' most persistent and sophisticated cyber threat. With limited technical expertise, Manila struggles with timely attribution of malign state-sponsored cyber operations, effectively giving actors like the PRC a free pass. APT threat actors linked to the PRC seek to monitor and disrupt the country's defense and communications infrastructure, especially as U.S.-Philippine defense cooperation deepens and the PRC's maritime aggression in the South China Sea intensifies. Data from cybersecurity firms indicate that PRC breaches of Philippine computer networks coincide with PRC Coast Guard activities in the South China Sea, suggesting that Beijing links its kinetic and cyber operations.[375] For instance, in August 2023, a PRC APT group launched a cyberattack on the Philippine government systems around the same time a PRC Coast Guard ship fired water cannons at a Philippine Coast Guard ship near the disputed Second Thomas Shoal.[376]

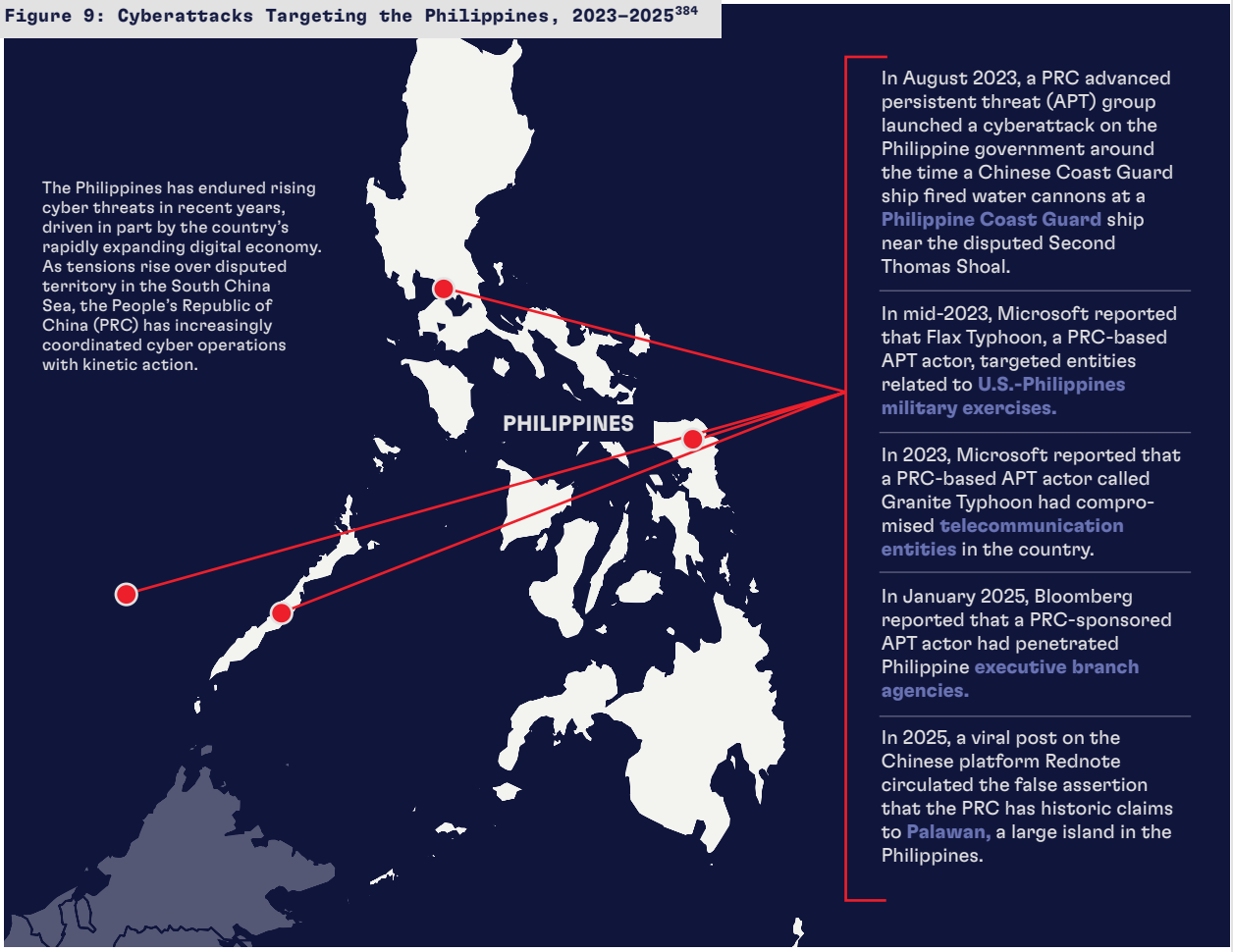
In mid-2023, Microsoft reported that Flax Typhoon, a PRC-based APT actor, targeted entities related to U.S.-Philippines military exercises. That same year, Microsoft reported that another PRC-based APT actor, Granite Typhoon, had compromised telecommunication entities in the country.[377] In January 2025, Bloomberg reported that a PRC-sponsored APT actor had penetrated Philippine executive branch agencies, including the president's office, gaining access as early as 2023, as part of a years-long campaign of espionage and data exfiltration.[378] When the government learned of the attack, officials did not attribute it to a state actor and merely stated, "We are appealing to the Chinese government to help us prevent further attacks."[379] This incident underscores both the technical and geopolitical challenges of attribution for a nation like the Philippines with deep economic ties to China.

Alongside APT threats linked to the PRC, the Philippines also faces information operations that seek to sway public opinion, push false narratives, and undermine government positions—particularly concerning territorial disputes in the South China Sea. For instance, PRC-linked disinformation efforts often criticize the 2016 Hauge Tribunal South China Sea ruling, which stated that the PRC's nine-dash line territorial claim had no legal foundation.[380] One prominent case includes a post on the Chinese platform Rednote, which circulated the false assertion that the PRC has historic claims to Palawan, a large island in the Philippines. After the post spread rapidly, the National Maritime Council swiftly denounced it as "cognitive warfare" and an "absurd fabrication."[381] The PRC has also repeatedly amplified the narrative that the Philippines promised to remove the beached BRP *Sierra Madre* from the disputed Second Thomas Shoal, a deliberately grounded warship the country uses to establish a continuing presence in the contested area.

While the country doubled its digital economy during the COVID-19 pandemic to $17 billion, ransomware attacks in the Philippines also doubled between 2022 and 2023.

Chinese companies have also established a significant presence in the Philippines' digital infrastructure, undermining the country's information security. The country's telecommunications infrastructure relies heavily on Huawei technology and partnerships with Chinese state-run companies, like China Telecommunication Group.[382] Huawei has installed over 12,000 CCTV cameras in Manila and Davao as part of the "Safe Philippines" project, and in

Figure 9: Cyberattacks Targeting the Philippines, 2023–2025[384]



December 2024, the company also launched a cloud region in the country.[383] Ubiquitous Chinese-linked technology and digital infrastructure degrades the country's broader cybersecurity environment.

Stakeholders

As cyber threats worsen, the Philippine government has stood up new agencies to combat cybersecurity and disinformation threats:

- **The Department of Information and Communications Technology (DICT):** coordinates and implements the national ICT development agenda, such as developing technology regulations and standards.[385]
  - **The National Cybersecurity Emergency Response Team (NCERT):** responds to cyber threats nationwide. According to research interviews conducted by CNAS researchers, U.S. investment was critical in reviving NCERT after an extended period of inactivity.[386]
  - **The Cybercrime Investigation and Coordinating Center (CICC):** monitors cybercrime and coordinates responses.[387]
- **The National Cybersecurity Inter-Agency Committee (NCIAC):** coordinates cyber efforts across government agencies.[388] The DICT is the government's secretariat and primary driver for cyber policy. Its members include the heads of key departments, including Justice, Foreign Affairs, and National Defense. The NCIAC also serves as the coordinating body for government agencies but has little authority over the private sector.

- **The Department of Foreign Affairs**: leads international engagement on cybersecurity, including bilateral and multilateral cyber dialogues.
- **The Department of National Defense**: oversees the Armed Forces of the Philippines and coordinates cyber defense cooperation with allies.
  - **The Armed Forces of the Philippines (AFP) Cyber Command**: announced in October 2023, will replace the AFP Cyber Group as the cyber defense unit of the AFP, responsible for safeguarding the military's digital infrastructure against cyber threats.[389]
- **The National Intelligence Coordinating Agency**: leads the Philippine intelligence community's cyber efforts and related intelligence sharing.
- **The Philippine National Police**: falls under the mandate of the Department of the Interior and Local Government, oversees the Anti-Cybercrime Group.[390]

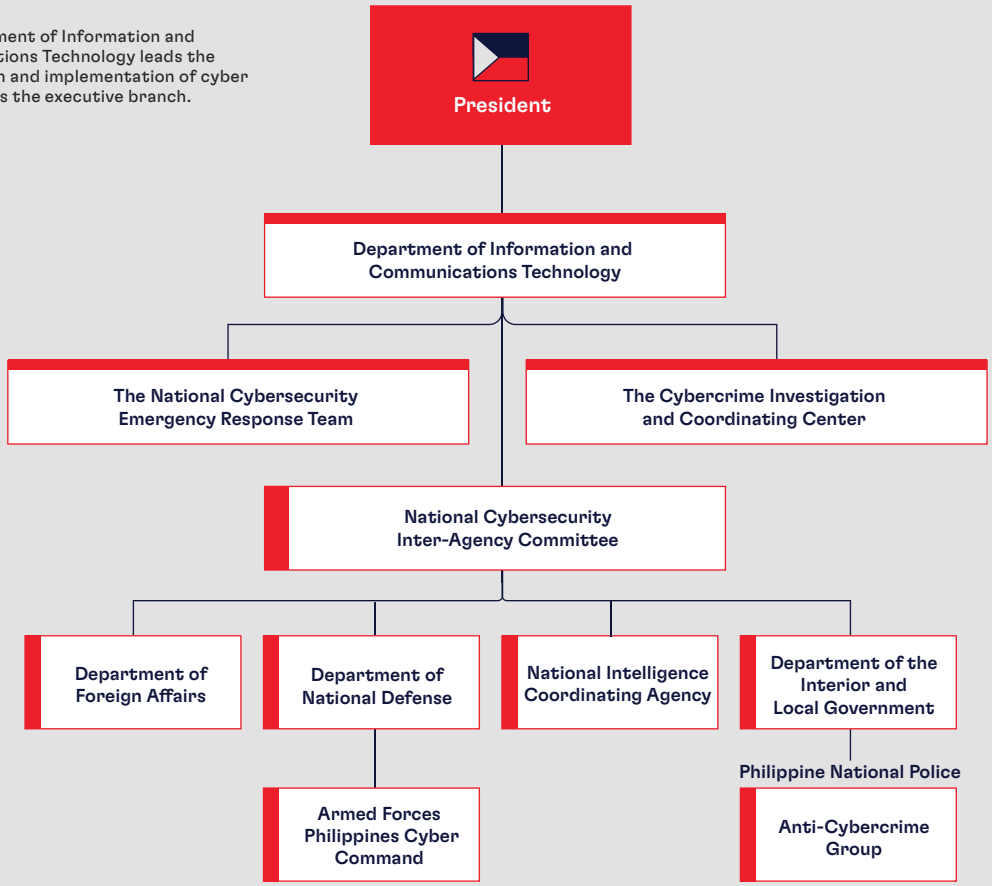
Policy

The Philippines' cyber policy framework remains nascent and relatively undeveloped compared to the three other countries examined in this report. However, the government took a major step forward when President Marcos adopted the five-year National Cybersecurity Plan in April 2024.[392] Key laws and policies for Philippine cybersecurity and resilience include:

- **2023–2028 National Cybersecurity Plan (NCSP)**: outlines three priorities: (1) protecting the Philippine state and population in

Figure 10: The Philippines' Cybersecurity Agencies[391]

The Department of Information and Communications Technology leads the coordination and implementation of cyber issues across the executive branch.



cyberspace; (2) expanding the cyber workforce; and (3) strengthening the cyber policy framework. Other goals include protecting critical information infrastructure and establishing guidelines for using cryptographic primitives and minimum cybersecurity practices in government.[393]

- **Cybersecurity Act**: proposed by the NCSP, calls for passing a Cybersecurity Act that would replace the NCIAC with a new National Cybersecurity Council to serve as the hub for cybersecurity issues across government.[394] All government institutions and private companies would report data breaches to the National Cybersecurity Council promptly or face fines, and the Council would provide quarterly reports on cybersecurity threats.[395] As of March 2025, the Philippines had yet to pass a Cybersecurity Act.
- **2012 Cybercrime Prevention Act**: defines and penalizes cybercrimes while empowering law enforcement agencies to enforce and investigate cyber offenses with judicial oversight. It also establishes the multi-agency CICC, under the Office of the President, for cybersecurity policy coordination.[396]
- **2012 Data Privacy Act**: establishes basic privacy rights for both government and private sector entities and created the National Privacy Commission to oversee compliance, conduct investigations, and enforce data protection policies.[397]

The NCSP sets a path for improving the Philippines' cyber readiness and capacity, building on foundational privacy and cybercrime laws. Opportunities for further progress include clear incident reporting requirements and cyber hygiene best practices for both government and industry. Even with clearer standards, the country's top cybersecurity coordinating body, the NCIAC, has limited enforcement authority over the private sector. Still, robust policy frameworks mean little without the pipeline of trained professionals to implement them.

People

The Philippines faces a massive cyber workforce shortage. An IBM report found that the country had only around 200 cybersecurity professionals designated as Certified Information Systems Security Professionals, the industry gold standard—compared to more than 2,800 in Singapore.[398]

The workforce shortage stems from an undeveloped pipeline for cyber talent. Educational institutions across the Philippines lack cybersecurity curricula, and the institutions with such courses are expensive for average Filipinos.[399] Once trained, cyber professionals often pursue higher wages abroad. Workers also lack clear pathways to work in the public sector, leaving the government's cyber teams understaffed and its systems under-protected. Underscoring this, the Philippine national cyber response team only has 35 members.[400] By contrast, an equivalent from South Korea (KrCERT/CC) had 160 members as of February 2023.[401]

An IBM report found that [the Philippines] had only around 200 cybersecurity professionals designated as Certified Information Systems Security Professionals, the industry gold standard—compared to more than 2,800 in Singapore.

The NCSP outlines steps to bridge the cyber workforce gap. These efforts include establishing an ICT academy under DICT, creating a Cybersecurity Center of Excellence, developing online training and job-matching platforms, and offering scholarships for cybersecurity students.[402] To address cyber workforce challenges in the public sector, the NCSP outlines administrative steps to index ICT and cybersecurity positions in the government, develop qualification and competency standards for these roles, and create certification pathways for cyber positions in the government.[403]

The NCSP sets a promising path forward, but significant work remains. Cyber experts need flexibility to move between public and private sectors, and both sectors should consider additional incentives to attract and retain talent. Efforts to provide competitive compensation and cross-sector opportunities could nurture a growing cyber workforce in

the Philippines. Furthermore, experts at the CNAS workshop in Manila noted that disruption across political administrations undermines policy continuity on talent development.[404]

Manila understandably seeks to harness the economic and social benefits of rapid digitalization and skilling, exemplified by initiatives such as the Philippine Digital Workforce Competitiveness Act, and the Philippine Digital Transformation Framework. These efforts, however, do not match the focus on digital skills with cyber hygiene.[405] This raises the risk that accelerating digitalization and technology adoption will outpace cybersecurity and resilience, deepening the country's already considerable vulnerability. Former DICT Secretary Ivan John E. Uy sought to address this with cyber hygiene initiatives and responsible digital citizenship training.[406] For instance, the government established October as Cybersecurity Awareness Month and committed to creating awareness programs to build cyber literacy in the NCSP.[407] Manila should view these efforts as the bare minimum of what stronger cybersecurity and resilience require.

Partnerships

Philippine cyber experts have consistently called for stronger public-private partnerships. The Philippine private sector helped to shape the NCSP, including through a presidential advisory body consisting of executives from major Philippine firms.[408] The DICT also plans to formalize the private sector's participation in the National Security Operations Center, which leads threat monitoring, vulnerability and penetration testing services, and general assessment of the government's cyber posture.[409] The private sector also assists the government in conducting malware analysis, and the government has established mechanisms for information sharing with industry.

Industry will be a critical partner in upskilling, training, and employing the Philippine cyber workforce, and both the private and public sectors should collaborate in creating competitive incentives for cybersecurity professionals to stay in the Philippines. According to former DICT Secretary Uy, a staggering 80 percent of Filipino cybersecurity professionals work abroad.[410]

Low trust in government also hinders public-private cooperation. The government has not answered rising cybercrime with commensurate increases in enforcement, owing to both a lack of expertise and resources to conduct post-incident investigations. The government has also fallen short in addressing ongoing data security concerns with the country's two dominant telecommunications providers, which are heavily dependent on components from the Chinese companies Huawei and ZTE.[411]

On the international stage, the Philippines is deepening engagements with allies and partners to strengthen cyber capabilities, share intelligence, and participate in common defense. The Philippines has been an active participant in the United Nations' Open-Ended Working Group on Information Communications Technologies, which was established in 2021 to establish collective rules and norms for behavior in cyberspace.[412] The Philippines signed onto the Budapest Convention on Cybercrime in 2021, the first multilateral treaty focused on cybercrime. Through ASEAN, the Philippines participates in initiatives such as the ASCCE and the ASEAN-Japan Cybersecurity Capacity Building Centre.[413] The country also joined the Cyber Risk Institute in April 2024.[414]

Australia has emerged as a key cyber partner for the Philippines. Both countries signed a memorandum of understanding on cyber and critical technology cooperation in February 2024, in which they pledged to share best practices and threat assessments.[415] According to the Australian ambassador to the Philippines, Australia plans to hold local workshops on building resilience to disinformation and will fund scholarships for training cyber professionals in the Philippines.[416]

As with the other countries examined in this report, the United States is the Philippines' most important partner to secure the Indo-Pacific and push back on the PRC's aggression in both the cyber and maritime domains. The 1951 Mutual Defense Treaty and 1998 Visiting Forces Agreement provide a legal basis for U.S. military presence in the country, and Washington and Manila can do more to clarify its application to forward-deployed U.S. cyber officials. Indeed, in May 2023, both countries explicitly named cyberspace as a shared security concern and called for increased cyber defense and cooperation.[417]

Building on this, the two countries held the first U.S.-Philippine cyber-digital policy dialogue in July 2024 and will integrate a cyber dimension into their defense collaboration, including through the annual Balikatan exercise.[418] The United States has also committed to investing in cyber capabilities in the Philippines, including on-demand training to help build a cyber workforce and stand up a new Cyber Command in the Philippine Armed Forces.

