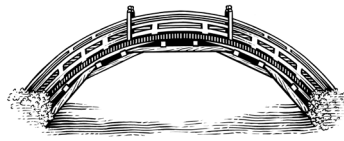


ROUNDTABLE

Cyber Resilience in the Indo-Pacific



Karthik Nachiappan

Arindrajit Basu

Gatra Priyandita

Dai Mochinaga

Dongyoun Cho

Introduction

Karthik Nachiappan

This *Asia Policy* roundtable maps and analyzes the state of cyber resilience in four key Indo-Pacific countries—India, Indonesia, Japan, and South Korea—by identifying and assessing the political and institutional conditions underpinning cybersecurity (cybersecurity strategies, laws, institutions, financing, and agencies) and how they interact with each other to deter and mitigate threats online. This introduction lays out the motivations to study cyber resilience in the Indo-Pacific. The four subsequent essays in this roundtable are framed around questions that measure and identify these countries’ cyber resilience—how they *resist*, *recover*, and *adapt* from malicious cyber activities.

The Rise of Cyberthreats

Intense security competition and rapid digitalization in the Indo-Pacific have increased cyber vulnerabilities, especially cyberattacks, cyber espionage, cybercrime, disinformation, and the targeting of critical public and private infrastructure. Data fraud and theft are rising: 35% of firms in the Asia-Pacific suffered data breaches costing \$1–\$20 million in 2023.¹ According to a Nord VPN survey, the United States experienced nearly 200 serious cyberattacks on its government agencies between 2006 and 2021, which was the most for any country (followed by the United Kingdom, India, Australia, and Japan).²

Some Asian countries are being used as sites to launch cyberattacks as hotspots with vulnerable infrastructure or as highly connected hubs to initiate and execute attacks. Russian and North Korean cyber activities and artificial intelligence–powered threats complicate Indo-Pacific

KARTHIK NACHIAPPAN is a Fellow in the Institute of South Asian Studies at the National University of Singapore (Singapore) and a Nonresident Senior Fellow at the Asia Pacific Foundation of Canada. His research focuses on India’s geoeconomics, such as how trade, technology, and climate change issues affect Indian foreign policy and what impact these policies have on Indo-Pacific security. He is the author of *Does India Negotiate?* (2020). He can be reached at <isaskn@nus.edu.sg>.

¹ “Cybersecurity in Asia Pacific: Rising Threats and GenAI Adoption,” PWC, Global Digital Trust Insights, May 29, 2024 ~ <https://www.pwc.com/gx/en/issues/cybersecurity/global-digital-trust-insights/asia-pacific.html>.

² Rieko Miki, “Quad Countries to Bolster Cyber Defense with Information-Sharing,” *Nikkei Asia*, April 25, 2023.

cybersecurity.³ China's tensions with countries such as India, Japan, and South Korea are acquiring a cyber dimension. In 2023 the U.S. government released a threat assessment that alleged Beijing was using cyber capabilities for espionage, malign influence, and information operations to advance Chinese views and interests. Such threats are generally increasing.⁴ Besides China, North Korea, and Russia, other states are backing various advanced persistent threats (APTs) to conduct cyberoperations.

Across the subregion, governments, private-sector firms, and other organizations have been targeted by sophisticated cyber campaigns to compromise computer systems and networks. Such APTs generally manifest through stealth attacks against critical targets in various countries. Vietnam, Indonesia, and India, for example, have suffered cyberattacks targeting government agencies, military establishments, financial institutions, and critical infrastructure.⁵ In 2023 the Asia-Pacific region experienced the highest surge in cyberattacks with an average of 1,835 per organization, above the global average of 1,250.⁶ Southeast Asia is experiencing a notable cybercrime epidemic, with malicious actors operating from there stealing approximately \$64 billion worldwide. Cybercrime has increased by 82% in Southeast Asia, and a recent report revealed that the region experienced 68 documented attacks out of 86 global APT campaigns in 2024.⁷

Prevailing cyberthreats are seldom restricted to state actors and boundaries, however. Some governments support cyberoperations through nonstate actors and “hacktivist” proxies. Online information operations to roil domestic politics during election campaigns are rising, for example. During Taiwan's 2024 presidential election, China allegedly conducted a “broad range of information operations” to attempt to tilt the outcome

³ Cybersecurity broadly refers to what countries, firms, and organizations do to protect their networks, systems, infrastructure, and data from attacks and unauthorized access. Dan Craigen, Nadia Diakun-Thibault, and Randy Purse, “Defining Cybersecurity,” *Technology Innovation Management Review* 4, no. 10 (2014): 13–21.

⁴ International Telecommunication Union Development Sector, *Global Cybersecurity Index 2020* (Geneva: International Telecommunication Union, 2021) ~ <https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E>.

⁵ 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>.

⁶ “Global Cyberattacks Continue to Rise with Africa and APAC Suffering Most,” Check Point Research, April 27, 2024 ~ <https://blog.checkpoint.com/research/global-cyberattacks-continue-to-rise>.

⁷ USIP Senior Study Group, “Transnational Crime in Southeast Asia: A Growing Threat to Global Peace and Security,” United States Institute of Peace, May 2024, 13.

in Beijing's favor.⁸ Disinformation pervaded the 2022 Philippine national election, with Marcos and Duterte deploying different narratives to gain an advantage.⁹ A potential hot war in Asia would likely have the features of a hybrid war, consisting of physical combat, information warfare, and cyberwarfare, compelling countries to draft cybersecurity strategies. The regional cyber landscape is fractious.

Most Asian countries are facing the need to renew and revamp their cyber architectures through concerted domestic action and international cooperation. Governments and firms can connect and integrate digitally to the extent they trust the network security of their partners. The Indo-Pacific is home to over half of the world's internet users, who are largely young and mobile; over 90% of these users access the internet through their phones.¹⁰ This teeming digital landscape is home to sectors and firms experiencing rapid growth.¹¹ Digital service exports of Asia-Pacific economies constituted nearly \$958 billion in 2022.¹² The brisk growth in digital trade, digital capital flows, and related cyber linkages across Asia render cybersecurity an essential task that government and nongovernmental actors must collectively pursue. The response must be comprehensive, involving domestic and international stakeholders to grasp and mitigate such threats. Achieving cyber resilience, however, requires a comprehensive approach that includes enhancing governance, risk management, data protection rules, and regional and international

⁸ Russell Hsiao, "A Preliminary Assessment of CCP Political Warfare in Taiwan's 2024 Elections," Global Taiwan Institute, Global Taiwan Brief 9, no. 1, January 10, 2024 ~ <https://globaltaiwan.org/issues/vol-9-issue-1>.

⁹ Aries A. Arugay and Maria Elize H. Mendoza, "Digital Autocratisation and Electoral Disinformation in the Philippines," *ISEAS Perspective*, no. 53 (2024) ~ https://www.iseas.edu.sg/wp-content/uploads/2024/06/ISEAS_Perspective_2024_53.pdf.

¹⁰ Trisha Ray et al., "The Digital Indo-Pacific: Regional Connectivity and Resilience," Observer Research Foundation, February 15, 2021 ~ <https://www.orfonline.org/research/the-digital-indo-pacific-regional-connectivity-and-resilience>.

¹¹ Digital growth is accelerating across the region. According to a study by the Boston Consulting Group, ASEAN's digital economy could be \$1 trillion by 2030 if current trends persist, and a recent McKinsey report claims that by 2025 India's digital economy could be worth \$350–\$440 billion. See "Study on the Asean Digital Economy Framework Agreement," Boston Consulting Group, October 21, 2023, 3 ~ https://asean.org/wp-content/uploads/2023/10/ASEAN-Digital-Economy-Framework-Agreement-Public-Summary_Final-published-version-1.pdf; and "Digital India: Technology to Transform a Connected Nation," McKinsey Global Institute, 2019, 1 ~ <https://www.mckinsey.com/~media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/digital%20india%20technology%20to%20transform%20a%20connected%20nation/mgi-digital-india-in-brief-april-2019.pdf>.

¹² Economic and Social Commission for Asia and the Pacific, UN Conference on Trade and Development, and UN Industrial Development Organization, *Asia-Pacific Trade and Investment Report 2023/24: Unleashing Digital Trade and Investment for Sustainable Development* (Geneva: United Nations, 2023) ~ <https://www.unescap.org/kp/APTIR2023>.

coordination, as well as constantly upgrading digital infrastructure.¹³ Cyber resilience is how countries resist, recover from, and adapt their digital infrastructure as a result of cyberthreats.

Developing Cyber Resilience in the Indo-Pacific

What is the state of cyber resilience in the Indo-Pacific? This question is pivotal to gauge how Asian countries can withstand cyber risks and vulnerabilities, recover rapidly, and adapt to better defend their digital infrastructure. Yet we lack an effective understanding and assessment of how specific Asian countries are dealing with cyberthreats domestically—i.e., instituting the necessary institutional changes to bolster their cyber capacities and capabilities. There is discernable variation in how countries deal with cybersecurity risks, with gaps between states on capacity and preparedness. We need to analyze cyber architectures across specific Indo-Pacific countries to ascertain how they fare concerning resilience, what specific aspects—resistance, recovery, or adaptation—they should focus on, and how they move toward that objective.