Increasingly, U.S.-Philippines defense cooperation has focused on improving the security of the AFP's communications and classified data. The U.S. Army worked with the AFP Signal Regiment in 2024 implement the Anti-jam Resilient Radio Objective Waveform to enhance data transmission and communication reliability.[419] In a significant breakthrough, both countries signed the General Security of Military Information Agreement in 2024, where the countries jointly agreed to cybersecurity standards for the sharing of classified information.[420] Although Philippine law does not appear to explicitly authorize U.S. HFOs or DFOs on Philippine networks, the government's eager embrace of greater cybersecurity cooperation suggests a high ceiling for additional partnership.

Progress and Recommendations

Among the four nations examined in this report, the Philippines stands out as the most vulnerable to cyber threats from malign state and nonstate actors alike. It is not because leaders in Manila have failed to appreciate growing cyber threats or prioritize cyber resilience. Rather, the country's rapidly growing digital economy has significantly expanded the potential attack surface, outpacing efforts to build a cyber workforce and expand basic cyber hygiene and awareness.

More than any of the four countries examined in this report, cyber progress in the Philippines will require close partnership with the United States, Australia, and other cyber-leading nations in the Indo-Pacific to align cybersecurity policies with prevailing best practices on intergovernmental coordination and incident reporting. Opportunities to deepen the U.S.-Philippine cyber partnership include creating accountability and deterrence for malicious cyber actors, greater regional collaboration in fighting cybercrime, protection for critical infrastructure such as undersea cables, and better CERT cooperation.[421]

Among the four nations examined in this report, the Philippines stands out as the most vulnerable to cyber threats from malign state and nonstate actors alike.

To address these issues, the report offers the following recommendations to leaders in the Philippine government:

Launch a national campaign to expand the cyber workforce. Manila should treat bridging the cyber workforce gap as a national security imperative. To this end, the government should partner with domestic and foreign technology companies to develop—and ideally require—cyber curriculum for secondary and higher education. These partnerships could also expand access to free online training and AI-enabled tools. The government should explore incentives to retain domestically trained talent through scholarships in exchange for government service, along with incentives to repatriate Philippine cyber talent now abroad. In addition, it should provide clearer certification pathways for private cyber professionals to transition into the public sector to fill critical shortages.

Empower a centralized authority, like the NCIAC, to develop uniform incident reporting standards and consolidate collection. Today, differing standards and unclear sharing protocols for incident reporting across agencies deprive the government of holistic situational awareness about cyber threats.

Partner with the United States, Japan, and Australia to promote secure and trusted ICT infrastructure. Expedite approvals for investments from the U.S. International Development Finance Corporation and Japan Bank for International Cooperation to promote secure subsea cable infrastructure and 5G telecommunications. Leverage the new Open RAN laboratory

in Quezon City—jointly supported by DICT and the U.S. government—to promote Open RAN networks as a secure alternative to Huawei- and ZTE-built telecommunications infrastructure.

Allocate more of the national security and defense budget to modernizing vulnerable IT infrastructure and explore incentives for critical infrastructure operators to do the same.

Integrate cybersecurity into digital skilling and workforce initiatives, like the Philippine Digital Workforce Competitiveness Act and the Philippine Digital Transformation Framework.

Publicly link increased cyberattacks to Chinese maritime aggression to build public awareness of the integrated threat. The perception of cyberattacks as nuisance criminal acts can undermine motivation to prioritize cyber resilience.

Push BPO companies to adopt cybersecurity best practices, such as strengthening physical security at facilities and migrating sensitive data to secure cloud-based solutions.

***

RECOMMENDATIONS

The United States and its Indo-Pacific allies face a landscape of cyber threats that has grown more varied, volatile, and dangerous than ever. As the PRC blows past the limits of conventional cyber operations focused on espionage and exfiltration to embrace a dangerous new game of pre-positioning in critical infrastructure, interfering in democratic elections, and wielding cyber operations to reinforce maritime and other aggression in the physical world, it has become clear that Washington and its Indo-Pacific allies require a new approach.

Efforts to strengthen domestic cyber resilience across the Indo-Pacific are necessary but insufficient given the region's increasingly dangerous cyber landscape. In most of the four countries studied in this report, broad adoption of even minimal best practices remains elusive. On their own, each of the four countries examined in this report face considerable technical and political hurdles to making clear, timely attributions for state-sponsored cyber operations. In practice, this limits accountability for the PRC's malign cyber operations, encouraging further aggression. The cumulative effect is a degraded cyber landscape across the Indo-Pacific, impeding each country's aspirations to harness the potential of accelerating digitalization and connectivity for their economies and societies, and limiting ambitions on both sides of the Pacific to deepen military, intelligence, and economic partnerships.

Although Washington has recently embraced a more public approach to "name and shame" PRC-sponsored cyber operations, its finger-wagging statements and targeted sanctions have thus far failed to stem growing dangers.

To confront rising cyber threats across the Indo-Pacific, the United States, and its partners need a newly assertive and coordinated approach that intensifies efforts on two fronts: (1) building capacity within each country to strengthen cybersecurity and resilience through policy reforms, technology modernization, and talent development, and (2) strengthening cooperation to enable more integrated, proactive cyber defense, clear and collective signaling for malign state cyber actors, and alternatives to push back on insecure PRC-linked digital infrastructure across the region.

To that end, this section offers extended recommendations first to leaders in the U.S. government. It then offers cross-cutting recommendations for government leaders in Japan, South Korea, Taiwan, and the Philippines to complement the earlier country-specific recommendations.

Many of these cross-cutting recommendations could easily apply to the United States, which faces significant challenges of its own to strengthen domestic cybersecurity and resilience. However, detailing these recommendations is beyond the scope of this report. Indeed, policymakers in Washington may find that Japan, South Korea, Taiwan, and the Philippines soon achieve progress that has long remained elusive for the United States, such as passing a unified cybersecurity law to streamline roles and responsibilities across government and strengthening incident reporting, response, and mitigation standards. Leaders across all five countries have much to learn from one another as they confront shared cyber threats.

United States

Launch a "Cyber Shield" for Indo-Pacific treaty allies.

Washington must think ambitiously to harness the collective power of its Indo-Pacific allies and partners and overcome asymmetries the PRC has exploited to escalate its malign cyber operations across the region. This new Cyber Shield would include three pillars:

- **JOINT RESOLVE.** Washington and its Indo-Pacific treaty allies should issue a joint statement calling out the PRC's cyber aggression and committing to a significant collective response, including but not limited to cyber measures, should it continue. Although not all nations could match U.S. cyber capabilities to effectively respond, they can contribute by ending Chinese-linked contracts, withdrawing from Chinese-led forums, or levying sanctions. With that said, public warnings would mean little—and could indeed be counterproductive—if they do not come with meaningful follow-through. On their own, nations like the Philippines or South Korea will likely remain reluctant to name and respond to PRC-linked cyber operations, even as they continue to rise. A public, collective commitment could increase their resolve.

- **JOINT RESPONSE.** Divergent interests and risk tolerances across key Indo-Pacific partners limit efforts to maximize collective defense by muddling whether, and to what extent, each nation will respond, if at all, to malign state-sponsored cyber actors. Although perfect alignment is unrealistic, the United States could lead the development of a joint escalation ladder, delineating the types of malign cyber operations and subsequent harm that would trigger a collective response. For example, a joint escalation ladder could clarify that crippling attacks against critical elections, energy, health, financial, or military infrastructure would trigger a response. Such a framework could clarify a range of potential response options and facilitate more agile, flexible, and effective countermeasures.

- **JOINT RESOURCES.** Washington should provide a comprehensive framework for Indo-Pacific allies and partners to access increased cyber intelligence sharing, proactive cyber defense operations, joint civilian and military cyber exercises, workforce training, and capacity building from the U.S. government and industry. In response, allies would agree to make sufficient investments to modernize military and intelligence cyber capabilities, pursue reforms to facilitate cyber threat detection, intelligence sharing and HFOs and DFOs, reduce regulations that discriminate against U.S. cybersecurity providers, and limit vulnerable PRC-linked technology and infrastructure. The U.S. government already encourages many of these efforts separately with different partners, but providing a clear and consistent roadmap could lend coherence to Washington's broader approach and offer more compelling incentives to partners.

Significantly expand military cyber engagement and capacity building by the U.S. military's five component commands in the Indo-Pacific area of responsibility (AOR) with priority regional allies and partners.

The U.S. military's five component commands interface regularly with regional counterparts and are best positioned to lead increased outreach based in operational realities, with coordinating support from U.S. Indo-Pacific Command and technical expertise from U.S. Cyber Command.

- Create new units within the five component commands—U.S. Pacific Fleet, U.S. Pacific Air Forces, U.S. Army Pacific, U.S. Marine Forces Pacific, and U.S. Space Forces, Indo-Pacific—dedicated to cyber engagement and capacity building with key regional allies and partners.

- Conduct regular joint tabletop military cyber exercises across the Indo-Pacific AOR with representatives from relevant component commands, U.S. Cyber Command, allied and partner militaries, and relevant industry stakeholders. These could take place either independently or on the margins of existing bilateral or multilateral exercises.

- Require a prominent cyber element in every bilateral and regional joint military exercise. Several major exercises in 2024 featured a cyber element, including the Super Garuda Shield exercise with the United States, Indonesia, and 12 other partners; the Yama Sakura 87 between the United States, Japan, and Australia; and Exercise Balikatan between the United States and the Philippines.
- Expand participation by Indo-Pacific nations in major cyber exercises, such as U.S. Cyber Command's annual Cyber Flag or the International Coordinated Cyber Security Activity.
- Place U.S. Cyber Command attachés in priority Indo-Pacific countries to promote cooperation and information sharing.
- Expand opportunities for U.S. Indo-Pacific Command Cyber Operations Integrated Planning Elements (CO-IPE), created in 2017, to host vetted foreign liaison officers from priority regional partners to improve information sharing and coordination.

Clarify legal and policy frameworks to facilitate expanded HFOs and DFOs in the Indo-Pacific.

In the four countries examined in this report, the legal basis for expanding these operations remains ambiguous at best. Washington should intensify efforts with partner governments to pursue legislative and policy reforms to enable expanded HFOs and DFOs with the host country's permission. Such a framework would clarify the conditions for soliciting and approving HFOs.

Preserve and strengthen the State Department's Bureau of Cyberspace and Digital Policy (CDP).

CDP has been highly effective at elevating cybersecurity and digital issues in U.S. foreign policy, both with foreign partners and within the Department itself. It replaced an ineffective, disparate approach to cyber and digital diplomacy that diffused and often buried responsibilities across the department with a consolidated locus of subject matter experts. CDP's creation also signaled to other government's Washington's prioritization of technology in foreign policy, and other governments have since moved to emulate CDP's model. Since its inception, demand for the CDP-led trainings on cyberspace and digital policy for U.S. foreign service officers has also consistently exceeded demand, and the number of bilateral and plurilateral cyber dialogues has proliferated. The Trump administration should strengthen the CDP by acting to:

- Expand the Cyber Capacity Building Fund authorized by Congress to allow CDP to provide agile support to allies.
- Ensure sufficient staff capacity to liaise with the U.S. DoD—specifically U.S. Cyber Command and U.S. Indo-Pacific Command—to better align U.S. cyber engagement abroad across the civilian and military domains.
- Designate CDP as the principal coordinator for all civilian cyber engagement and capacity building. CDP nominally leads U.S. cyber diplomacy in bilateral, multilateral, and international forums, and cyber capacity building overseas, while serving as an in-house subject matter expert for State. In practice, cyber capacity building, and diplomatic engagement occurs across the interagency, often with little to no coordination. Although each agency brings domain expertise to the table, the effect is a proliferation of poorly coordinated cyber engagements that burden foreign partners. The Trump administration should make CDP the "control tower" for civilian U.S. cyber engagements abroad; at the same time, it should do so in a way that does not unduly impede bilateral cyber cooperation on discrete operational areas such as law enforcement.
- Rationalize cyber dialogues. As of June 2025, the United States was party to at least 60 distinct cyber and tech dialogues. Although this reflects welcome demand from foreign allies and partners for engagement, it burdens CDP's limited staff—and foreign counterparts with even fewer resources—who spend countless hours managing these recurring events. The administration should prioritize these dialogues for the most strategically vital and cyber

vulnerable allies and partners—including Japan, South Korea, Taiwan, and the Philippines. The administration should also seek opportunities to convert or complement existing cyber dialogues with regional discussions to reinforce the importance of collective cyber defense.

- Reconsider the planned reorganization of CDP under the undersecretary for economic growth, energy, and the environment ("E") and instead preserve it as an independent bureau reporting directly to the secretary or deputy secretary. Collapsing CDP under "E" risks subsuming cyber and digital policy within the bureaucracy; even if the undersecretary under the Trump administration prioritizes cyber and digital affairs, there is no guarantee their successor will do the same. Furthermore, splitting off CDP's cybersecurity team would also weaken its ability to conduct holistic cyber engagement and diplomacy with foreign counterparts and reduce the effectiveness of its current, integrated structure.

Develop a unified strategy for promoting secure and resilient ICT infrastructure in the Indo-Pacific drawing on the full range of U.S. government tools.

There are numerous offices, funding authorities, and initiatives across the U.S. government to promote secure ICT infrastructure in the Indo-Pacific. The sum of these efforts falls short of its parts as agencies pursue different priority countries, sectors, and even strategic objectives—diffusing funds globally and limiting impact. Despite attempts to better coordinate these efforts, progress has been uneven and has failed to match either the coherence or resource level of the PRC's Digital Silk Road.

To close this gap, the administration should direct the Department of State to lead a government-wide effort to inventory relevant programs and initiatives, identify priority countries—with a focus on the Indo-Pacific—as well as priority ICT sectors with direct security implications for U.S. interests. Once identified, these priorities should drive U.S. investments to maximize limited resources. A new cyber and digital strategy, as mentioned above, should include this review.

Pursue agreements to expand the Cyber Trust Mark with Indo-Pacific partners, mirroring the January 2024 agreement with the EU.

The Cyber Trust Mark is a voluntary certification—like the Energy Star rating indicating the energy efficiency of consumer appliances—to ensure connected devices, such as routers, and smart thermostats meet high cybersecurity standards. This would be especially useful in South Korea, which faces surging botnet attacks from compromised connected devices.

Encourage Japan's participation in AUKUS Pillar II, which creates a framework for improved intelligence sharing and cyber cooperation.

This is provided the Japanese government implements the new information security law and makes sufficient investments to modernize technology and IT infrastructure to harden defenses and facilitate intelligence sharing.

Scale joint military cybersecurity cooperation with Taiwan.

The FY 2024 NDAA authorized joint military cybersecurity activities, training, and assistance to harden Taiwan's military infrastructure and networks while leveraging U.S. military and commercial cybersecurity technologies. This should include U.S. Cyber Command significantly expanding HFOs in Taiwan.

Prioritize the provision of defensive cybersecurity capabilities through the new Taiwan Security Cooperation Initiative.

This initiative authorizes the DoD to provide up to $300 million in total assistance, including defensive cybersecurity capabilities.

Japan, South Korea, Taiwan, and the Philippines

Mandate adoption of cybersecurity best practices across government.

This includes a prohibition on the use of personal devices for work-related activities, MFA, and end-to-end encryption for internal communications. Participants at workshops hosted by CNAS researchers in Tokyo, Seoul, Taipei, and Manila all noted that cybersecurity practices across government remain uneven, with many employees routinely using personal devices for business.[422] At the same time, this will require investment and reforms to modernize IT and information security policy, and practice to reduce incentives for government workers to seek unsecure alternatives. The NIST Cybersecurity Framework 2.0 provides comprehensive guidance for both government and industry to manage cybersecurity risks.[423]

Prioritize cybersecurity in increased defense spending.

This includes replacing at-risk, legacy IT infrastructure, acquiring AI-enabled threat detection and response platforms, and secure, cloud-based cybersecurity solutions where appropriate. There are narrow cases—especially in specific national security and intelligence contexts—where air-gapped, on-premise servers remain appropriate. However, most government services would benefit from migrating to modern, cloud-based systems secured by the latest AI-enabled cyber defenses.

Deepen partnerships with local and foreign technology companies to benefit from broader threat data and best-in-class capabilities.

Local laws to privilege domestic technology companies, however well-intentioned, often impede public agencies and private companies from accessing best-in-class cybersecurity solutions.

Clarify legal and security frameworks to allow forward-deployed teams from U.S. Cyber Command.

Reforms would facilitate the approval process for U.S. Cyber Command personnel to deploy in-country. This could include episodic deployments of Cyber Protection Teams from the Cyber National Mission Force to conduct HFOs, as well as full-time attachés.

Designate a single point of entry to route intergovernmental cyber coordination.

An alternative would be to designate clear points of contact for essential cyber roles, including policy, intelligence sharing and threat identification, and emergency response.

Develop an integrated strategy to counter malign foreign influence.

The strategy would combine intelligence, cyber, diplomatic, and economic tools to better identify, deter, disrupt, and respond to adversary influence operations. Foreign adversaries do not see a distinction between the "traditional" cyber and information domains, but government bureaucracies often diffuse responsibilities for identifying, analyzing, and responding to foreign malign influence campaigns across different agencies—often with poor coordination. Part of this strategy should include timely disclosing of coordinated foreign malign influence operations with Indo-Pacific partners and allies.

Establish clear and uniform skills and competencies for cybersecurity roles in government, aligning wherever possible with private sector certifications.

This will provide clarity to students, workers, and educational institutions about requirements to secure public sector cybersecurity roles, expanding the pipeline. It would also facilitate two-way career transitions for cybersecurity professionals between the public and private sectors.

Leverage AI tools to boost productivity of limited cybersecurity professionals.

All four countries face challenges in bridging their cyber workforce gaps, and progress will take time. Governments should embrace AI tools that enable fewer cyber professionals to do more, for instance, by automating repetitive tasks, enhancing threat detection, and improving incident response. In a survey of over 1,100 U.S. cybersecurity professionals, 82 percent "expressed optimism that AI will improve job efficiency."[424]

Develop a strategy to transition from compromised ICT hardware, software, and infrastructure from vendors linked to foreign adversaries.

Complete decoupling from Chinese-linked technology vendors is unrealistic, but at a minimum, governments should restrict compromised products in security-sensitive contexts and limit new acquisitions.

Encourage businesses to adopt Secure by Design and Secure by Default principles.

Launched by CISA in 2023, Secure by Design is a voluntary pledge for ICT providers to make a "good-faith effort" toward implementing seven goals that "prioritize the security of customers as a core business requirement, rather than merely treating it as a technical feature."[425] Secure by Default, introduced by the UK government in 2019, focuses on limiting zero-day vulnerabilities by defaulting products to the highest security settings, instead of requiring users to manually select them.

Boost public awareness about the ties between escalating cyberattacks and national security.

Foreign adversaries benefit from outdated public attitudes that view cyberattacks as a nuisance, criminal issue instead of a national security imperative. Governments have a role to play in increasing this awareness. This can also reduce the stigma of reporting cyber breaches, which remain strong in many Indo-Pacific markets according to research interviews for this report.[426]

***

CONCLUSION

The Indo-Pacific is at a cyber crossroads. Several trends for the region seem fixed in the short term: growing geostrategic importance as the principal theater for U.S.-China competition; ongoing digitalization of its public and private sectors; and increasing cyber threats from the PRC, North Korea, Russia, and a growing shadow industry of cybercriminals and hacktivists for hire. The question for governments from Tokyo to Taipei is whether they can navigate the tumultuous cyber landscape ahead with the bold actions on policies, personnel, and partnerships required to boost security and resilience. The United States has a vested interest in their success given the vital military, intelligence, and commercial ties across the Indo-Pacific and aspirations to deepen them further still.

Governments across the Indo-Pacific have undertaken an overdue but welcome shift in elevating cybersecurity as foundational to national security. The volume of new strategies, plans, and dialogues across the Indo-Pacific, however, can risk lending the impression that regional governments are making sufficient progress. They are not.

Arresting the rise of cyber threats across the region demands a newly assertive and coordinated approach from the United States and its Indo-Pacific allies and partners to both strengthen cybersecurity within each country and cyber cooperation among them to enable more integrated, proactive cyber defense. Differences in risk tolerances, capabilities, and policies between the United States and allied governments are inevitable, but leaders should work to close gaps that adversaries rush to exploit. They must also strengthen the cyber frameworks and capabilities to inflict meaningful costs on adversaries when they conduct malicious cyber operations, including through a new Cyber Shield to bolster joint resolve, response, and resources.

Strengthening cybersecurity across the Indo-Pacific is a generational effort that will require sustained investment, prioritization, and partnership from leaders across both government and industry. None of this will be easy, but it is essential to realizing a future for the Indo-Pacific defined not by fears of digital vulnerability, but common aspirations for greater connectivity, collaboration, and partnership. That future remains up for grabs.

1. *Indo-Pacific Strategy of the United States* (The White House, February 2022), https://bidenwhitehouse.archives.gov/wp-content/uploads/2022/02/U.S.-Indo-Pacific-Strategy.pdf.

2. *National Security Strategy of Japan* (Cabinet Secretariat, December 2022), https://www.cas.go.jp/jp/siryou/221216anzenhoshou/nss-e.pdf.

3. *Republic of Korea National Cybersecurity Strategy* (Republic of Korea Office of the President, Office of National Security, February 1, 2024), https://drive.google.com/file/d/1tFMCjggC2Q9_Du-ze-GoiAYBcu5Jw-Lo/view?usp=sharing.

4. Chung Li-hua and Jake Chung, "Digital Resilience Plan Advances," *Taipei Times*, November 17, 2023, https://www.taipeitimes.com/News/front/archives/2023/11/17/2003809291.

5. *National Cybersecurity Plan 2023-2028* (Republic of the Philippines Department of Information and Communications Technology, February 2024), https://cms-cdn.e.gov.ph/DICT/pdf/NCSP-2023-2028-FINAL-DICT.pdf.

6. Sunha Bae, "Deterrence Under Pressure: Sustaining U.S.–ROK Cyber Cooperation Against North Korea," Center for Strategic and International Studies, April 1, 2025, https://www.csis.org/analysis/deterrence-under-pressure-sustaining-us-rok-cyber-cooperation-against-north-korea

7. "People's Republic of China Cyber Threat," Cybersecurity and Infrastructure Security Agency, https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors/china.

8. Patrick Wintour, Julian Borger, and Justin McCurry, "Russia Planned Cyber-Attack on Tokyo Olympics, Says UK," *The Guardian*, October 20, 2020, https://www.theguardian.com/world/2020/oct/19/russia-planned-cyber-attack-on-tokyo-olympics-says-uk.

9. "Philippines," CIA World Factbook, April 30, 2025, https://www.cia.gov/the-world-factbook/countries/philippines/; "Building Cybersecurity Capability in the Philippines," Open Gov, December 28, 2022, https://opengovasia.com/2022/12/28/building-cybersecurity-capability-in-the-philippines/.

10. "CYBER 101: Hunt Forward Operations," U.S. Cyber Command, archived November 15, 2022, https://web.archive.org/web/20221115175331/https://www.cybercom.mil/Media/News/Article/3218642/cyber-101-hunt-forward-operations/.

11. *To Receive Testimony on the Posture of United States Special Operations Command and United States Cyber Command in Review of the Defense Authorization Request for Fiscal Year 2025 and the Future Years Defense Program: Hearing Before the Senate Committee on Armed Services*, 118th Cong. (2024) (statement of General Timothy D. Haugh, Commander of U.S. Cyber Command), https://www.armed-services.senate.gov/imo/media/doc/20242.pdf.

12. Alex Botting and Inés Jordan-Zoob, "The Indo-Pacific Region Needs a Comprehensive Digital Trade Agenda," Wilson Center, September 15, 2023, https://www.wilsoncenter.org/article/indo-pacific-region-needs-comprehensive-digital-trade-agenda.

13. "The Indo-Pacific Strategy," U.S. Department of State, https://www.state.gov/indo-pacific-strategy/.

14. *Advancing Digital Connectivity in the Indo-Pacific Region* (United States Agency for International Development, July 30, 2018, archived September 30, 2023), https://web.archive.org/web/20250129105740/https://2017-2020.usaid.gov/sites/default/files/documents/1861/USAID_DCCP_Fact_Sheet_080719f.pdf.

15. *Advancing Digital Connectivity in the Indo-Pacific Region.*

16. Sapna Chadha, "How Southeast Asia Can Become a $1 Trillion Digital Economy," World Economic Forum, December 12, 2023, https://www.weforum.org/stories/2023/12/how-southeast-asia-can-become-trillion-digital-economy/.

17. *E-Conomy SEA 2024* (Google, TEMASEK, and Bain & Company, 2024), https://services.google.com/fh/files/misc/e_conomy_sea_2024_report.pdf.

18. Chadha, "How Southeast Asia Can Become a $1 Trillion Digital Economy."

19. "India Country Commercial Guide," International Trade Administration, September 18, 2024, https://www.trade.gov/country-commercial-guides/india-digital-economy.

20. *Advancing Digital Connectivity in the Indo-Pacific Region.*

21. *Indo-Pacific Strategy of the United States*.

22. "Nation State Threats," Microsoft Security, https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report-2022-nation-state-attacks.

23. "Nation-State Cyber Actors," Cybersecurity and Infrastructure Security Agency, https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors.

24. "Nation-State Cyber Actors."

25. Council on Foreign Relations Cyber Operations Tracker Database (North Korea, China, and Russia, 2025; accessed February 7, 2025), https://www.cfr.org/cyber-operations/.

26. *China's Alternative Cyber Governance Regime: Hearing Before the U.S. China Economic Security Review Commission,* 116th Cong. (2020) (statement of Adam Segal, Ira A. Lipman, Chair in Emerging Technologies and National Security and Director, Digital and Cyberspace Policy Program Council on Foreign Relations), https://www.uscc.gov/sites/default/files/testimonies/March%2013%20Hearing_Panel%203_Adam%20Segal%20CFR.pdf.

27. Jen Easterly, "Unsafe at Any CPU Speed: The Designed-in Dangers of Technology and What We Can Do About It" (public event, Carnegie Mellon University, Pittsburgh, PA, February 27, 2023), https://www.cisa.gov/securebydesign/dir-easterly-remarks-carnegie-mellon-university.

28. Council on Foreign Relations Cyber Operations Tracker Database.

29. "People's Republic of China Cyber Threat."

30. Swati Khandelwal, "Chinese Hackers Target Air-Gapped Networks in Southeast Asia," The Hacker News, April 13, 2015, https://thehackernews.com/2015/04/a-state-spon-

sored-cyber-espionage-group.html.

31. Colin Packham, "Exclusive: Australia Concluded China Was Behind Hack on Parliament, Political Parties—Sources," Reuters, September 15, 2019, https://www.reuters.com/article/world/exclusive-australia-concluded-china-was-behind-hack-on-parliament-political-pa-idUSKBN1W106H/.

32. Natasha Bertrand, Kevin Liptak, and Brian Fung, "Biden Administration Debating Whether and How to Sanction China for Ransomware Attacks," CNN, July 20, 2021, https://edition.cnn.com/2021/07/19/politics/china-biden-ransomware/index.html.

33. James Pomfret and Yew Lun Tian, "APT31: The Chinese Hacking Group Behind Global Cyberespionage Campaign," March 26, 2024, https://www.reuters.com/technology/cybersecurity/apt31-chinese-hacking-group-behind-global-cyberespionage-campaign-2024-03-26/.

34. Microsoft Threat Intelligence, "Volt Typhoon Targets US Critical Infrastructure with Living-Off-the-Land Techniques," Microsoft, May 24, 2023, https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/; Microsoft Threat Intelligence, "Flax Typhoon Using Legitimate Software to Quietly Access Taiwanese Organizations," Microsoft, August 24, 2023, https://www.microsoft.com/en-us/security/blog/2023/08/24/flax-typhoon-using-legitimate-software-to-quietly-access-taiwanese-organizations/.

35. Pomfret and Tian, "APT31: The Chinese Hacking Group Behind Global Cyberespionage Campaign."

36. *Microsoft Digital Defense Report 2023* (Microsoft Threat Intelligence, October 2023), https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023.

37. Dustin Volz, "In a Secret Meeting, China Acknowledged Role in U.S. Infrastructure Hacks," *The Wall Street Journal*, April 10, 2025, https://www.wsj.com/politics/national-security/in-secret-meeting-china-acknowledged-role-in-u-s-infrastructure-hacks-c5ab37cb?st=Ts2qFf&reflink=article_copyURL_share.

38. "Stately Taurus Targets the Philippines as Tensions Flare in the South Pacific," Unit 42, November 17, 2023, https://unit42.paloaltonetworks.com/stately-taurus-targets-philippines-government-cyberespionage/.

39. "Rhetoric Foreshadows Cyber Activity in the South China Sea," CrowdStrike Blog, June 1, 2015, https://www.crowdstrike.com/en-us/blog/rhetoric-foreshadows-cyber-activity-in-the-south-china-sea/.

40. Omer Yoachimik and Jorge Pacheco, "DDoS Threat Report For 2023 Q4," Cloudflare, January 9, 2024, https://blog.cloudflare.com/ddos-threat-report-2023-q4/.

41. Jessica Chen Weiss, "A World Safe for Autocracy?" *Foreign Affairs,* June 11, 2019, https://www.foreignaffairs.com/articles/china/2019-06-11/world-safe-autocracy.

42. *Annual Threat Assessment of the U.S. Intelligence Community* (Office of the Director of National Intelligence, February 5, 2024), https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf.

43. Weiss, "A World Safe for Autocracy?"; Sherisse Pham and Yuli Yang, "Telegram Reports Powerful Cyberattack From China During Hong Kong Protests," CNN, June 13, 2019, https://www.cnn.com/2019/06/13/tech/telegram-ddos-attack-hong-kong-china/index.html.

44. Nicole Perlroth, Kate Conger, and Paul Mozur, "China Sharpens Hacking to Hound Its Minorities, Far and Wide." *The New York Times*, October 22, 2019, https://www.nytimes.com/2019/10/22/technology/china-hackers-ethnic-minorities.html.

45. Liza Lin and Austin Ramzy, "Leaked Hacking Documents Show China's Focus on Tracking Ethnic Minorities," *The Wall Street Journal*, February 27, 2024, https://www.wsj.com/world/china/china-hacking-documents-target-ethnic-minorities-1c582813.

46. Lin and Ramzy, "Leaked Hacking Documents Show China's Focus on Tracking Ethnic Minorities."

47. Christopher Tong, "China Turns to Private Hackers as It Cracks Down on Online Activists on Tiananmen Square Anniversary," The University of Maryland Baltimore County, June 7, 2024, https://umbc.edu/stories/china-private-hackers-tiananmen-square-anniversary/; U.S. Department of Justice, "Seven Hackers Associated with Chinese Government Charged with Computer Intrusions Targeting Perceived Critics of China and U.S. Businesses and Politicians," press release, March 25, 2024, https://www.justice.gov/opa/pr/seven-hackers-associated-chinese-government-charged-computer-intrusions-targeting-perceived.

48. Zeba Siddiqui, "Five Eyes Intelligence Chiefs Warn on China's 'Theft' of Intellectual Property," Reuters, October 18, 2023, https://www.reuters.com/world/five-eyes-intelligence-chiefs-warn-chinas-theft-intellectual-property-2023-10-18/.

49. Adam Segal, "China Has Raised the Cyber Stakes," *Foreign Affairs,* January 21, 2025, https://www.foreignaffairs.com/united-states/china-has-raised-cyber-stakes.

50. Segal, "China Has Raised the Cyber Stakes."

51. Daryna Antoniuk, "Japan Sees Increased Cyberthreats to Critical Infrastructure, Particularly from China," The Record, February 16, 2024, https://therecord.media/japan-critical-infrastructure-cyberthreats.

52. *Microsoft Digital Defense Report 2023*

53. Ken Dilanian, Summer Concepcion, and Kyla Guilfoil, "FBI Director Warns Chinese Hackers Aim to 'Wreak Havoc' on U.S. Critical Infrastructure," NBC News, January 31, 2024, https://www.nbcnews.com/politics/national-security/fbi-director-warn-chinese-hackers-aim-wreak-havoc-us-critical-infrastr-rcna136524.

54. Niharika Mandhana and Gordon Fairclough, "China Is 'Prepositioning' for Future Cyberattacks—and the New NSA Chief Is Worried," *The Wall Street Journal,* June 3, 2024, https://www.wsj.com/politics/national-security/china-is-prepositioning-for-future-cyberattacksand-the-new-nsa-chief-is-worried-5ede04ef.

55. Mandhana and Fairclough, "China Is 'Prepositioning' for Future Cyberattacks—and the New NSA Chief Is Worried."

56. *China's Alternative Cyber Governance Regime: Hearing Before the U.S.-China Economic Security Review Commission* (statement of Adam Segal).

57. *China's Alternative Cyber Governance Regime: Hearing Before the U.S.-China Economic Security Review Commission* (statement of Adam Segal).

58. Dr. Gatra Priyandita, Bart Hogeveen, and Dr. Ben Stevens, *State-Sponsored Economic Cyber-Espionage for Commercial Purposes* (Australian Strategic Policy Institute and the International Cyber Policy Centre, No. 67, 2022), https://ad-aspi.s3.ap-southeast-2.amazonaws.com/2022-12/State-sponsored%20economic%20cyber-espionage_0.pdf?VersionId=L0VXw3il0y4lQv4PcMLT07.a7yZzdJNs.

59. *China's Alternative Cyber Governance Regime: Hearing Before the U.S.-China Economic Security Review Commission* (statement of Adam Segal).

60. *Indo-Pacific Strategy of the United States.*

61. *Annual Threat Assessment of the U.S. Intelligence Community.*

62. Edith M. Lederer, "UN Experts Investigating 58 Suspected North Korean Cyberattacks Valued at About $3 Billion," Associated Press, February 9, 2024, https://apnews.com/article/un-experts-north-korea-cyberattacks-nuclear-sanctions-8e84703049dfb4fda011829115777c9e.