This roundtable shows that cyber resilience in the Indo-Pacific is checkered, characterized by progressive moves in regional countries to protect their cyberspace despite differences in how they manage and mitigate cyberthreats. These differences are a product of states' strategic circumstances that compel domestic changes to bolster cybersecurity. External pressures alone, however, are insufficient for this task; such pressures to improve cybersecurity must be backed and leveraged politically from within a state. Looking at India, Indonesia, Japan, and South Korea, we can see that all four countries have invested in building capacious and responsive institutions to monitor cyber incidents and have instilled the need to remain consultative and collaborative with domestic and international counterparts. In other words, all four countries have acquired sufficient capability to resist cyberattacks. However, differences exist

¹³ If cybersecurity is largely understood as the defense and protection of digital networks from cyberthreats and disruptions, it is generally accompanied by cyber resilience that has a wider systemic focus and covers institutions, measures, and protocols that countries institute to resist cyberattacks. Cyber resilience requires a strong focus on leadership, people, and process to make necessary adjustments in a fluid internet domain complicated with threats. Misael Sousa de Araujo, Bruna Aparecida Souza Machado, and Francisco Uchoa Passos, "Resilience in the Context of Cyber Security: A Review of the Fundamental Concepts and Relevance," in "Progress and Research in Cybersecurity and Data Privacy," ed. Chuanyi Liu et al., special issue, *Applied Sciences* 14, no. 5 (2024): 2116. See also Matthias Bossardt, "Cyber Resilience: Creating Competitive Advantages and Promoting Trust," KPMG, 2020 ~ <https://assets.kpmg.com/content/dam/kpmgsites/ch/pdf/blc-news-cyber-resilience.pdf.coredownload.inline.pdf>.

between the four countries in the other two pillars of resilience—recovery and adaptation. Japan and South Korea have made iterative changes to bolster their cybersecurity, largely driven by an imperative to deter growing cyberthreats, whereas India and Indonesia have yet to make that strategic choice, opting instead to manage and mitigate existing risks.

Japan and South Korea have crossed a threshold with robust cybersecurity strategies necessitated by a deteriorating regional security environment and interest in supporting a rules-based international order that remains congruent with the U.S.-led Indo-Pacific security logic. This inclination supports prioritizing recovery and adaptation to deter and mitigate cyberthreats. India and Indonesia have yet to reach this level largely due to different political and developmental logic driving cyber governance. Yet, this seemingly constrained state does not imply little regard to bolster cybersecurity. New Delhi and Jakarta are making domestic changes and forming strategic partnerships to address cyber vulnerabilities.

The essays in the roundtable, summarized in brief below, unpack how these four countries—India, Indonesia, Japan, and South Korea—fare on the three aspects of cyber resilience: resistance, recovery, and adaptation.

Arindrajit Basu argues that India has developed adequate institutional mechanisms to govern its cyberspace, beefing up its cyber incident response and recovery institutions and establishing partnerships on cyber activities with other countries. This institutional prioritization accompanies India’s “exposure to an increased number, range, and sophistication of cyberattacks.” Domestic coordination has increased between the government, private sector, and independent security analysts, raising awareness of cybersecurity issues. However, the lack of a coherent cybersecurity strategy impedes India’s ability to proactively deter cyberthreats and signal its intent as a credible and responsible cybersecurity stakeholder. Clarity will help the government achieve its cyber objectives as India’s digital economy becomes crucial to national security and prosperity. The stakes are high. India’s thriving digital trajectory in an insecure and polarized neighborhood depends on getting cybersecurity right.

Gatra Priyandita claims that Indonesia’s cybersecurity landscape will be tested as “cyber-enabled threats rise.” While Indonesia has acquired a sufficient capacity to resist cyber-enabled threats, it struggles to recover and adapt, leaving its cyberspace vulnerable to exploitation online. Jakarta lacks effective institutional mechanisms to govern Indonesian cyberspace, especially when recovering from cyberattacks. Indonesia’s challenges, however, could be remedied by allocating more resources to cyberdefense

and situating cyber laws and rules in a robust institutional framework that supports cybersecurity. The absence of a national cybersecurity law creates a vacuum that leaves the country's key cyber institution, the Badan Siber dan Sandi Negara (National Cyber and Crypto Agency), particularly vulnerable to political shifts and policy uncertainty that undermine effective cyber "governance, enforcement, and resource allocation." That said, Jakarta is prioritizing international cooperation on cyber affairs, recognizing that the dynamic and transnational nature of risks encourage new forms of collaboration, capacity building, and diplomacy, particularly on issues such as cyber terrorism.

Dai Mochinaga argues that Japan has considerably upgraded its domestic cyber architecture and posture in recent years. The country's trajectory from a largely defensive cyber actor to a constructive and proactive cyber stakeholder has been driven by domestic political pressure, national security considerations, demands to protect civilian infrastructure, and adaptable cyberthreats. Tokyo's active cyberdefense approach in its 2022 National Security Strategy signifies a fundamental shift, bringing Japan closer to the U.S. cyberdefense approach. However, this shift in Japan's cybersecurity architecture also arrives with "significant organizational and budgetary changes," which raises thorny implementation quandaries, given the proliferation of actors involved in cyberdefense. These trade-offs must be overcome to ensure that Japan's cyber posture remains fit for purpose as threats mount. As well, Japan must sustain progress to successfully defend itself against cyberthreats, with or without sufficient U.S. pressure. Tokyo must also balance this ostensibly assertive cyber posture with international norms and its desire to uphold the international rules-based order.