63. Council on Foreign Relations Cyber Operations Tracker Database.

64. *Microsoft Digital Defense Report 2023.*

65. Kate Irwin, "FBI: North Korean Hackers Are Using Malware to Attack Crypto Exchanges," PCMag, September 4, 2024, https://www.pcmag.com/news/fbi-north-korean-hackers-are-using-malware-to-attack-crypto-exchanges.

66. Michelle Nichols, "Exclusive: UN Experts Investigate 58 Cyberattacks Worth $3 Bln by North Korea," Reuters, February 8, 2024, https://www.reuters.com/technology/cybersecurity/un-experts-investigate-58-cyberattacks-worth-3-bln-by-north-korea-2024-02-08/; *North Korean Tactics, Techniques, and Procedures for Revenue Generation* (Office of the Director of National Intelligence, July 2023), https://www.dni.gov/files/CTIIC/documents/products/North-Korean-TTPs-for-Revenue-Generation.pdf.

67. *Microsoft Digital Defense Report 2023.*

68. "#StopRansomware: Ransomware Attacks on Critical Infrastructure Fund DPRK Malicious Cyber Activities," Cybersecurity and Infrastructure Security Agency, February 9, 2023, https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-040a.

69. Kurt Baker, "Advanced Persistent Threats (APT) Explained," CrowdStrike, March 4, 2025, https://www.crowdstrike.com/cybersecurity-101/advanced-persistent-threat-apt/.

70. U.S. Department of Justice, "North Korean Regime-Backed Programmer Charged with Conspiracy to Conduct Multiple Cyber Attacks and Intrusions," press release, September 6, 2018, https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and; Chloe Albanesius,"FBI: North Korea 'Responsible' for Sony Pictures Hack," PCMag, December 19, 2024, https://www.pcmag.com/news/fbi-north-korea-responsible-for-sony-pictures-hack.

71. Matt Kapko, "Crypto Analysts Stunned by Lazarus Group's Capabilities in $1.46B Bybit Theft," Cyberscoop, February 25, 2025, https://cyberscoop.com/bybit-lazarus-group-north-korea-ethereum/.

72. *Annual Threat Assessment of the U.S. Intelligence Community.*

73. Will Ripley, "North Korean Defector: 'Bureau 121' Hackers Operating in China," CNN, January 7, 2015, https://www.cnn.com/2015/01/06/asia/north-korea-hackers-shenyang/index.html.

74. Daniel Russel, "North Korea's Next Weapon of Choice: Cyber," The Asia Society, April 30, 2019, https://asiasociety.org/magazine/article/north-koreas-next-weapon-choice-cyber; Tom Hegel and Dakota Cary, "DPRK IT Workers: A Network of Active Front Companies and Their Links to China," SentinelLabs, November 21, 2024, https://www.sentinelone.com/labs/dprk-it-workers-a-network-of-active-front-companies-and-their-links-to-china/.

75. Russel, "North Korea's Next Weapon of Choice: Cyber."

76. Council on Foreign Relations Cyber Operations Tracker Database.

77. Anne Davies, "Australia Joins US and UK in Blaming Russian-Backed Hackers for Cyber-Attacks," *The Guardian*, April 17, 2018, https://www.theguardian.com/technology/2018/apr/17/australia-joins-us-and-uk-in-blaming-russia-for-cyber-attacks.

78. *North Korean Tactics, Techniques, and Procedures for Revenue Generation.*

79. Ellen Nakashima, "Russian Spies Hacked the Olympics and Tried to Make It Look Like North Korea Did It, U.S. Officials Say," *The Washington Post*, February 24, 2018, https://www.washingtonpost.com/world/national-security/russian-spies-hacked-the-olympics-and-tried-to-make-it-look-like-north-korea-did-it-us-officials-say/2018/02/24/44b5468e-18f2-11e8-92c9-376b4fe57ff7_story.html.

80. Tom Burt, "New Cyberattacks Targeting Sporting and Anti-Doping Organizations," Microsoft, October 28, 2019, https://blogs.microsoft.com/on-the-issues/2019/10/28/cyberattacks-sporting-anti-doping/.

81. *APT28: A Window Into Russia's Cyber Espionage Operations?* (FireEye, 2014), https://services.google.com/fh/files/misc/apt28-window-russia-cyber-espionage-operations.pdf.

82. Andy Greenberg, "Sandworm Hackers Caused Another Blackout in Ukraine—During a Missile Strike," *Wired*, November 9, 2023, https://www.wired.com/story/sandworm-ukraine-third-blackout-cyberattack/.

83. Vivek Gullapalli, "Why Is the Asia Pacific Region a Target for Cybercrime—and What Can Be Done about It?," World Economic Forum, June 12, 2023, https://www.weforum.org/agenda/2023/06/asia-pacific-region-the-new-ground-zero-cybercrime/.

84. Sune Engel Rasmussen and Daniel Michaels, "America's Rivals

Have a New Favorite Weapon: Criminal Gangs," *The Wall Street Journal*, November 22, 2024, https://www.wsj.com/world/americas-rivals-have-a-new-favorite-weapon-criminal-gangs-3c12a35f.

85. "Cyber Attack Compromised Indonesia Data Centre, Ransom Sought," Reuters, June 24 2024, https://www.reuters.com/technology/cybersecurity/cyber-attack-compromised-indonesia-data-centre-ransom-sought-reports-antara-2024-06-24/.

86. "Cyber Attack Compromised Indonesia Data Centre, Ransom Sought."

87. *Microsoft Digital Defense Report 2023.*

88. Kurt Baker, "Ransomware as a Service (RAAS) Explained How It Works & Examples," CrowdStrike, January 30, 2023, https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/.

89. Todd Moore, "Protect Your Organization from Cybercrime-as-a-Service Attacks," Thales Blog, October 12, 2023, https://cpl.thalesgroup.com/blog/encryption/cybercrime-as-a-service-caas-explaned.

90. "Billion-Dollar Cyberfraud Industry Expands in Southeast Asia as Criminals Adopt New Technologies," United Nations Office on Drugs and Crime Regional Office for Southeast Asia and the Pacific, October 7, 2024, https://www.unodc.org/roseap/en/2024/10/cyberfraud-industry-expands-southeast-asia/story.html.

91. Jonathan Head, Lulo Luo, and Thanyarat Doksone, "'I Need Help': Freed from Myanmar's Scam Centres, Thousands Are Now Stranded," BBC, February 26, 2025, https://www.bbc.com/news/articles/c5yr7j18edjo.

92. Rui Serra, "The Surge in Native Language Phishing Emails," Anubisnetworks, April 15, 2021, https://www.anubisnetworks.com/blog/surge_in_native_language_emails.

93. "Hacktivists," Cyber.UK, https://cyber.uk/areas-of-cyber-security/cyber-security-threat-groups-2/hacktivists/.

94. Mihir Bagwe, "Malaysian Hacktivists Target Indian Websites as Payback," Bank Info Security, June 13, 2022, https://www.bankinfosecurity.asia/malaysian-hacktivists-target-indian-websites-as-payback-a-19325.

95. "South Korea Says Pro-Russia Groups Responsible for Cyberattacks After North's Troop Dispatch," Reuters, November 8, 2024, https://www.reuters.com/world/south-korea-says-pro-russia-groups-responsible-cyberattacks-after-norths-troop-2024-11-08/.

96. C. Todd Lopez, "In Cyber, Differentiating Between State Actors, Criminals Is a Blur," U.S. Department of Defense News, May 14, 2021, https://www.defense.gov/News/News-Stories/Article/Article/2618386/in-cyber-differentiating-between-state-actors-criminals-is-a-blur/.

97. "Countering Disinformation," United Nations, https://www.un.org/en/countering-disinformation.

98. Gabriel R. Sanchez and Keesha Middlemass, "Misinformation Is Eroding the Public's Confidence in Democracy," Brookings Institution, July 26, 2022, https://www.brookings.edu/articles/misinformation-is-eroding-the-publics-confidence-in-democracy/.

99. *How the People's Republic of China Seeks to Reshape the Global Information Environment* (U.S. Department of State Global Engagement Center, September 28, 2023), https://www.state.gov/wp-content/uploads/2023/09/HOW-THE-PEOPLES-REPUBLIC-OF-CHINA-SEEKS-TO-RESHAPE-THE-GLOBAL-INFORMATION-ENVIRONMENT_Final.pdf; Steven Lee Myers and Paul Mozur, "China Is Waging a Disinformation War Against Hong Kong Protesters," *The New York Times*, August 13, 2019, https://www.nytimes.com/2019/08/13/world/asia/hong-kong-protests-china.html.

100. Sue Ahearn, "How China Is Winning the Information War in the Pacific," The Strategist, March 17, 2022, https://www.aspistrategist.org.au/how-china-is-winning-the-information-war-in-the-pacific/.

101. Guy Rosen, "Raising Online Defenses Through Transparency and Collaboration," Meta, August 29, 2023, https://about.fb.com/news/2023/08/raising-online-defenses/.

102. Matthew Brockett, "New Zealand Accuses China, Russia, and Iran of Attempting Foreign Interference," *Time,* August 11, 2023, https://time.com/6303977/new-zealand-foreign-interference-report-china/.

103. *How the People's Republic of China Seeks to Reshape the Global Information Environment.*

104. *Annual Threat Assessment of the U.S. Intelligence Community.*

105. Office of the Director of National Intelligence, "ODNI Statement on Declassified Intelligence Community Assessment of Russian Activities and Intentions in Recent U.S. Elections," press release, archived February 17, 2024, https://web.archive.org/web/20250213213346/https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2017/3035-odni-statement-on-declassified-intelligence-community-assessment-of-russian-activities-and-intentions-in-recent-u-s-elections#conten.

106. Olga Lautman, "We're Winning, Say Russia's Fake News Manufacturers," Center for European Policy Analysis, October 16, 2024, https://cepa.org/article/were-winning-say-russias-fake-news-manufacturers/.

107. Lautman, "We're Winning, Say Russia's Fake News Manufacturers."

108. Andrew Greene, "Intelligence Officials Identify Russian Efforts to Interfere in Australian Politics," ABC Australia, February 10, 2022, https://www.abc.net.au/news/2022-02-10/russia-foreign-interference-australian-election/100819910.

109. Grace B. Mueller, et al., *Cyber Operations During the Russo-Ukrainian War* (Center for Strategic and International Studies, July 2023), https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-07/230713_Mueller_CyberOps_RussiaUkraine.pdf?VersionId=tlzslXBig6NG2QKBsqTlOlf0wENNeo87.

110. *How the Economy, Skills Gap and Artificial Intelligence are Challenging the Global Cybersecurity Workforce* (ISC2, October 31, 2023), https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf?rev=28b46de71ce24e6ab-

7705f6e3da8637e.

111. "Gap of 2.6 Million Cybersecurity Professionals Looms," Asia Pacific Security Magazine, November 7, 2023, https://www.asiapacificsecuritymagazine.com/gap-of-2-6-million-cybersecurity-professionals-looms/.

112. Interviews at CNAS-JIIA private workshop on April 19, 2024, and CNAS-Stratbase ADR Institute private workshop in Manila on June 24, 2024. All interviews were conducted in confidentiality, and the names of interviewees are withheld by mutual agreement.

113. Interviews at the CNAS-Prospect Foundation private workshop in Taipei on April 16, 2024, the CNAS-JIIA private workshop in Tokyo on April 19, 2024, the CNAS-Stratbase ADR Institute private workshop in Manila on June 24, 2024, and the CNAS-Asan Institute for Policy Studies private workshop in Seoul on June 27, 2024. All interviews were conducted in confidentiality, and the names of interviewees are withheld by mutual agreement.

114. Interviews at the CNAS-Prospect Foundation private workshop in Taipei on April 16, 2024, the CNAS-JIIA private workshop in Tokyo on April 19, 2024, the CNAS-Stratbase ADR Institute private workshop in Manila on June 24, 2024, and the CNAS-Asan Institute for Policy Studies private workshop in Seoul on June 27, 2024. All interviews were conducted in confidentiality, and the names of interviewees are withheld by mutual agreement.

115. Julia Voo, "Contested Connectivity: Cyber Threats in the Asia-Pacific," Institute for International Strategic Studies, May 15, 2024, https://www.iiss.org/en/online-analysis/online-analysis/2024/05/contested-connectivity-cyber-threats-in-the-asia-pacific/.

116. CSA Singapore, "ASEAN-Singapore Cybersecurity Centre of Excellence," press release, October 6, 2021, https://www.csa.gov.sg/news-events/press-releases/asean-singapore-cybersecurity-centre-of-excellence.

117. *ASEAN Cybersecurity Cooperation Strategy 2021–2025* (Association for Southeast Asian Nations, February 1, 2022), https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf; CSA Singapore, "Singapore Moves Ahead to Establish the ASEAN Regional CERT to Strengthen Regional Cybersecurity," press release, February 2, 2024, https://www.csa.gov.sg/News-Events/Press-Releases/2024/singapore-moves-ahead-to-establish-the-asean-regional-cert-to-strengthen-regional-cybersecurity.

118. "Cyber Affairs and Critical Technology: Capacity Building," Australian Department of Foreign Affairs and Trade, https://www.dfat.gov.au/international-relations/themes/cyber-affairs-and-critical-technologyinternational-cyber-and-critical-technology-capacity-building; CSA Singapore, "Singapore Moves Ahead to Establish the ASEAN Regional CERT to Strengthen Regional Cybersecurity"; and U.S. Department of Homeland Security, "DHS Bolsters Indo-Pacific Maritime Cybersecurity Through Partnership with Indonesia," press release, June 18, 2024, https://www.dhs.gov/news/2024/06/18/dhs-bolsters-indo-pacific-maritime-cybersecurity-through-partnership-indonesia.

119. Interviews at the CNAS-Prospect Foundation private workshop in Taipei on April 16, 2024, the CNAS-JIIA private workshop in Tokyo on April 19, 2024, the CNAS-Stratbase ADR Institute private workshop in Manila on June 24, 2024, and the CNAS-Asan Institute for Policy Studies private workshop in Seoul on June 27, 2024. All interviews were conducted in confidentiality, and the names of interviewees are withheld by mutual agreement.

120. "U.S. Security Cooperation with Japan," Bureau of Political-Military Affairs, U.S. Department of State, January 20, 2025, https://www.state.gov/u-s-security-cooperation-with-japan/.

121. "U.S. Relations with Japan," U.S. Department of State, January 21, 2020, archived March 19, 2025, https://web.archive.org/web/20250319091430/https://www.state.gov/u-s-relations-with-japan/.

122. *Cyber Capabilities and National Power: A Net Assessment* (The International Institute for Strategic Studies, June 28, 2021), https://www.iiss.org/research-paper/2021/06/cyber-capabilities-national-power/.

123. *Cyber Capabilities and National Power: A Net Assessment.*

124. Jun Osawa, "How Japan Is Modernizing Its Cybersecurity Policy," Stimson Center, February 2, 2023, https://www.stimson.org/2023/japan-cybersecurity-policy/; NSBT Japan, "Japan's 'Active Cyber Defense' System: Now Set to Become Reality?," Asian Military Review, October 8, 2024, https://www.asianmilitaryreview.com/2024/10/japans-active-cyber-defense-system-now-set-to-become-reality/.

125. Ellen Nakashima, "China Hacked Japan's Sensitive Defense Networks, Officials Say." *The Washington Post,* August 8, 2023, https://www.washingtonpost.com/national-security/2023/08/07/china-japan-hack-pentagon/.

126. *National Security Strategy of Japan.*

127. Nakashima, "China Hacked Japan's Sensitive Defense Networks, Officials Say."

128. Greg Rattray and Seungmin (Helen) Lee, *US-Japan Cyber Cooperation: Meeting Challenges and Operationalizing Opportunities* (Weatherhead East Asian Institute, Columbia University, December 2023), https://weai.columbia.edu/sites/default/files/content/pics/JRP/Rattray_Lee_US_Japan_CyberCoop.pdf.

129. "70 Percent of Japanese Respondents Face Skills Shortages Within Security Teams," ISC2, May 19, 2023, https://www.isc2.org/Insights/2023/05/70-percent-of-Japanese-Respondents-Face-Skills-Shortages-within-Security-Teams.

130. Kaori Kaneko, Tim Kelly, and John Geddie, "The Glitch in Japan's Plans to Bolster U.S. Defence," Reuters, April 26, 2024, https://www.reuters.com/world/glitch-japans-plans-bolster-us-defence-2024-04-26/.

131. *JPCERT/CC Incident Handling Report April 1, 2024–June 30, 2024* (Japan Computer Emergency Response Team Coordination Center, December 6, 2024), https://www.jpcert.or.jp/english/doc/IR_Report2024Q1_en.pdf; *JPCERT/CC Incident Handling Report, January 1, 2024–March 31, 2024* (Japan Computer Emergency Response Team Coordination Center, June 6, 2024), https://www.jpcert.or.jp/english/doc/IR_Report2023Q4_en.pdf; *JPCERT/CC Incident Handling Report July 1, 2024– September 30, 2024* (Japan Computer Emergency Response Team Coordination Center, December 6, 2024), https://www.jpcert.or.jp/english/

doc/IR_Report2024Q2_en.pdf; and *JPCERT/CC Incident Handling Report October 1, 2023–December 31, 2023* (Japan Computer Emergency Response Team Coordination Center, March 27, 2024), https://www.jpcert.or.jp/english/doc/IR_Report2023Q3_en.pdf.

132. Interviews at the CNAS-JIIA private workshop in Tokyo on April 19, 2024. All interviews were conducted in confidentiality, and the names of interviewees are withheld by mutual agreement.

133. "Classified Japanese Diplomatic Info Leaked After Chinese Cyberattacks," Kyodo News, February 5, 2024, https://english.kyodonews.net/news/2024/02/33b5e4b96c1f-urgent-classified-japanese-diplomatic-info-leaked-after-chinese-cyberattacks.html; "U.S. Warned Japan of China's Hacking of Official Diplomatic Telegram System; Reinforcing Cybersecurity Key Concern," *The Japan News by the Yomiuri Shimbun*, February 5, 2024, https://japannews.yomiuri.co.jp/politics/defense-security/20240205-166966/.

134. Alexander Martin, "Japan's Cybersecurity Agency Breached by Suspected Chinese Hackers: Report," The Record, August 29, 2023, https://therecord.media/japan-cybersecurity-agency-breached-report.

135. Shimpachi Yoshida, "Ransomware Attacks Surge More Than 50% in Japan in 2022," *The Asahi Shimbun*, February 6, 2023, https://www.asahi.com/ajw/articles/14832967.

136. Daryna Antoniuk, "Japan's Ruling Political Party Hit by Cyberattack from Alleged Pro-Russian Hackers," The Record, October 17, 2024, https://therecord.media/japan-political-party-hit-by-cyberattack-pro-russian-hackers

137. Alicia Hope, "Cyber Attack by Russian Hackers Disrupted 20 Japanese Government Websites," CPO Magazine, September 15, 2022, https://www.cpomagazine.com/cyber-security/cyber-attack-by-russian-hackers-disrupted-20-japanese-government-websites/.

138. Alessandro Mascellino, "Japan Government Websites Hit by Cyber-Attacks, Killnet Suspected," *Infosecurity Magazine*, September 7, 2022, https://www.infosecurity-magazine.com/news/japan-govt-websites-killnet/.

139. *Calibrating Expansion: 2023 Annual Cybersecurity Report* (Trend Micro, March 6, 2024), https://documents.trendmicro.com/images/TEx/articles/Calibrating-Expansion_2023-Annual-Cybersecurity-Report.pdf.

140. Akinobu Iwasawa and Rei Kobayashi, "North Korean Crypto Thefts Target Japan, Vietnam, Hong Kong," *Nikkei Asia,* May 15, 2023, https://asia.nikkei.com/Spotlight/Cryptocurrencies/North-Korean-crypto-thefts-target-Japan-Vietnam-Hong-Kong.

141. Reuters, "Cyberattack on Toyota's Supply Chain Shuts Its 14 Factories in Japan for 24 Hours," CNN, March 1, 2022, https://www.cnn.com/2022/03/01/business/toyota-japan-cyberattack-production-restarts-intl-hnk/index.html; Takahiko Hyuga, Min Jeong Lee, and Jamie Tarabay, "Cybersecurity Nightmare in Japan Is Everyone Else's Problem, Too," *The Japan Times,* April 25, 2023, https://www.japantimes.co.jp/news/2023/04/25/business/japan-cybersecurity-problem/.

142. Ayami Ko, et al., "Nagoya Port Cyberattack May Become Security Wake-Up Call," *The Asahi Shimbun*, July 12, 2023, https://www.asahi.com/ajw/articles/14954966.

143. Leo Lewis, "Japan's Cyber Security Agency Suffers Months-Long Breach," *Financial Times,* August 28, 2023, https://www.ft.com/content/de0042f8-a7ce-4db5-bf7b-aed8ad3a4cfd.

144. "Classified Japanese Diplomatic Info Leaked After Chinese Cyberattacks"; "U.S. Warned Japan of China's Hacking of Official Diplomatic Telegram System; Reinforcing Cybersecurity Key Concern"; Martin, "Japan's Cybersecurity Agency Breached by Suspected Chinese Hackers: Report"; Reuters, "Cyberattack on Toyota's Supply Chain Shuts Its 14 Factories in Japan for 24 Hours"; Hyuga, Lee, and Tarabay, "Cybersecurity Nightmare in Japan Is Everyone Else's Problem, Too"; Ko, et al., "Nagoya Port Cyberattack May Become Security Wake-Up Call"; and Nakashima, "China Hacked Japan's Sensitive Defense Networks, Officials Say."

145. "About NISC," National Center of Incident Readiness and Strategy for Cybersecurity, https://www.nisc.go.jp/eng/index.html#sec1.

146. "Cybersecurity," Japan Ministry of Economy, Trade and Industry, https://www.meti.go.jp/english/policy/safety_security/cybersecurity/index.html.

147. "Japan National Police Agency Establish New Bureau to Combat Serious Cybercrimes," Japan Anti Fraud Organization, https://japanantifraud.org/japan-national-police-agency-establish-new-bureau-to-combat-serious-cybercrimes/.

148. "Cybersecurity," Ministry of Foreign Affairs of Japan, October 8, 2024, https://www.mofa.go.jp/policy/page18e_000015.html.

149. "About NISC"; "Government Offices' Functions and Website Contents," National Public Safety Commission, https://japan.kantei.go.jp/link/link1.html; "Organizational Structure and Authority," National Police Agency, https://www.npa.go.jp/english/National_Police_Agency.html.

150. Nawa Toshio, "Threat Landscape: Corporate Japan Its Own Worse Enemy in the Ransomware War," Nippon.com, November 20, 2024, https://www.nippon.com/en/in-depth/d01035/; Akinobu Iwasawa, "Cyberattacks on Japan Soar as Hackers Target Vulnerabilities," *Nikkei Asia*, January 28, 2023, https://asia.nikkei.com/Spotlight/Datawatch/Cyberattacks-on-Japan-soar-as-hackers-target-vulnerabilities; and Walter Sim, "Hit by Wave of Online Attacks, Japan Shifts to 'Active Cyber Defence,'" *The Straits Times*, January 20, 2025, https://www.straitstimes.com/asia/east-asia/hit-by-wave-of-cyber-attacks-japan-shifts-to-active-cyber-defence.

151. Sophie Rice, "NTT and Palo Alto Enhance 5G Network Security," Cyber Magazine, February 28, 2025, https://cybermagazine.com/network-security/how-ntt-and-palo-alto-are-protecting-iot-ot-infrastructure; "NTT Security Rating," Security Scorecard, https://scores.securityscorecard.io/security-rating/security.ntt; and Leo Lewis, "Japan's 'Myth of Security' Raises Cyberattack Risk," *Financial Times,* May 5, 2023, https://www.ft.com/content/bd990583-2948-4769-b090-eac644a2ad69.

152. Kelsey Ables, "Japan Won Its 'War' on Floppy Disks, But Its Love of Archaic Tech Lingers," *The Washington Post,* July 5, 2024, https://www.washingtonpost.com/world/2024/07/05/japan-floppy-disks/.

153. Christopher B. Johnstone, "Japan's Transformational National Security Strategy," Center for Strategic and International Studies, December 8, 2022, https://www.csis.org/analysis/japans-transformational-national-security-strategy.

154. Alessandro Mascellino, "Japan Faces Prolonged Cyber-Attacks Linked to China's MirrorFace," Infosecurity Magazine, January 9, 2025, https://www.infosecurity-magazine.com/news/japan-faces-cyberattacks-china/.

155. *Cybersecurity Strategy: Towards a World-Leading, Resilient and Vigorous Cyberspace* (Information Security Policy Council, June 10, 2013), https://nsarchive.gwu.edu/document/19020-national-security-archive-japanese-government.

156. "Commitment to a Free, Fair and Secure Cyberspace," National Center for Incident Readiness and Strategy for Cybersecurity, https://www.nisc.go.jp/eng/index.html.

157. *Cyber Capabilities and National Power: A Net Assessment.*

158. *Cyber Capabilities and National Power: A Net Assessment.*

159. *National Security Strategy of Japan.*

160. *National Security Strategy of Japan.*

161. Jacob Stokes, et al., *Strengthening the Shield: Japan's Defense Transformation and the U.S.-Japan Alliance* (Center for a New American Security, September 2023), https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/CNAS-Report_Strengthening-the-Shield_091223_final-web.pdf.

162. Osawa, "How Japan Is Modernizing Its Cybersecurity Policy."

163. *Cyber Capabilities and National Power: A Net Assessment.*

164. *Cyber Capabilities and National Power: A Net Assessment.*

165. *Cyber Capabilities and National Power: A Net Assessment.*

166. *Act on the Protection and Utilization of Important Economic and Security Information,* Government of Japan, https://www.cao.go.jp/keizai_anzen_hosho/hogokatsuyou/hogokatsuyou.html.

167. Gabriele Ninivaggi and Himari Semans, "Japan's Cabinet Approves Legislation on 'Active' Cybersecurity," *The Japan Times*, February 7, 2025, https://www.japantimes.co.jp/news/2025/02/07/japan/politics/active-cyber-defense-bill/; *Act on the Prevention of Damage from Unauthorized Acts Against Important Electronic Computers*, Cabinet Bill No. 4, 217th Diet (2025), https://www.sangiin.go.jp/japanese/joho1/kousei/gian/217/meisai/m217080217004.htm; *Law to Amend Related Laws in Conjunction with the Enforcement of the Act on the Prevention of Damage from Unauthorized Acts Against Important Electronic Computers*, Cabinet Bill No. 5, 217th Diet (2025), https://www.sangiin.go.jp/japanese/joho1/kousei/gian/217/meisai/m217080217005.htm.

168. "70 Percent of Japanese Respondents Face Skills Shortages Within Security Teams."

169. *How the Economy, Skills Gap and Artificial Intelligence are Challenging the Global Cybersecurity Workforce.*

170. *Mapping the Future of US-Japan Cybersecurity Cooperation: Workforce Challenges and Opportunities* (US-Japan NEXT Alliance Initiative, July 2024) https://spfusa.org/wp-content/uploads/2024/07/Mapping-the-Future-of-US-Japan-Cybersecurity-Cooperation-Workforce-Challenges-and-Opportunities.pdf.

171. *Mapping the Future of US-Japan Cybersecurity Cooperation: Workforce Challenges and Opportunities.*

172. "Nurturing Talents and Professionals for the Digital Age," Information-Technology Promotion Agency, https://www.ipa.go.jp/en/it-talents/skill-standard/skill-framework-documents.html.

173. Phil Muncaster, "Japan Set to Develop Elite White Hat Agency," Infosecurity Magazine, May 20, 2016, https://www.infosecurity-magazine.com/news/japan-set-to-develop-elite-white/.

174. *Cyber Capabilities and National Power: A Net Assessment.*

175. *Cyber Capabilities and National Power: A Net Assessment.*

176. *Cyber Capabilities and National Power: A Net Assessment.*

177. Shinnosuke Nagatomi, "Japan Aims to Boost Self-Defense Force Cyber Personnel to 4,000," *Nikkei Asia*, July 3, 2024, https://asia.nikkei.com/Spotlight/Cybersecurity/Japan-aims-to-boost-Self-Defense-Force-cyber-personnel-to-4-000.

178. Kaneko, Kelly, and Geddie, "The Glitch in Japan's Plans to Bolster U.S. Defence."

179. Nagatomi, "Japan Aims to Boost Self-Defense Force Cyber Personnel to 4,000."

180. "Japan Ready to Improve Working Conditions for SDF Members," *The Japan Times,* December 21, 2024, https://www.japantimes.co.jp/news/2024/12/21/japan/politics/sdf-improve-working-conditions/.

181. Nagatomi, "Japan Aims to Boost Self-Defense Force Cyber Personnel to 4,000."

182. Ken Kotani, "Japan's Five Eyes Chance and Challenge," East Asia Forum, August 26, 2021, https://eastasiaforum.org/2021/08/26/japans-five-eyes-chance-and-challenge/; *Cyber Capabilities and National Power: A Net Assessment.*

183. Ryan Gallagher, "The Untold Story of Japan's Secret Spy Agency," The Intercept, May 19, 2018, https://theintercept.com/2018/05/19/japan-dfs-surveillance-agency/.

184. *Progress and Budget in Fundamental Reinforcement of Defense Capabilities: Overview of the FY2024 Budget* (Japanese Ministry of Defense, June 7, 2024), https://www.mod.go.jp/en/d_act/d_budget/pdf/20240607a.pdf.

185. *Cyber Capabilities and National Power: A Net Assessment.*

186. *Cyber Capabilities and National Power: A Net Assessment.*

187. *Cyber Capabilities and National Power: A Net Assessment.*

188. *Cyber Capabilities and National Power: A Net Assessment.*

189. Reiko Miki, "Japan, U.S., Philippines to Form Joint Cyberde-

fense Network," *Nikkei Asia,* April 3, 2024, https://asia.nikkei.com/Politics/Defense/Japan-U.S.-Philippines-to-form-joint-cyberdefense-network.

190. The White House, "FACT SHEET: Quad Leaders' Tokyo Summit 2022," press release, May 23, 2022, https://biden-whitehouse.archives.gov/briefing-room/statements-releases/2022/05/23/fact-sheet-quad-leaders-tokyo-summit-2022/; U.S. Department of State, "Joint Statement from the Quad Foreign Ministers' Meeting in Tokyo," press release, July 29, 2024, https://2021-2025.state.gov/joint-statement-from-the-quad-foreign-ministers-meeting-in-tokyo/.

191. Hyuga, Lee, and Tarabay, "Cybersecurity Nightmare in Japan Is Everyone Else's Problem, Too."

192. *Basic Position of the Government of Japan on International Law Applicable to Cyber Operations* (Ministry of Foreign Affairs of Japan, May 28, 2021), https://www.mofa.go.jp/files/100200935.pdf; "Statement by Mr. AKAHORI Takeshi, Ambassador for Cyber Policy of the Ministry of Foreign Affairs of Japan, on the Occasion of the Virtual Informal Meeting of the OEWG on ICTs," Permanent Mission of Japan to the United Nations, September 29, 2020, https://www.un.emb-japan.go.jp/itpr_en/akahori092920.html.

193. U.S. Department of Defense, "Joint Statement of the Security Consultative Committee ("2+2")," press release, July 28, 2024, https://www.defense.gov/News/Releases/Release/Article/3852169/joint-statement-of-the-security-consultative-committee-22/.

194. "Joint Statement 2024 from US-Japan Digital Economy Private Working Group U.S.-Japan Dialogue on Digital Economy," Keidanren Japan Business Federation, February 6, 2022, https://www.keidanren.or.jp/en/policy/2024/016.html.

195. "Joint Statement of the U.S.-Japan Cyber Defense Policy Working Group," Ministry of Defense, Government of Japan, May 30, 2015, https://nsarchive.gwu.edu/document/21938-document-07.

196. Elizabeth Beattie, "Google Opens Asia-Pacific Cybersecurity Research Center in Tokyo," *The Japan Times*, March 7, 2024, https://www.japantimes.co.jp/business/2024/03/07/tech/google-japan-cybersecurity-center/.

197. "Microsoft to Invest US$2.9 Billion in AI and Cloud Infrastructure in Japan While Boosting the Nation's Skills, Research, and Cybersecurity," Microsoft, April 10, 2024, https://news.microsoft.com/apac/2024/04/10/microsoft-to-invest-us2-9-billion-in-ai-and-cloud-infrastructure-in-japan-while-boosting-the-nations-skills-research-and-cybersecurity/.

198. Marcus Law, "Microsoft, AWS & Oracle: Why Big Tech Is Investing in Japan," *Technology Magazine*, April 22, 2024, https://technologymagazine.com/articles/microsoft-aws-oracle-why-big-tech-is-investing-in-japan.

199. Osawa, "How Japan Is Modernizing Its Cybersecurity Policy."

200. *Act on the Prevention of Damage from Unauthorized Acts Against Important Electronic Computers*; *Law to Amend Related Laws in Conjunction with the Enforcement of the Act on the Prevention of Damage from Unauthorized Acts Against Important Electronic Computers*.

201. *Cyber Capabilities and National Power: A Net Assessment.*

202. Interviews at CNAS-JIIA private workshop on April 19, 2024. All interviews were conducted in confidentiality, and the names of interviewees are withheld by mutual agreement.

203. "Development Cooperation Profiles," OECD, June 17, 2024, https://www.oecd.org/en/publications/2023/06/development-co-operation-profiles_17afa013/full-report/official-development-assistance-trends-in-times-of-crisis_97509fe9.html#chapter-d1e19-b5cd116b47.

204. "Japan's Security Policy, Official Security Assistance (OSA)," Ministry of Foreign Affairs of Japan, https://www.mofa.go.jp/fp/ipc/page4e_001366.html?utm.

205. "U.S. Relations with the Republic of Korea," U.S. Department of State, February 8, 2020, archived April 1, 2025, https://web.archive.org/web/20250401005143/https://www.state.gov/u-s-relations-with-the-republic-of-korea/.

206. "South Korea Traces Cyber-Attacks to Chinese IP Address," *The Guardian*, March 21, 2013, https://www.theguardian.com/world/2013/mar/21/south-korea-cyber-attack-chinese.

207. *How the Economy, Skills Gap and Artificial Intelligence are Challenging the Global Cybersecurity Workforce*.

208. Yang Min-cheol, "National Intelligence Service: "80% of Public Sector Hacking Originates from North Korea... Kim Jong-un Commands," KBS, January 24, 2024, https://news.kbs.co.kr/news/pc/view/view.do?ncd=7874396.

209. Kim Arin, "Seoul's Spy Agency Accuses China of Major Cyber Attacks," *The Korea Herald*, January 24, 2024, https://www.koreaherald.com/article/3312349.

210. *2024*년 상반기 사이버 위협 동향 보고서 *[2024 First Half Cyber Threat Trends Report]* (과학기술정보통신부 [Ministry of Science and ICT], 한국인터넷진흥원 [Korea Internet & Security Agency], September 6, 2024), 4, https://www.kisa.or.kr/20205/form?postSeq=1026&page=1#fndoDocumentPreview.

211. *2024*년 상반기 사이버 위협 동향 보고서 *[2024 First Half Cyber Threat Trends Report],* 6.