Finally, Dongyoun Cho argues that a robust cybersecurity approach enables South Korea to resist, recover, and adapt to imminent and evolving cyberthreats. A challenging cyber landscape—characterized by persistent attacks from China, North Korea, and Russia—has compelled South Korean officials to institute an ambitious and comprehensive cybersecurity strategy that emphasizes efficient incident response mechanisms and international cyber partnerships to bolster resilience. However, as Cho highlights, a critical issue lies in South Korea's fragmented governance model, which is built on a patchwork of sector-specific laws that address information protection and cyberdefense across the government, civil, and military domains. While this approach allows for tailored regulations for specific sectors—such as public institutions, telecommunications, critical infrastructure, finance, military, high-tech industries, healthcare, and small and medium-sized


enterprises—it lacks a unified and comprehensive foundational law. This gap hinders the creation of a cohesive national cybersecurity strategy and impedes cross-sectoral coordination. Cho cautions that progress cannot be taken for granted in an increasingly interconnected and vulnerable digital world, underscoring the urgency of addressing these governance challenges to achieve cyber resilience.

The four Indo-Pacific countries featured in this roundtable—India, Indonesia, Japan, and South Korea—are independently and jointly working to strengthen cybersecurity and cyber resilience. Institutional changes have occurred. Investments are largely increasing to improve cybersecurity. Laws and regulations governing cyberspace are being passed or considered. All four governments are working with international partners to bolster their cyber capacities. Resistance has improved across the four countries, but differences remain in their capabilities for recovery and adaptation, constrained by domestic political and strategic forces. The critical factor that significantly and decisively shapes the pivot toward greater cyber resilience is embedding the recovery and adaptation dimensions into a strategic paradigm that optimizes defensive measures with sufficient offensive capabilities in an increasingly hostile cyber landscape.

This decision, however, is not shaped by cybersecurity pressures alone but also by underlying strategic motivations. Japan's and South Korea's push to transform their cyber strategies and align them with the U.S. regional deterrence strategy enables Seoul and Tokyo to manage and deter cyber risks. That said, they must also ensure that adequate institutional space exists to pivot their strategies as emergent threats surface. Given diplomatic traditions that prize autonomy and space, India and Indonesia will likely resist announcing their cybersecurity strategies. While New Delhi and Jakarta have made incremental and profound changes to their cybersecurity postures, constraints that manifest through institutional gaps, resources, and strategy could limit their capabilities to mitigate and recover from extant threats. Yet their amenable attitude toward strategic cyber partnerships could help address gaps in threat perceptions, acquire information on cyberattacks and hostile actors, and neutralize them.

This roundtable suggests that the regional cybersecurity context appears fluid with intense security competition intersecting with digitalization. The digital space, in effect, becomes an arena, tool, and weapon through which countries jostle for greater influence and balance in the Indo-Pacific. However, there is no silver bullet for these and other Asian countries to manage and mitigate cyberthreats. Digitalization will only accelerate.

Emerging technologies such as artificial intelligence and quantum computing could both help address and further complicate cybersecurity.

While defending against cyberthreats, states must prioritize resistance and recovery and double down on adaptation or measures to protect digital infrastructures over the long term. This can happen through domestic coordination and international cyber cooperation, helping countries fill gaps and information asymmetries when cyber disruptions occur. The four countries featured in this roundtable have extensive and proliferating international cyber partnerships. It will be important to sustain these over time. 

India's Cyber Resilience: Strategy, Financing, and Collaboration

Arindrajit Basu

Increased digitization coupled with a vexed geopolitical location amid difficult neighbors has led India to face an increasing number of security threats in the cyber realm.¹ To respond, India has made important strides on building resilience by establishing cybersecurity agencies and institutions, allocating funding to these institutions, and fermenting collaborations with international counterparts and domestic stakeholders. Yet given its vast size and broad demographics, developing appropriate skills among the workforce that deals with cyber infrastructure remains a challenge and vulnerability.

India's holistic and proactive approach to cybersecurity resilience fares well vis-à-vis resistance, recovery, and adaptation. In particular, India has recently amped up its long-term cybersecurity vision to improve its adaptation abilities, upgrading its approach to account for an increased range and volume of cyberthreats from domestic and international actors. Notwithstanding these improvements, however, India's cyber institutions remain hamstrung by an overarching reticence to be publicly open about their functioning, collaboration with other stakeholders, and broader strategic approach.