212. *2024*년 상반기 사이버 위협 동향 보고서 *[2024 First Half Cyber Threat Trends Report], 6.*

213. *2024*년 상반기 사이버 위협 동향 보고서 *[2024 First Half Cyber Threat Trends Report],* 6.

214. Interviews at CNAS-Asan Institute for Policy Studies private workshop on June 27, 2024. All interviews were conducted in confidentiality, and the names of interviewees are withheld by mutual agreement.

215. *Attackers Without Borders: The South Korean View of Global Malicious Traffic* (Greynoise, October 13, 2023), https://www.greynoise.io/resources/attackers-without-borders-the-south-korean-view-of-global-malicious-traffic.

216. *2024* 국가정보보호백서 *[2024 National Cybersecurity White Paper]* ([국가정보원[National Intelligence Service] 과학기술정보통신부[Ministry of Science and ICT] 행정안전부 [Ministry of the Interior and Safety 개인정보보호위원회[Personal Information Protection Commission] 금융위원회[Financial

Services Commission] and 외교부[Ministry of Foreign Affairs], August 2024), 9, https://www.nis.go.kr/resources/synap/skin/doc.html?fn=NIS_FILE_1714698643350 .

217. The 2024 National Cybersecurity White Paper states, "우리나라에서는 2023년 1월부터 9월까지 외교부 대상 공격 8천여 건 등 외교 관련 정보 절취목적의 사이버공격이 1만 7천여 건에 이르렀다 [In South Korea, from January to September 2023, there were approximately 17,000 cyberattacks aimed at stealing diplomatic information, including around 8,000 attacks targeting the Ministry of Foreign Affairs]." See *2024* 국가정보보호백서 *[2024 National Cybersecurity White Paper]*, 1.

218. *Republic of Korea National Cybersecurity Strategy*; "Taking Joint Action with the Republic of Korea to Combat the Democratic People's Republic of Korea's Illicit Revenue Generation," U.S. Department of State, May 23, 2023, https://2021-2025.state.gov/taking-joint-action-with-the-republic-of-korea-to-combat-the-democratic-peoples-republic-of-koreas-illicit-revenue-generation/.

219. "국정원 '공공분야 해킹 80%가 北 소행…선거 개입 공작 가능' [National Intelligence Service: '80% of Public Sector Hacking Is North Korea's Work. . . Possibility of Election Interference']," YTN, January 24, 2024, https://www.youtube.com/watch?v=FuwFauBTVjM.

220. Russel, "North Korea's Next Weapon of Choice: Cyber"; "'라자루스', '안다리엘', '김수키'…북 해킹 공격에 방산업체 10여 곳 피해 [Lazarus, Andariel, Kimsuky… Over 10 Defense Contractors Affected by North Korean Hacking Attacks]," KBS News, April 22, 2024, https://www.youtube.com/watch?v=rfnlQrazaoQ.

221. Dominik Breitenbacher and Kaspars Osis, *Operational In-(ter)ception: Targeted Attacks Against European Aerospace and Military Companies* (ESET, June 2020), https://web-assets.eseteststatic.com/wls/2020/06/ESET_Operation_Interception.pdf; Divyanshu Rai, "Lazarus Hackers Are Weaponizing Open-Source Software," LinkedIn, September 30, 2022, https://www.linkedin.com/pulse/lazarus-hackers-weaponizing-open-source-software-divyanshu-rai/.

222. Choi Hye-rim, "'라자루스'·'안다리엘'·'김수키'…북 해킹 조직 방산업체 무차별 침투 [Lazarus, Andariel, Kimsuki . . . North Korean Hacking Organizations Indiscriminately Infiltrate Defense Industries]," KBS News, April 24, 2024, https://news.kbs.co.kr/news/pc/view/view.do?ncd=7947357.

223. "North Korean Hacking Organization Launches Full-Scale Attack on Domestic Defense Companies [Defense Media Agency]" KFN News, April 23, 2024, https://www.youtube.com/watch?v=QZkQ7ahucJU.

224. Duyeon Kim, *Republic of Korea Cybersecurity Brief*, unpublished manuscript (June 19, 2024), 11; *2023*년 하반기 사이버 위협 동향 보고서*[Cyber Threat Trend Report Second Half of 2023*, (과학기술정보통신부 [Ministry of Science and ICT], 한국인터넷진흥원 [Korea Internet & Security Agency], January 18, 2024), 16, https://www.kisa.or.kr/20205/form?postSeq=1025&page=1.

225. Yang Min-Cheol, "North Korea's Lazarus Disguised as Chinese Virtual Asset Investors to Conduct Phishing Attacks," KBS News, April 30, 2024, https://news.kbs.co.kr/news/pc/view/view.do?ncd=7952307.

226. Kim Arin, "North Korea Trying to Work Generative AI into Hacking Operations," *The Korea Herald*, January 24, 2024, https://www.koreaherald.com/article/3312349.

227. Arin, "North Korea Trying to Work Generative AI into Hacking Operations."

228. *Multi-Year Chinese APT Campaign Targets South Korean Academic, Government, and Political Entities* (Recorded Future by Insikt Group, September 19, 2023), https://go.recordedfuture.com/hubfs/reports/cta-2023-0919.pdf.

229. *2024* 국가정보보호백서 *[2024 National Cybersecurity White Paper]* 17.

230. *2024* 국가정보보호백서 *[2024 National Cybersecurity White Paper]* 17.

231. *2024* 국가정보보호백서 *[2024 National Cybersecurity White Paper]* 17.

232. Hoshik Nam and Alejandro Sanchez, "South Korea's Growing Role as a Major Arms Exporter: Future Prospects in Latin America," War on the Rocks, August 21, 2024, https://warontherocks.com/2024/08/south-koreas-growing-role-as-a-major-arms-exporter-future-prospects-in-latin-america/; "*2024* 국가정보보호백서 *[2024 National Cybersecurity White Paper]*, 9.

233. "South Korea's KF-21 Boramae Twin-Seater Fighter Jet Steps Closer to Deployment Following Latest Test Flight," Army Recognition Group, February 20, 2025, https://armyrecognition.com/news/aerospace-news/2025/south-koreas-kf-21-boramae-twin-seater-fighter-jet-steps-closer-to-deployment-following-latest-test-flight.

234. Nam and Sanchez, "South Korea's Growing Role as a Major Arms Exporter: Future Prospects in Latin America"; "*2024* 국가정보보호백서 *[2024 National Cybersecurity White Paper]*, 9; Yang, "North Korea's Lazarus Disguised as Chinese Virtual Asset Investors to Conduct Phishing Attacks"; "North Korean Hacking Organization Launches Full-Scale Attack on Domestic Defense Companies [Defense Media Agency]"; *2024* 국가정보보호백서 *[2024 National Cybersecurity White Paper],* 17; and "'라자루스', '안다리엘', '김수키'…북 해킹 공격에 방산업체 10여 곳 피해 [Lazarus, Andariel, Kimsuky… Over 10 Defense Contractors Affected by North Korean Hacking Attacks]."

235. *2024* 국가정보보호백서 *[2024 National Cybersecurity White Paper],* 13.

236. *2024* 국가정보보호백서 *[2024 National Cybersecurity White Paper].*

237. *2024* 국가정보보호백서 *[2024 National Cybersecurity White Paper].*

238. *2024* 국가정보보호백서 *[2024 National Cybersecurity White Paper]*, 12.

239. So Jeong Kim, "South Korea's Capacity Building Against North Korean Cyberthreats," National Bureau of Asian Research, December 19, 2023, https://www.nbr.org/publication/south-koreas-capacity-building-against-north-korean-cyberthreats/.

240. Choe Sang-Hun, "South Korea Blames North for June Cyberattacks," *The New York Times*, July 16, 2013, https://www.nytimes.com/2013/07/17/world/asia/south-korea-blames-

north-for-june-cyberattacks.html; Matthew Weaver, "Cyber Attackers Target South Korea and US," *The Guardian*, July 8, 2009, https://www.theguardian.com/world/2009/jul/08/south-korea-cyber-attack.

241. "Responding to North Korean Cyber Threats, White Hat Conference 2023," KFN News, November 16, 2023, https://www.youtube.com/watch?v=pTPXSZG0e7A.

242. *Republic of Korea National Cybersecurity Strategy; 2023 Cyber Strategy of The Department of Defense* (U.S. Department of Defense, 2023) https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.PDF.

243. *2023 Cyber Strategy of The Department of Defense.*

244. Meghna Pradhan, "Cyber Insecurity in South Korea: Decoding Cybersecurity Vulnerabilities," SSPC Issue Brief, September 2, 2024, https://sspconline.org/sites/default/files/2024-10/IB_SSPC-Pradhan-Sept-2024.pdf.

245. *2024* 국가정보보호백서 *[2024 National Cybersecurity White Paper].*

246. "South Korea—Information and Communication Technology," International Trade Administration, December 5, 2023, https://www.trade.gov/country-commercial-guides/south-korea-information-and-communication-technology.

247. "South Korea—Information and Communication Technology."

248. Bae Kim & Lee LLC, "Major Amendment to the IT Network Act," Lexology, August 8, 2024, https://www.lexology.com/library/detail.aspx?g=8dcb7d8e-8caf-4472-9daf-91ec-0d6070a2.

249. "South Korea: Data Protection Laws of the World," DLA Piper, https://www.dlapiperdataprotection.com/index.html?t=law&c=KR.

250. Kim, "South Korea's Capacity Building Against North Korean Cyberthreats."

251. *Republic of Korea National Cybersecurity Strategy*; "PPP Calls for Opposition's Support on Pending Cyber Law Amid N.K. Hacking Threats," Yonhap News Agency, December 5, 2023, https://en.yna.co.kr/view/AEN20231205003500315.

252. *Republic of Korea National Cybersecurity Strategy;* "Basic Cyber Security Bill (27 Members Including Cho Tae-yong)," The Codit, https://thecodit.com/kr-en/bill/sh/20200630-000000002101220; "National Cyber Security Act (13 Members Including Congressman Kim Byung-ki)," The Codit, https://thecodit.com/kr-en/bill/sh/20211104-000000002113145; "Basic Cyber Security Bill (12 Members Including Congressman Young-chan Yoon)," The Codit, https://thecodit.com/kr-en/bill/sh/20211202-000000002113670.

253. "Basic Cyber Security Bill (27 Members Including Cho Tae-yong)"; "National Cyber Security Act (13 Members Including Congressman Kim Byung-ki)"; Jo Jae-hak, "Cyber Threats Are Growing. . . 'National Cyber Security Basic Act' Sleeping in the National Assembly," etnews, April, 28, 2024, https://www.etnews.com/20240428000043; "Basic Cyber Security Bill (12 Members Including Congressman Young-chan Yoon)."

254. Jiyoung Sohn, Timothy W. Martin, and Josh Chin, "South Korea Impeaches President Yoon Suk Yeol Over Martial-Law Decision," *The Wall Street Journal*, December 14, 2024, https://www.wsj.com/world/asia/south-korea-president-yoon-suk-yeol-impeached-49b0779c.

255. According to a 2023 survey conducted by KISA, sales in South Korea's cybersecurity sector increased by 23.5 percent between 2021 and 2022, while the number of professionals in cybersecurity grew by 29.9 percent during the same period. However, among the cybersecurity companies surveyed over 71 percent of companies identified hiring and retaining personnel as the biggest challenge faced in technology development, see *2023 Domestic Information Security Industry Survey Report* (Ministry of Science and Information and Communication Technology, Korea Information Security Industry Association, August 2023), https://www.kisia.or.kr/bucket/uploads/2023/09/05/2023%EB%85%84%20%EA%B5%AD%EB%82%B4%20%EC%A0%95%EB%B3%B4%EB%B3%B4%ED%98%B8%EC%82%B0%EC%97%85%20%EC%8B%A4%ED%83%9C%EC%A1%B0%EC%82%AC%20%EB%B3%B4%EA%B3%A0%EC%84%9C_lAxPZSY.pdf.

256. *2024* 국가정보보호백서 *[2024 National Cybersecurity White Paper],* 186.

257. "School of Cybersecurity," Korea University School of Cybersecurity, accessed May 2, 2025, https://gss.korea.edu/sis_en/organisations/sis.do.

258. "School of Cybersecurity."

259. Park Soo-yoon, "사이버장교 교육했더니 딴길로…사이버국방학 졸업생 17%만 임관 [Cyber Officer Training, But Then It Went the Other Way. . . Only 17% of Cyber Defense Graduates Get Commissioned]," Yonhap News Agency, September 17, 2023, https://www.yna.co.kr/view/AKR20230915148800504.

260. Park, "사이버장교 교육했더니 딴길로…사이버국방학 졸업생 17%만 임관 [Cyber Officer Training, But Then It Went the Other Way. . . Only 17% of Cyber Defense Graduates Get Commissioned]"; "단독]애써 키운 사이버전 장교 90% 떠난다[Exclusive, 90% of Cyber Warfare Officers Who Were Carefully Raised Are Leaving]," April 14, 2023, https://www.youtube.com/watch?v=9lw4WRLX0p4.

261. Park, "사이버장교 교육했더니 딴길로…사이버국방학 졸업생 17%만 임관 [Cyber Officer Training, But Then It Went the Other Way. . . Only 17% of Cyber Defense Graduates Get Commissioned]"; "단독]애써 키운 사이버전 장교 90% 떠난다 [Exclusive, 90% of Cyber Warfare Officers Who Were Carefully Raised Are Leaving]";

262. "제54차 한미안보협의회의 공동성명 [Joint Statement of the 54th ROK-US Security Consultative Meeting]," 주한미국대사관 및 영사관 [U.S. Embassy and Consulates in Korea] November 3, 2022, https://kr.usembassy.gov/ko/110322-54th-security-consultative-meeting-joint-communique-ko/; U.S. Department of State, "7th U.S.-ROK Cyber Policy Consultations," press release, January 24, 2024, https://2021-2025.state.gov/7th-u-s-rok-cyber-policy-consultations/.

263. "Strategic Cybersecurity Cooperation Framework Between the Republic of Korea and the United States of America," ROK Ministry of Foreign Affairs, April 2023, 2, https://www.mofa.go.kr/www/brd/m_26779/down.do?brd_id=100112&seq=182&data_tp=A&file_seq=1.

264. U.S. Forces Korea, "Freedom Shield 24 Set to Begin," press release, February 27, 2024, https://www.usfk.mil/Media/Press-Products/Press-Releases/Article/3688893/freedom-shield-24-set-to-begin/.

265. Joe Saballa, "S. Korea to Join US-Led Multinational Cyber Defense Exercise," The Defense Post, June 29, 2022, https://thedefensepost.com/2022/06/29/south-korea-cyber-defense/; "제54차 한미안보협의회의 공동성명 [Joint Statement of the 54th ROK-US Security Consultative Meeting],"; and "Cyber Command Moving Out. . . Another 11.1 Billion Won Spent in Successive Relocations," MBC News, October 3, 2022, https://www.youtube.com/watch?v=_vYIS3S2xOI.

266. U.S. Cyber Command, "U.S. Cyber Command Hosts First Offensive Cyber Flag 2024 Exercise," press release, September 3, 2024, https://www.cybercom.mil/Media/News/Article/3893166/us-cyber-command-hosts-first-offensive-cyber-flag-2024-exercise/.

267. Saballa, "S. Korea to Join US-Led Multinational Cyber Defense Exercise."

268. U.S. Pacific Fleet, "Japan-ROK-U.S. Conduct Second Exercise Freedom Edge," press release, November 13, 2024, https://www.cpf.navy.mil/newsroom/news/article/3965275/japan-rok-us-conduct-second-exercise-freedom-edge/.

269. "Republic of Korea-UK Strategic Cyber Partnership," UK Government, November 23, 2023, https://www.gov.uk/government/publications/uk-republic-of-korea-strategic-cyber-partnership/republic-of-korea-uk-strategic-cyber-partnership.

270. "Cybersecurity," Security Council Report, June 1, 2024, https://www.securitycouncilreport.org/monthly-forecast/2024-06/cybersecurity-2.php.

271. "OEWG's Ninth Substantive Session: Limited Progress in Discussions," DigWatch, December 30, 2024, https://dig.watch/updates/oewgs-ninth-substantive-session-limited-progress-in-discussions.

272. *2024* 국가정보보호백서 *[2024 National Cybersecurity White Paper]*, 20.

273. *2024* 국가정보보호백서 *[2024 National Cybersecurity White Paper]*, 51.

274. *2024* 국가정보보호백서 *[2024 National Cybersecurity White Paper]*, 51.

275. Fortinet, "Fortinet Signs Cyber Partnership Agreement with Korea Internet & Security Agency (KISA)," press release, August 9, 2016, https://web.archive.org/web/20250502062151/https://www.fortinet.com/corporate/about-us/newsroom/press-releases/2016/cyber-partnership-korea-internet-security-agency.

276. "WildFire South Korea Cloud," Paloalto, July 19, 2024, https://docs.paloaltonetworks.com/wildfire/u-v/wildfire-whats-new/latest-wildfire-cloud-features/wildfire-south-korea-cloud.

277. Giacomo Lee, "South Korea: Microsoft Azure First Hyperscaler to Serve Korean Public Sector," ERP Today, December 3, 2024, https://erp.today/south-korea-microsoft-azure-first-hyperscaler-to-serve-korean-public-sector/.

278. Lee Kyung-tak, "Google Cloud Secures Certification, Targets South Korean Public Sector Market," Chosun Biz, February 3, 2025, https://biz.chosun.com/en/en-it/2025/02/03/M2F4QRHEBRFNTKBHCRBQMY6S7Y/.