This essay argues that this lack of clarity has dampened India's efforts when it comes to the three prongs of resistance, recovery, and adaptation. While ambiguity may serve India's strategic interests in limited cases in dealing with a rapidly evolving and dynamic global landscape, it weakens the country's progress on cyber resilience in other respects. The essay begins with a broad overview of the cyberthreat landscape in India. Subsequently, it details the national strategies and institutions set up to resist these cyberthreats and then highlights the incident-response and reporting mechanisms that enable India's cyber institutions to recover from such incidents. Finally, the essay analyzes the long-term strategies—financing,

ARINDRAJIT BASU is a PhD Candidate at Leiden University (the Netherlands). He can be reached at <a.basu@fgga.leidenuniv.nl>.

NOTE: The author would like to thank Karthik Nachiappan for patient and incisive edits and review on iterations of this essay, Karan Saini for discussions, and Sandeep Bharadwaj and Anuradha Rao for astute feedback as discussant and session chair, respectively, at the authors' workshop.

¹ Sameer Patil, *Securing India in the Cyber Era* (New Delhi: Routledge, 2022), 1–5.

multi-stakeholder partnerships, and international collaboration—that enable India to adapt to a complex geopolitical environment where cyber risk is a reality.

An Overview of Cyberthreats Faced by India

India has received an increasing number of cyberattacks every year: Check Point Research found that it experienced a 46% year-on-year increase in cyberattacks in the second quarter of 2024.² India faced the second-highest number of weekly national attacks in the Asia-Pacific region during this period, behind only Taiwan.³ A number of these cyberattacks are allegedly state-sponsored; India is among the top three countries in the world targeted by nation-state-based actors, according to a 2023 Microsoft report.⁴

Critical infrastructure has often been the target of cyberattacks. Notable incidents include the D-Track malware attack that penetrated Kudankulam Nuclear Power Plant’s administrative network in 2019 and the IT network disruption of the All India Institute of Medical Sciences, one of India’s leading government-run hospitals in 2022.⁵ Critical infrastructure aside, cybersecurity research firm Sophos found that nearly 64% of Indian organizations were targeted by ransomware attacks in 2023.⁶ And beyond cyberattacks, Indian users—senior citizens, in particular—have been victims of financial fraud perpetrated by malicious actors exploiting a lack of user awareness.⁷

² “India Records Second Highest Weekly Attacks per Organisation in APAC at 3201, Second Only to Taiwan: Check Point Research,” CRN, July 18, 2024 [~ https://www.crn.in/news/india-records-second-highest-weekly-attacks-per-organisation-in-apac-at-3201-second-only-to-taiwan-check-point-research](https://www.crn.in/news/india-records-second-highest-weekly-attacks-per-organisation-in-apac-at-3201-second-only-to-taiwan-check-point-research).

³ Ibid.

⁴ “India Amongst Top Three Most Targeted APAC Countries as AI Use, Ransomware Increases: Report,” *Hindu*, October 7, 2023 [~ https://www.thehindu.com/sci-tech/technology/india-amongst-top-three-most-targeted-apac-countries-use-ai-ransomware-increase-report/article67391822.ece](https://www.thehindu.com/sci-tech/technology/india-amongst-top-three-most-targeted-apac-countries-use-ai-ransomware-increase-report/article67391822.ece).

⁵ Melissa Robbins, “Cyberattack Hits Indian Nuclear Plant,” *Arms Control Today*, December 2019 [~ https://www.armscontrol.org/act/2019-12/news/cyberattack-hits-indian-nuclear-plant](https://www.armscontrol.org/act/2019-12/news/cyberattack-hits-indian-nuclear-plant); and Aashish Aryan, “AIIMS Cyber Attack Took Place Due to Improper Networks Segmentation: Govt in RS,” *Economic Times*, February 10, 2023 [~ https://economictimes.indiatimes.com/tech/technology/aiims-cyber-attack-took-place-due-to-improper-networksegmentation-govt-in-rs/articleshow/97805598.cms?from=mdr](https://economictimes.indiatimes.com/tech/technology/aiims-cyber-attack-took-place-due-to-improper-networksegmentation-govt-in-rs/articleshow/97805598.cms?from=mdr).

⁶ “Significant Percentage of Indian Firms Hit by Ransomware in 2023: Report,” *Business Standard*, May 14, 2024 [~ https://www.business-standard.com/industry/news/significant-percentage-of-indian-firms-hit-by-ransomware-in-2023-report-124051400646_1.html](https://www.business-standard.com/industry/news/significant-percentage-of-indian-firms-hit-by-ransomware-in-2023-report-124051400646_1.html).

⁷ “FBI Report Ranks India in Top 5 Countries with Victims of Cybercrimes,” *Mint*, May 30, 2022 [~ https://www.livemint.com/technology/tech-news/fbi-report-ranks-india-in-top-5-countries-with-victims-of-cybercrimes-11653896623002.html](https://www.livemint.com/technology/tech-news/fbi-report-ranks-india-in-top-5-countries-with-victims-of-cybercrimes-11653896623002.html).