279. "U.S.-Taiwan Relationship," U.S. Department of State, February 13, 2025, archived April 22, 2025, https://web.archive.org/web/20250422135722/https://www.state.gov/u-s-relations-with-taiwan/.

280. Chad De Guzman, "For Taiwan, Trump's Strategic Ambiguity Brings Anxious Uncertainty," *Time*, February 27, 2025, https://time.com/7262281/us-taiwan-relations-trump-china-strategic-ambiguity-anxious-uncertainty-explainer.

281. *2024*年中共網駭攻擊態樣分析(報告全文) *[Analysis of Patterns of Cyber Attacks by the CCP in 2024 (Full Report)*], (國家安全局[National Security Bureau], 2024), https://www.nsb.gov.tw/zh/assets/documents/新聞稿/2024年中共網駭攻擊態樣分析(報告全文)-中文.pdf.

282. *2024*年中共網駭攻擊態樣分析(報告全文) *[Analysis of Patterns of Cyber Attacks by the CCP in 2024 (Full Report)*].

283. Yoachimik and Pacheco, "DDoS Threat Report for 2023 Q4."

284. "Disinformation Is on the Rise. How Does It Work?" *The Economist*, May 1, 2024, https://www.economist.com/science-and-technology/2024/05/01/disinformation-is-on-the-rise-how-does-it-work; Enescan Lorci, "The Nexus of Cybersecurity and National Security: Taiwan's Imperatives Amidst Escalating Cyber Threats," Global Taiwan Institute, March 20, 2024, https://globaltaiwan.org/2024/03/the-nexus-of-cybersecurity-and-national-security-taiwans-imperatives-amidst-escalating-cyber-threats/.

285. Ryan Gallagher, "Google Warns China Is Ramping Up Cyberattacks Against Taiwan," *Bloomberg,* November 29, 2023, https://www.bloomberg.com/news/articles/2023-11-29/google-warns-china-is-ramping-up-cyberattacks-against-taiwan.

286. Insikt Group, "Chinese State-Sponsored RedJuliett Intensifies Taiwanese Cyber Espionage via Network Perimeter Exploitation," Recorded Future, June 24, 2024, https://www.recordedfuture.com/research/redjuliett-intensifies-taiwanese-cyber-espionage-via-network-perimeter.

287. Insikt Group, "Chinese State-Sponsored RedJuliett Intensifies Taiwanese Cyber Espionage via Network Perimeter Exploitation."

288. "Hackers Stole 'Sensitive' Data From Taiwan Telecom Giant: Ministry," France 24, January 3, 2024, https://www.france24.com/en/live-news/20240301-hackers-stole-sensitive-data-from-taiwan-telecom-giant-ministry.

289. Baker, "Advanced Persistent Threats (APT) Explained."

290. Microsoft Threat Intelligence, "Flax Typhoon Using Legitimate Software to Quietly Access Taiwanese Organizations."

291. Helen Davidson, "Explainer: What Is Volt Typhoon and Why Is It the 'Defining Threat of Our Generation'?" *The Guardian*, February 13, 2024, https://www.theguardian.com/technology/2024/feb/13/volt-typhoon-what-is-it-how-does-it-work-chinese-cyber-operation-china-hackers-explainer.

292. "Taiwan's Dominance of the Chip Industry Makes It More

Important," *The Economist*, March 6, 2023, https://www.economist.com/special-report/2023/03/06/taiwans-dominance-of-the-chip-industry-makes-it-more-important.

293. Duncan Riley, "Taiwan's Foxsemicon Falls Victim to LockBit Ransomware Attack," Silicon Angle, January 17, 2024, https://siliconangle.com/2024/01/17/taiwans-foxsemicon-falls-victim-lockbit-ransomware-attack/.

294. Russel, "North Korea's Next Weapon of Choice: Cyber."

295. U.S. Department of Justice, "Fourteen North Korean Nationals Indicted for Carrying Out Multi-Year Fraudulent Information Technology Workers Scheme and Related Extortions," press release, December 12, 2024, https://www.justice.gov/archives/opa/pr/fourteen-north-korean-nationals-indicted-carrying-out-multi-year-fraudulent-information.

296. Yoachimik and Pacheco, "DDoS Threat Report for 2023 Q4."

297. Anne An, "Cyber Tools and Foreign Policy: A False Flag Chinese 'APT' and Nancy Pelosi's Visit to Taiwan," Trellix, September 29, 2022, http://trellix.com/blogs/research/cyber-tools-and-foreign-policy/;"Hackers Stole 'Sensitive' Data From Taiwan Telecom Giant: Ministry."

298. Bang Xiao and Joshua Boscaini, "Taiwan Billboards Hacked with Anti-Nancy Pelosi Messages During Historic Visit," ABC Australia, August 4, 2022, https://www.abc.net.au/news/2022-08-04/taiwan-billboards-hacked-with-anti-nancy-pelosi-messages/101300164?utm.

299. An, "Cyber Tools and Foreign Policy: A False Flag Chinese 'APT' and Nancy Pelosi's Visit to Taiwan."

300. Valeriya Mechkova, et al., *Measuring Internet Politics: Digital Society Project (DSP) Annual Report v4* (Digital Society Project, August 2022), https://digitalsocietyproject.org/wp-content/uploads/2022/08/DSP_working_paper_1_v4.pdf; Yang Mien-chieh and Jonathan Chin, "Taiwan Most Targeted for False Information: Study," *Taipei Times*, March 20, 2022, https://www.taipeitimes.com/News/taiwan/archives/2022/03/20/2003775114.

301. Mien-chieh and Chin, "Taiwan Most Targeted for False Information: Study."

302. Rishi Iyengar, "How China Exploited Taiwan's Election—and What It Could Do Next," *Foreign Policy*, January 23, 2024, https://foreignpolicy.com/2024/01/23/taiwan-election-china-disinformation-influence-interference/.

303. Albert Zhang, "As Taiwan Voted, Beijing Spammed AI Avatars, Faked Paternity Tests, and 'Leaked' Documents," Australian Strategic Policy Institute, January 18, 2024, https://www.aspistrategist.org.au/as-taiwan-voted-beijing-spammed-ai-avatars-faked-paternity-tests-and-leaked-fake-documents/.

304. Zhang, "As Taiwan Voted, Beijing Spammed AI Avatars, Faked Paternity Tests, and 'Leaked' Documents."

305. "Disinformation Is on the Rise. How Does It Work?"

306. "Disinformation Is on the Rise. How Does It Work?"

307. Laura He, "Wait, Is TikTok Really Chinese?" CNN, March 28, 2024, https://www.cnn.com/2024/03/18/tech/tiktok-bytedance-china-ownership-intl-hnk/index.html.

308. Meaghan Tobin and Amy Chang Chien, "Taiwan, on China's Doorstep, Is Dealing with TikTok Its Own Way," *The New York Times*, May 16, 2024, https://www.nytimes.com/2024/05/16/business/tiktok-taiwan.html.

309. Taiwan Ministry of Digital Affairs, "Ministry of Digital Affairs Bans General Public from Using TikTok?" press release, December 27, 2022, https://moda.gov.tw/press/clarification/3473.

310. Zhang, "As Taiwan Voted, Beijing Spammed AI Avatars, Faked Paternity Tests, and 'Leaked' Documents."

311. Riley, "Taiwan's Foxsemicon Falls Victim to LockBit Ransomware Attack"; Sam Sabin, "Taiwanese Government Websites Go Down During Pelosi's Visit," Axios, August 2, 2022, https://www.axios.com/2022/08/02/taiwan-government-websites-pelosi-visit; "Hackers Stole 'Sensitive' Data From Taiwan Telecom Giant: Ministry;" and Microsoft Threat Intelligence, "Flax Typhoon Using Legitimate Software to Quietly Access Taiwanese Organizations."

312. "Policy Elucidation," Taiwan Ministry of Digital Affairs, http://moda.gov.tw/en/major-policies/policy-elucidation/1305.

313. "History," Taiwan Ministry of Digital Affairs, Administration for Cyber Security, August 27, 2022, https://moda.gov.tw/en/ACS/aboutus/history/608.

314. "About Us," National Institute of Cyber Security, November 12, 2024, https://www.nics.nat.gov.tw/en/about/introduction/.

315. As was raised in the CNAS private dialogue held in Taipei.

316. "Regulations Governing the Establishment," Ministry of Digital Affairs Administration for Cyber Security, December 25, 2020, https://moda.gov.tw/en/ACS/nicst/establishment/660.

317. "Ministry of National Defense Launches New Cybersecurity Command," Ministry of Foreign Affairs Republic of China (Taiwan), July 3, 2017, https://nspp.mofa.gov.tw/nsppe/content_tt.php?unit=2&post=117794.

318. CNAS analysis of Taiwan's government agencies, including the following sources: "Organization," Administration for Cyber Security, Ministry of Digital Affairs, https://moda.gov.tw/en/ACS/nicst/organization/662; "About Ministry of National Defense," Ministry of National Defense Republic of China, January 1, 2022, https://www.mnd.gov.tw/english/Publish.aspx?p=74731&title=About%20MND-&SelectStyle=Ministry%20of%20National%20Defense; and "About Ministry of Digital Affairs," Ministry of Digital Affairs, https://moda.gov.tw/en/aboutus/organization/620.

319. "Cofacts," Rights CoLAB, https://rightscolab.org/case_study/cofacts/; "About Doublethink Lab," Doublethink Lab, https://doublethinklab.org/.

320. "Cisco to Establish Cybersecurity Centre in Taiwan," Reuters, June 17, 2024, https://www.reuters.com/technology/cybersecurity/cisco-establish-cybersecurity-centre-taiwan-2024-06-17/?utm.

321. Shiela Chiang, "Amazon's AWS to Launch New Infrastructure Region in Taiwan Amid Rapid Asia-Pacific Expansion," CNBC,

June 12, 2024, https://www.cnbc.com/2024/06/12/aws-to-launch-new-infrastructure-region-in-taiwan-as-it-expands-in-apac.html.

322. Ming-Chang Wu, "Can New Taiwan-U.S. Cooperation on Cybersecurity Raise the Profile of Taiwan in the Global Chip Supply Chain?" Semi, January 8, 2024, https://www.semi.org/en/blogs/technology-and-trends/can-new-taiwan-us-cooperation-on-cybersecurity-raise-the-profile-in-the-global-chip-supply-chain.

323. "Promoting the Six Core Strategic Industries," National Development Council, January 18, 2021, https://english.ey.gov.tw/News3/9E5540D592A5FECD/208da633-0f71-439a-8ef6-3d1e2aea1f34?utm.

324. "Cyber Security Policies and Regulations," Administration for Cyber Security, Ministry of Digital Affairs, accessed May 2, 2025, https://moda.gov.tw/en/ACS/operations/policies-and-regulations/648.

325. Valentin Weber, "Taiwan's Offensive Cyber Capabilities and Ramifications for Taiwan-China Conflict," Council on Foreign Relations, December 7, 2022, https://www.cfr.org/blog/taiwans-offensive-cyber-capabilities-and-ramifications-taiwan-china-conflict.

326. Tseng Ken-Ying, "A Comparison of Cybersecurity Regulations: Taiwan," Asia Business Law Journal, October 19, 2022, https://law.asia/taiwan-cybersecurity-regulations-2022/.

327. Ken-Ying, "A Comparison of Cybersecurity Regulations: Taiwan."

328. Ken-Ying, "A Comparison of Cybersecurity Regulations: Taiwan."

329. Laws and Regulations of the Republic of China (Taiwan), *Cybersecurity Management Act* (June 6, 2018), https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=A0030297.

330. *Cybersecurity Management Act* (June 6, 2018).

331. *Cybersecurity Management Act* (June 6, 2018); "A Comparison of Cybersecurity Regulations: Taiwan," PWC, https://www.pwc.com/id/en/pwc-publications/services-publications/legal-publications/a-comparison-of-cybersecurity-regulations/taiwan.html?utm.

332. "Cyber Security Policies and Regulations."

333. Ken-Ying, "A Comparison of Cybersecurity Regulations: Taiwan,"

334. Lorci, "The Nexus of Cybersecurity and National Security: Taiwan's Imperatives Amidst Escalating Cyber Threats"; "Cyber Security Policies and Regulations," Administration for Cyber Security, Ministry of Digital Affairs, accessed June 16, 2025, https://moda.gov.tw/en/ACS/operations/policies-and-regulations/648.

335. "Cyber Security Policies and Regulations."

336. Interviews at CNAS-Prospect Foundation private workshop on April 16, 2024. All interviews were conducted in confidentiality, and the names of interviewees are withheld by mutual agreement.

337. Lee Hsin-fang, "Information Security: At Least 900 Cybersecurity Jobs Need to be Filled to Combat Chinese Espionage," *Taipei Times*, April 6, 2021, https://www.taipeitimes.com/News/taiwan/archives/2021/04/06/2003755174.

338. Shelley Shan, "Cybertalent, Information Security Need Boost: NPP," *Taipei Times*, August 10, 2022, https://www.taipeitimes.com/News/taiwan/archives/2022/08/10/2003783292.

339. CNAS private dialogue in Taipei.

340. CNAS private dialogue in Taipei.

341. "ISIP," Cybersec 2023, https://cybersec.ithome.com.tw/2023/en/exhibition-page/1596.

342. "Google to Train 2,000 Cybersecurity Experts in Taiwan by 2025," ICRT, June 18, 2024, https://www.icrt.com.tw/info_details.php?mlevel1=6&mlevel2=12&news_id=265559&reUrlAddr=L25ld3NfZGF0YWJhc2UucGhwPyZtbGV2ZWwxPTYmbWxldmVsMj0zNyZwYWdlPTc=.

343. "Cisco to Establish Cybersecurity Centre in Taiwan."

344. "教育部資訊安全人才培育計畫 [Ministry of Education Information Security Talent Training Program]," Information Security Talent Training Program, https://isip.moe.edu.tw/.

345. Huynh Tam Sang, Tong Thai Thien, and Le Thi Yen Nhi, "How Taiwan Fights the Disinformation War," The Interpreter, June 20, 2024, https://www.lowyinstitute.org/the-interpreter/how-taiwan-fights-disinformation-war.

346. Mark A. Stokes, *Revolutionizing Taiwan's Security* (Project 2049 Institute, May 2018), https://project2049.net/wp-content/uploads/2018/05/revolutionizing_taiwans_security_leveraging_c4isr_for_traditional_and_non_traditional_challenges.pdf.

347. Jocelinn Kang, "States Vulnerable to Foreign Aggression Embrace the Cloud: Lessons from Taiwan," Australian Strategic Policy Institute, February 28, 2025, https://www.aspistrategist.org.au/states-vulnerable-to-foreign-aggression-embrace-the-cloud-lessons-from-taiwan/.

348. Kang, "States Vulnerable to Foreign Aggression Embrace the Cloud: Lessons from Taiwan."

349. "Google to Train 2,000 Cybersecurity Experts in Taiwan by 2025,"; "Building Skills to Keep Taiwan's Data Safe," Microsoft, https://local.microsoft.com/blog/building-skills-to-keep-taiwans-data-safe/.

350. Office of the President Republic of China (Taiwan), "Inaugural Address of ROC 16th-Term President Lai Ching-te," press release, May 20, 2024, https://english.president.gov.tw/News/6726.

351. Sean Scanlan, "Taiwan President Calls for Cybersecurity Cooperation," *Taiwan News*, May 14, 2023, https://www.taiwannews.com.tw/news/5686311.

352. U.S. Embassy & Consulates in India, "Representatives from the United States, India, and Taiwan Collaborate on Cybersecurity under the Global Cooperation and Training Framework," press release, December 11, 2023, https://in.usembassy.gov/representatives-from-the-united-states-india-and-taiwan-collaborate-on-cybersecurity-under-the-global-cooperation-and-training-framework/.

353. "Member Teams," Asia Pacific Computer Emergency Response Team, https://www.apcert.org/about/structure/members.html.

354. Jonathan Masters and Will Merrow, "U.S. Military Support for Taiwan in Five Charts," Council on Foreign Relations, September 25, 2024, https://www.cfr.org/article/us-military-support-taiwan-five-charts.

355. Defense Security Cooperation Agecny, "Taipei Economic and Cultural Representative Office in the United States (TECRO) – Taiwan Advanced Tactical Data Link System Upgrade Planning," press release, February 21, 2024, https://media.defense.gov/2024/Dec/18/2003615490/-1/-1/0/PRESS%20RELEASE%20-%20TECRO%2024-09%20CN.PDF.

356. Executive Yuan, "Taiwan and US Co-Hosting Multinational Cybersecurity Exercise," press release, June 11, 2019, https://english.ey.gov.tw/Page/61BF20C3E89B856/0f357b66-7ed3-4123-98c6-b91097b82536.

357. "Talent Circulation Alliance White Paper," American Institute in Taiwan, June 12, 2020, https://www.ait.org.tw/talent-circulation-alliance-white-paper/.

358. Wu, "Can New Taiwan-U.S. Cooperation on Cybersecurity Raise the Profile of Taiwan in the Global Chip Supply Chain?"

359. "Taiwan, US to Expand Cybersecurity Agreement," *Taipei Times*, September 21, 2023, https://www.taipeitimes.com/News/biz/archives/2023/09/21/2003806535.

360. Taiwan Enhanced Resilience, 22 U.S.C. § Chapter 48A, https://uscode.house.gov/view.xhtml?path=/prelim@title22/chapter48A&edition=prelim.

361. Taiwan Relations, 22 U.S.C. § Chapter 48, https://uscode.house.gov/view.xhtml?path=%2Fprelim%40title22%2Fchapter48&req=granuleid%3AUSC-prelim-title22-chapter48&f=&fq=&num=0&hl=false&edition=prelim.