India's exposure to an increasing number, range, and sophistication of cyberattacks necessitates a nuanced approach to cyber resilience that increases cybersecurity awareness among individual users while simultaneously shoring up infrastructural hardiness and strategic thinking in both government institutions and the private sector. The remainder of this essay evaluates the extent to which India has stepped up to address this complex challenge.

Resist: Cybersecurity Strategy and Institutions

The first step toward cyber resilience is putting a cyber strategy in place and establishing cyber institutions. This section assesses India's performance on both counts.

Strategy. In June 2013 the Department of Electronics and Information Technology (now the Ministry of Electronics and Information Technology, or MeitY) released India's National Cyber Security Policy.⁸ No publicly available national cyber strategy has been published since. The policy itself is quite high-level, presenting a range of broad strategies and objectives that India should adopt to secure its cyberspace.⁹ Although the objectives and strategies are well-conceived, they are outdated given the advances in emerging technologies such as artificial intelligence and the increase in the frequency and range of cyberattacks targeting the country. That said, the 2013 policy recommended the establishment of the National Critical Information Infrastructure Protection Centre (NCIIPC), which was established the same year.¹⁰ However, many high-level recommendations in the strategy have not been implemented due to capacity constraints and difficulties with cohesion and coordination among the various stakeholders and institutions inside and outside government.¹¹

⁸ Ministry of Electronics and Information Technology (India), *National Cyber Security Policy* (New Delhi, 2013) ≈ https://www.meity.gov.in/writereaddata/files/downloads/National_cyber_security_policy-2013%281%29.pdf.

⁹ These objectives include creating a secure cyber ecosystem, creating an assurance framework, encouraging opening standards, strengthening the regulatory framework, creating mechanisms for security threat early-warning, managing vulnerabilities and responses to security threats, securing e-governance services, protecting critical information infrastructure, promoting research and development in cybersecurity, reducing supply chain risks, creating cybersecurity awareness, developing effective public-private partnerships, and information sharing and cooperation among various entities.

¹⁰ See National Critical Information Infrastructure Protection Centre ≈ <https://nciipc.gov.in>.

¹¹ Hannes Ebert, "Hacked IT Superpower: How India Secures Its Cyberspace as a Rising Digital Democracy," *India Review* 19, no. 4 (2020): 376–413 ≈ <https://www.tandfonline.com/doi/full/10.1080/14736489.2020.1797317>.

In 2019 the National Security Council Secretariat, which falls within the Prime Minister's Office, set up a task force to develop a new national cybersecurity strategy.¹² It also hosted an open consultation with requests for comments on three prongs: (1) strengthening national cyberspace, (2) strengthening structures, people, processes, and capabilities, and (3) synergizing resources, including through cooperation and collaboration.

Notwithstanding several reports hinting that the strategy will be released "soon," the text has not yet been made public.¹³ However, key stakeholders in the public and private sector have seen various drafts and are purportedly already implementing its 81 deliverables in their daily functioning,¹⁴ although no entity has publicly commented yet on how it is implementing this strategy. Why this much-needed update to the 2013 policy has not yet been published remains unclear.

Meanwhile, in 2024 the Indian Army released a Joint Doctrine for Cyberspace Operations that "lays emphasis on understanding military aspects of cyberspace operations and provides conceptual guidance to commanders, staff and practitioners in the planning, and conduct of operations in cyberspace, as also to raise awareness in our warfighters at all levels."¹⁵ Although the doctrine has also not yet been published online, the press release suggests that it will guide both offensive and defensive aspects of the military's role in cyberspace.¹⁶

The overarching reticence to publish and clearly articulate a national cyber strategy reflects India's long-standing approach to grand strategy that has generally evaded public articulation or justification. Scholars who defend this approach stress that strategic thinking and strategic culture do not necessarily need to be articulated in one location to cohesively and rationally shape national decision-making.¹⁷ Others believe that anchoring

¹² Aditi Agrawal, "National Security Council Invites Comments on National Cyber Security Strategy until Dec 31," MediaNama, December 2, 2019 ~ <https://www.medianama.com/2019/12/223-national-cyber-security-strategy-comments-invite>.

¹³ Nadeem Inamdar, "National Cyber Security Strategy to Be Released Soon," *Hindustan Times*, June 13, 2023 ~ <https://www.hindustantimes.com/cities/pune-news/national-cyber-security-strategy-2023-to-be-released-soon-101686596627065.html>.

¹⁴ Information obtained from a roundtable in New Delhi on March 2, 2023, organized under the Chatham House Rule.

¹⁵ "CDS Gen Anil Chauhan Releases Joint Doctrine for Cyberspace Operations," Ministry of Defence (India), Press Release, June 18, 2024 ~ <https://pib.gov.in/PressReleasePage.aspx?PRID=2026240>.

¹⁶ Ibid.

¹⁷ Ashley J. Tellis, "Between the Times: India's Predicaments and Its Grand Strategy," Carnegie Endowment for International Peace, December 3, 2012 ~ <https://carnegieendowment.org/posts/2012/12/between-the-times-indias-predicaments-and-its-grand-strategy?lang=en>; and Dhruva Jaishankar, *Vishwa Shastra: India and the World* (Gurugram: Penguin Random House India, 2024), 12.

New Delhi's policy thinking in a regularly issued and publicly available national security strategy would enable India to comprehensively take stock of the country's threats and opportunities, provide an established framework for long-term planning, and serve as a signaling instrument to both allies and adversaries.¹⁸

The lack of a single, publicly available document does not indicate an absence of institutions, legislation, and other documents that help us evaluate India's overarching approach to cyberspace. That said, clear and confident normative articulation in an overarching strategy that is compiled with inputs from the broad array of governing institutions would provide clarity to stakeholders and underscore India's global reputation as a responsible cyberpower.

Legislation. India's domestic legislative framework governing cybersecurity is captured in the Information Technology (IT) Act that was originally passed in 2002 and has since been amended several times. The legislation imposes monetary penalties for several offences related to computer infrastructure or resources. Covered offences include unauthorized access, unauthorized downloads, introduction of a computer contaminant, damage, and denial of access.¹⁹ The act also criminalizes several behaviors such as tampering with source-code documents, impersonation using a computer resource, and cyberterrorism, which includes the denial of access to computer resources that threatens the unity, integrity, or sovereignty of India.²⁰ India is now deliberating a fresh Digital India Act that would replace the IT Act and bring legislation in line with contemporary technological and political developments.²¹

Institutions. India's cybersecurity ecosystem is fronted by a plethora of institutions across key ministries, including the Prime Minister's Office, MeitY, the Ministry of Defence, and the Ministry of

¹⁸ Arzan Tarapore, "India Needs the Anchor of a National Security Strategy," *Hindu*, June 26, 2024 ~ <https://www.thehindu.com/opinion/op-ed/india-needs-the-anchor-of-a-national-security-strategy/article68332647.ece>.

¹⁹ *The Information Technology Act, 2000*, Government of India, October 17, 2000, section 43 ~ <https://www.indiacode.nic.in/handle/123456789/1999>.

²⁰ *Ibid.*, section 66.

²¹ Durga Priya Manda and Anant Narayan Misra, "Report: India to Replace Information Technology Act with the Proposed Digital India Act: Out with the Old, In with the New?" *Global Privacy Law Review* 5, no. 1 (2024): 50–53 ~ <https://kluwerlawonline.com/journalarticle/Global+Privacy+Law+Review/5.1/GPLR2024002>.

Home Affairs.²² The establishment in 2015 of the Office of the National Cybersecurity Coordinator that advises the Prime Minister's Office and National Security Advisor on cybersecurity matters was a much needed recognition of cyber resilience as a key national security and strategic priority. Additionally, the two subministerial-level institutions most significantly involved with incident response and recovery are India's Computer Emergency Response Team (CERT-In) and the NCIIPC. CERT-In, which falls within MeitY's remit, has been statutorily designated under Section 70B of the IT Act as the national agency in charge of incident response for all systems except those in sectors identified as critical infrastructure.²³ The NCIIPC, which is structured within the Prime Minister's Office, is responsible for sectors that can be considered critical infrastructure and their incident responses.²⁴

In the past decade, the burgeoning of institutions tasked with handling various aspects of cyber resilience emphasizes the increasing relevance of the cyber domain in India's strategic thinking. As the next sections demonstrate, these institutions have improved in their overall effectiveness but would do better with greater transparency and communication when responding to cyber incidents.

Recovery: Incident-Response and Reporting Mechanisms

CERT-In and the NCIIPC are the institutions working at the forefront of incidence recovery and response. Given its role as India's nodal cyber response agency, CERT-In functions 24 hours a day, and in 2023 handled 1,592,917 incidents.²⁵ The team issued a detailed set of guidelines in 2022 specifying the modalities of reporting cyber incidents, along with a

²² For a detailed overview and summary of India's cyber institutions, see Gunjan Chawla, "The Architecture of Cybersecurity Institutions in India," MediaNama, February 19, 2020 \approx <https://www.medianama.com/2020/02/223-architecture-cybersecurity-institutions-india-structure/>; Hannes Ebert, Kate Saslow, and Thorsten Wezling, "Cyber Resilience and Diplomacy in India," EU Cyber Direct, Digital Dialogue, July 2020; and Arindrajit Basu and Bharat Gurugavendran, "Unveiling India's Cyber Strategy: Navigating International Law and Indian State Practice on Security Operations," in *Cybersecurity Governance and Normative Frameworks: Non-Western Countries and International Organizations Perspectives*, ed. Pietro Garguio, Davide Giovannelli, and Annita Larissa Sciacovelli (Napoli: Editoriale Scientifica, 2024), 67–109.