362. David Sacks, "Taiwan's Latest Defense Budget Risks Falling Further Behind China," Council on Foreign Relations, August 9, 2024, https://www.cfr.org/blog/taiwans-latest-defense-budget-risks-falling-further-behind-china.

363. Holmes Liao, "Beyond a Budget Boost: Modernizing Taiwan's Defense," The Diplomat, March 12, 2025, https://thediplomat.com/2025/03/beyond-a-budget-boost-modernizing-taiwans-defense/.

364. Si Ying Thian, "'Turning Conflicts Into Co-Creation': Taiwan Government Harnesses Digital Policy for Democracy," GovInsider, December 6, 2023, https://govinsider.asia/intl-en/article/turning-conflicts-into-co-creation-taiwans-digital-ministry-moda-harnesses-digital-policy-for-democracy.

365. Arpita Dutta, "'An Influx of 100,000 Indian Workers to Taiwan'—What Is Scarier: Numbers or the Nation?" CommonWealth Magazine, December 11, 2023, https://english.cw.com.tw/article/article.action?id=3580.

366. Sandra Erwin, "Space Force Preparing for the Proliferated Low Earth Orbit Satellite Networks," Space News, July 8, 2024, https://spacenews.com/space-force-preparing-for-the-age-of-proliferated-low-earth-orbit-satellite-networks/.

367. "U.S. Relations with the Philippines," U.S. Department of State, February 23, 2023, archived on April 5, 2025, https://web.archive.org/web/20250405092749/https://www.state.gov/u-s-relations-with-the-philippines/.

368. "Philippines and U.S. Conclude Balikatan Exercises, Shoulder-to-Shoulder," U.S. Marine Corps Forces, Pacific, May 10, 2024, https://www.marforpac.marines.mil/Media-Room/Pacific-Marines-Stories/Article/Article/3771258/philippines-and-us-conclude-balikatan-exercises-shoulder-to-shoulder/.

369. "The Strong Partnership Between U.S. Businesses and Outsourcing in the Philippines," FGC, October 27, 2023, https://fgcplus.com/us-businesses-and-outsourcing-in-philippines/.

370. *Cisco AI Readiness Index: Intentions Outpacing Abilities, The Philippines* (Cisco, 2023), https://www.cisco.com/c/dam/m/en_us/solutions/ai/readiness-index/documents/cisco-ai-readiness-index-philippines.pdf.

371. *Global Cybersecurity Index 2024 Report* (International Telecommunication Union, 2024), https://www.itu.int/en/ITU-D/Cybersecurity/pages/global-cybersecurity-index.aspx; *Global Cybersecurity Index 2020 Report* (International Telecommunication Union, 2020), https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E.

372. Kris Crismundo, "Ransomware Attacks in PH Double in 2023," Philippine News Agency, January 16, 2024, https://www.pna.gov.ph/articles/1217037; "Philippines Country Commercial Guide: eCommerce," International Trade Administration, January 24, 2024, https://www.trade.gov/country-commercial-guides/philippines-ecommerce.

373. Vittoria Elliott, "345,000 Sensitive Legal Documents From the Philippines Government Have Been Exposed Online," Rest of World, April 30, 2021, https://restofworld.org/2021/philippines-data-exposure/; "1.2M Police Records & 800GB of Info on Philippines Law Enforcement Exposed," Secure Blink, April 20, 2023, https://www.secureblink.com/cybersecurity-news/1-2-m-police-records-and-800-gb-of-info-on-philippines-law-enforcement-exposed.

374. *National Cybersecurity Plan 2023–2028,* (Republic of the Philippines Department of Information and Communications Technology, February 2024), https://cms-cdn.e.gov.ph/DICT/pdf/NCSP-2023-2028-FINAL-DICT.pdf.

375. "Philippines Accuses China of Firing Water Cannon at Boats in South China Sea," BBC, August 5, 2023, https://www.bbc.com/news/world-asia-66419333; "Stately Taurus Targets the Philippines As Tensions Flare in the South Pacific."

376. Evan Wright and Elizabeth Whatcott, "To Meet China's Challenges to Philippine Soverignty, Don't Forget Cybersecurity," Philstar Global, June 29, 2024, https://www.philstar.com/news-commentary/2024/06/29/2366478/meet-chinas-challenges-philippine-sovereignty-dont-forget-cybersecurity; Hannah Beech, "Blasting Bullhorns and Water Cannons, Chinese Ships Wall Off the Sea," *The New York Times*, September 23, 2023, https://www.nytimes.com/2023/09/23/world/asia/china-sea-philippines-us.html.

377. *Same Targets, New Playbooks: East Asia Threat Actors Employ Unique Methods,* (Microsoft Threat Intelligence, April 4, 2024), https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/east-asia-threat-actors-employ-unique-methods.

378. Jamie Tarabay, "Chinese Hackers Target Philippine President and Steal Military Data," *Bloomberg*, January 6, 2025, https://www.bloomberg.com/news/articles/2025-01-07/chinese-hackers-target-philippine-president-steal-military-data.

379. "Philippines Wards Off Cyber Attacks from China-Based Hackers," Reuters, February 5, 2024, https://www.reuters.com/world/asia-pacific/philippines-wards-off-cyber-attacks-china-based-hackers-2024-02-05.

380. Susannah Patton, "Unpacking China's Propaganda Narratives Against the Philippines," The Interpreter, June 2024, https://www.lowyinstitute.org/the-interpreter/unpacking-china-s-propaganda-narratives-against-philippines.

381. Melvin Gascon, "Beware of Chinese 'Lies' Claiming Palawan—PH Maritime Council," Inquirer.net, March 7, 2025, https://www.inquirer.net/431574/beware-of-chinese-lies-claiming-palawan-ph-maritime-council/; Joviland Rita, "PH Calls Chinese Ownership Claim of Palawan 'Absurd,' 'Fabrication,'" GMA Integrated News, March 4, 2025, https://www.gmanetwork.com/news/topstories/nation/938130/palawan-china-philippine-navy-social-media-claim-ownership/story/#goog_rewarded.

382. Richard Javad Heydarian, "Ignoring the US, Philippines Goes with Huawei," *Asia Times*, July 18, 2019, https://asiatimes.com/2019/07/ignoring-the-us-philippines-goes-with-huawei/#.

383. Niharika Mandhana, "Huawei's Video Surveillance Business Hits Snag in Philippines," *The Wall Street Journal*, February 20, 2019, https://www.wsj.com/articles/huaweis-video-surveillance-business-hits-snag-in-philippines-11550683135; Dan Swinhoe, "Huawei Launches Cloud Region in Philippines," Data Center Dynamics, December 5, 2024, https://www.datacenterdynamics.com/en/news/huawei-launches-cloud-region-in-philippines/.

384. Wright and Whatcott, "To Meet China's Challenges to Philippine Sovereignty, Don't Forget Cybersecurity"; *Same Targets, New Playbooks: East Asia Threat Actors Employ Unique Methods;* Tarabay, "Chinese Hackers Target Philippine President and Steal Military Data"; Gascon, "Beware of Chinese 'Lies' Claiming Palawan—PH Maritime Council"; and Beech, "Blasting Bullhorns and Water Cannons, Chinese Ships Wall Off the Sea."

385. "Who We Are," Republic of the Philippines Department of Information and Communications Technology, https://dict.gov.ph/home.

386. Interviews at CNAS-Stratbase ADR Institute private workshop in Manila on June 24, 2024. All interviews were conducted in confidentiality, and the names of interviewees are withheld by mutual agreement.

387. "Cybercrime Investigation and Coordinating Center (CICC)," GOVPH, accessed May 2, 2025, https://cicc.gov.ph/?appgw_azwaf_jsc=6cvMh8MmACIz1FqAAp4XB-PZ53WdWYjBUBwm0Mn8RwAo; "About Us," Philippine National Computer Emergency Response Team, https://www.ncert.gov.ph/about-us/.

388. "Executive Order No. 95," The LawPhil Project, November 15, 2019, https://lawphil.net/executive/execord/eo2019/eo_95_2019.html.

389. Armed Forces of the Philippines, "AFP Reinforces Cyber Security in a Change of Command Ceremony," press release, October 3, 2024, https://www.afp.mil.ph/news/afp-reinforces-cyber-security-in-a-change-of-command-ceremony.

390. "Philippine National Police Anti-Cybercrime Group (PNP-ACG)," Cybersecurity Intelligence, https://www.cybersecurityintelligence.com/philippine-national-police-anti-cybercrime-group-pnp-acg-4731.html.

391. "Who We Are"; *National Cybersecurity Plan 2023–2028*; "CERT-PH," NCERT, https://www.ncert.gov.ph/about-us/ncert/; "Cybercrime Investigation and Coordinating Center (CICC)"; "About Us"; and "Executive Order No. 95."

392. "PBBM Adopts DICT's National Cybersecurity Plan 2023–2028," Presidential Communications Office, April 6, 2024, https://pco.gov.ph/news_releases/pbbm-adopts-dicts-national-cybersecurity-plan-2023-2028.

393. "Republic Act No. 10175, "The LawPhil Project, https://lawphil.net/statutes/repacts/ra2012/ra_10175_2012.html.

394. Cybersecurity Act, S.B. 1365, 19th Cong. (Phil. 2022), https://legacy.senate.gov.ph/lis/bill_res.aspx?congress=19&q=SBN-1365.

395. Cybersecurity Act.

396. "Republic Act No. 10175."

397. "Republic Act No. 10175"; "The Data Privacy Act and Its IRR," National Privacy Commission, https://privacy.gov.ph/the-data-privacy-act-and-its-irr/.

398. *National Cybersecurity Talent Workforce Assessment Report of the Philippines* (IBM, 2022), https://drive.google.com/file/d/1TpcH9bmClamu3Qg9vqW3DIHKODMgKOgr/view?usp=share_link&usp=embed_facebook.

399. Aubrey Rose A. Inosante, "Academic Programs Seen to Help Address Workforce Gap in Cybersecurity Sector," BusinessWorld, May 22, 2024, https://www.bworldonline.com/technology/2024/05/23/596761/academic-programs-seen-to-help-address-workforce-gap-in-cybersecurity-sector/.

400. Cliff Harvey Venzon and Ditas B Lopez, "Philippines Turns to Hackers for Help as US Warns of China Cyber Threat," *Bloomberg*, January 7, 2024, https://www.bloomberg.com/news/articles/2024-01-07/philippines-turn-to-hackers-for-cybersecurity-help-as-tensions-with-china-rise.

401. *Annual Report 2022* (Asia Pacific Computer Emergency Response Team, 2022), https://www.apcert.org/documents/pdf/APCERT_Annual_Report_2022.pdf.

402. *National Cybersecurity Plan 2023–2028*.

403. *National Cybersecurity Plan 2023–2028*.

404. Interviews at CNAS-Stratbase ADR private workshop on June 24, 2024. All interviews were conducted in confidentiality, and the names of interviewees are withheld by mutual agreement.

405. "Republic Act No. 11927," The LawPhil Project, https://lawphil.net/statutes/repacts/ra2022/ra_11927_2022.html; *Philippine Digital Transformation Strategy 2022*,

(Department of Information and Communications Technology, 2022, archived October 11, 2019), https://web.archive.org/web/20191011010155/https://www.gov.ph/documents/820828/1076083/Philippine+Digital+Transformation+Strategy_20190208.pdf/74f4f221-2915-8136-a4c0-e6829c47dce9?t=1549932892309.

406. Ivan John E. Uy, et al., "Cybersecurity in the Indo-Pacific: Philippines," (public event, CNAS, Makati City, Philippines, June 24, 2024), https://www.cnas.org/events/cybersecurity-in-the-indo-pacific-philippines.

407. *National Cybersecurity Plan 2023–2028.*

408. *National Cybersecurity Plan 2023–2028*; Ralf Rivas, "The Billionaires Advising Marcos How to Run the Economy," Rappler, June 27, 2023, https://www.rappler.com/business/billionaires-advising-marcos-jr-run-philippine-economy/.

409. *National Cybersecurity Plan 2023–2028.*

410. Katlene O. Cacho, "DICT to Position PH as Cybersecurity Hub," Sunstar, August 16, 2023, https://www.sunstar.com.ph/cebu/local-news/dict-to-position-ph-as-cybersecurity-hub.

411. "Philippines Imports: Telecommunication Equipment," CEIC, https://www.ceicdata.com/en/indicator/philippines/imports-telecommunication-equipment.

412. "Seventh Substantive Session of the Open-Ended Working Group on Security and the Use of Information and Communications Technologies 2021–2025," Permanent Mission of the Republic of the Philippines to the United Nations, March 6, 2024, https://www.un.int/philippines/statements_speeches/seventh-substantive-session-open-ended-working-group-security-and-use-0.

413. "Joint Statement on the United States-Philippines Cyber-Digital Policy Dialogue," U.S. Department of State, archived July 26, 2024, https://web.archive.org/web/20240726162934/https://www.state.gov/joint-statement-on-the-united-states-philippines-cyber-digital-policy-dialogue; "The Philippines Strengthens Digital Cooperation with Singapore," OpenGov, January 19, 2023, https://opengovasia.com/2023/01/19/the-philippines-strengthens-digital-cooperation-with-singapore/.

414. "Fact Sheet: Celebrating the Strength of the U.S.-Philippines Alliance," The White House, April 11, 2024, https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2024/04/11/fact-sheet-celebrating-the-strength-of-the-u-s-philippines-alliance/.

415. "Summary of Memorandum of Understanding Between the Government of the Republic of the Philippines and the Government of Australia on Cyber and Critical Technology Cooperation," Australian Department of Foreign Affairs and Trade, https://www.dfat.gov.au/countries-economies-and-regions/summary-memorandum-understanding-between-government-republic-philippines-and-government-australia-cyber-and-critical-technology-cooperation.

416. Uy, et al., "Cybersecurity in the Indo-Pacific: Philippines."

417. "FACT SHEET: U.S.-Philippines Bilateral Defense Guidelines," U.S. Department of Defense, May 3, 2023, https://www.defense.gov/News/Releases/Release/Article/3383607/fact-sheet-us-philippines-bilateral-defense-guidelines/.

418. "Joint Statement on the Philippines-United States Fourth 2+2 Ministerial Dialogue," U.S. Department of Defense, July 30, 2024, https://www.defense.gov/News/Releases/Release/Article/3854902/joint-statement-on-the-philippines-united-states-fourth-22-ministerial-dialogue/; "Joint Statement on the United States-Philippines Cyber-Digital Policy Dialogue."

419. Vincent Labador, "Risk Reduction Event Makes Significant Strides in Partner Force Interoperability," U.S. Army, April 12, 2024, https://www.army.mil/article/275300/risk_reduction_event_makes_significant_strides_in_partner_force_interoperability.

420. Karen Lema, "Philippines, United States Sign Military Intelligence-Sharing Deal," Reuters, November 18, 2024, https://www.reuters.com/world/philippines-united-states-sign-military-intelligence-sharing-deal-2024-11-18/.

421. "Joint Statement on the United States-Philippines Cyber-Digital Policy Dialogue."

422. Interviews at the CNAS-Prospect Foundation private workshop in Taipei on April 16, 2024, the CNAS-JIIA private workshop in Tokyo on April 19, 2024, the CNAS-Stratbase ADR Institute private workshop in Manila on June 24, 2024, and the CNAS-Asan Institute for Policy Studies private workshop in Seoul on June 27, 2024. All interviews were conducted in confidentiality, and the names of interviewees are withheld by mutual agreement.

423. *NIST Cybersecurity Framework (CSF) 2.0* (National Institute of Standards and Technology, February 26, 2024), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf.

424. "New ISC2 Study Reveals Impact of AI on Cyber Professionals and Urgent Need for Preparedness," February 21, 2024, https://www.isc2.org/Insights/2024/02/AI-Survey.

425. "Secure by Design," Cybersecurity and Infrastructure Security Agency, https://www.cisa.gov/securebydesign.

426. Interviews at CNAS-JIIA private workshop on April 19, 2024, and CNAS-Stratbase ADR Institute private workshop in Manila on June 24, 2024. All interviews were conducted in confidentiality, and the names of interviewees are withheld by mutual agreement.

About the Center for a New American Security

The mission of the Center for a New American Security (CNAS) is to develop strong, pragmatic and principled national security and defense policies. Building on the expertise and experience of its staff and advisors, CNAS engages policymakers, experts and the public with innovative, fact-based research, ideas and analysis to shape and elevate the national security debate. A key part of our mission is to inform and prepare the national security leaders of today and tomorrow.

CNAS is located in Washington, DC, and was established in February 2007 by co-founders Kurt M. Campbell and Michèle A. Flournoy. CNAS is a 501(c)3 tax-exempt nonprofit organization. Its research is independent and non-partisan.

AMERICA'S EDGE 2025

The United States faces a rapidly changing global security landscape. Evolving technology, shifting alliances, and emerging threats require America to harness bold, innovative approaches. America's Edge is a Center-wide initiative featuring research, events, and multimedia for enhancing America's global edge.

CNAS Editorial

DIRECTOR OF STUDIES
Katherine L. Kuzminski

PUBLICATIONS & EDITORIAL DIRECTOR
Maura McCarthy

SENIOR EDITOR
Emma Swislow

ASSOCIATE EDITOR
Caroline Steel

CREATIVE DIRECTOR
Melody Cook

DESIGNER
Alina Spatz

Cover Art & Production Notes

COVER ILLUSTRATION
Melody Cook

PRINTER
CSI Printing & Graphics
Printed on an HP Indigo Digital Press

Center for a New American Security
1701 Pennsylvania Ave NW
Suite 700
Washington, DC 20006
CNAS.org
@CNASdc

Contact Us
202.457.9400
info@cnas.org

Center for a
New American
Security