²³ *The Information Technology Act, 2000*, section 70B.

²⁴ Arindrajit Basu, "India's International Cyber Operations: Tracing National Doctrine and Capabilities," UN Institute for Disarmament Research, December 2022 \approx <https://unidir.org/publication/indias-international-cyber-operations-tracing-national-doctrine-and-capabilities>. Following the procedure laid out in Section 70A of the IT Act, the NCIIPC has so far identified power, energy, banking, health, financial services, insurance, telecom, transport, government, and strategic and public enterprises as critical information infrastructure.

²⁵ Indian Computer Emergency Response Team (CERT-In), "Annual Report 2023," 2023.

well-conceived template that organizations can use to provide the most relevant information when reporting an incident.²⁶ The guidelines specify that a point of contact must be set up to liaise with CERT-In, and they cover twenty specific types of incidents to be reported within the first six hours, including port or vulnerability scans, reconnaissance incidents, malware, data leaks, and distributed denial-of-service attacks. Some aspects of the reporting rules have been criticized by private-sector stakeholders and security experts for being too cumbersome and undermining the security needs of organizations.²⁷

The NCIIPC, which deals with critical infrastructure sectors, has also issued a standard operating procedure for managing incident responses.²⁸ The procedure outlines several steps integral to any incident-response process, including composition of the incident-response team, the reporting process, incident mitigation, and the dissemination of information.

Notwithstanding these detailed guidelines that aid vulnerability reporting and guide incident responses, the specifics of both institutions' responses to reported incidents are not disclosed to the public or even to the individual that reports the event. While some incidents may warrant secrecy due to the sensitive nature of the information involved, greater transparency and communication with a select community of security researchers and experts would strengthen India's understanding and prediction of the cyberthreat landscape.

²⁶ CERT-In has also established a responsible vulnerability disclosure and coordination policy specifying contact details for reporting vulnerabilities. For information on security practices, procedures, prevention, response, and reporting of cyber incidents for safe and trusted internet, see *The Information Technology Act, 2000*, section 70B(6).

²⁷ Cybersecurity experts have complained that the six-hour window to report incidents, which is not in line with global standards, provides companies very little time to effectively evaluate the incident. They have also expressed dissatisfaction with the requirement to log all information on their systems for 180 days, which could serve as a honeypot opportunity for threat actors; the broad definition of reportable incidents, including probing and scanning; and the financial stress on private-sector organizations to comply with these guidelines. See Sarvesh M, "Why India's New Cybersecurity Directive Is a Bad Joke," *MediaNama*, May 5, 2022 ~ <https://www.medianama.com/2022/05/223-cert-cybersecurity-directions-are-a-joke-3/>; Sarvesh M, "India's Cybersecurity Directive Goes Against Security, Tech Companies Argue," *MediaNama*, May 9, 2022 ~ <https://www.medianama.com/2022/05/223-iti-letter-cert-cybersecurity-directive-2/>; and Neeti Biyani et al., "India CERT-IN Cybersecurity Directions 2022," *Internet Society*, Internet Impact Brief, June 1, 2022 ~ <https://www.internetsociety.org/resources/doc/2022/internet-impact-brief-india-cert-in-cybersecurity-directions-2022>.

²⁸ "Standard Operating Procedure," National Critical Information Infrastructure Protection Centre (India), June 2017 ~ <https://tneb.tnebnet.org/cyber/csntan/SOPIncidentResponse.pdf>.


Adapting: Financing and Collaboration

Financing. India's cybersecurity institutions and projects are largely financed through the central budget (also known as the union budget). However, some states, like Karnataka, have also allocated a specific budget to cybersecurity to implement state-level cyber initiatives focused on building capacity and raising awareness.²⁹

The lion's share of cybersecurity funding in the union budget is received by MeitY. As **Table 1** demonstrates, the funding allocated to cyber institutions and cybersecurity-related projects has been steadily rising. The budget allocated to CERT-In, for example, rose sharply from 420 million rupees (\$5.0 million) in 2018–19 to 2,160 million rupees (\$25.7 million) in 2020–21 and has stayed in that range since then. The amount allocated to other cybersecurity projects, including to the National Cyber Crime Coordination Centre, has increased steadily from 4,000 million rupees in 2023–24 to 7,590 million rupees in the budget for 2024–25. The National Cyber Coordination Centre was also established under MeitY to provide a macroscopic view of cyberthreats and generate situational awareness.³⁰ The union budget additionally provided 415,860 million rupees to set up the Indian Cyber Crime Coordination Centre to serve as the nodal entity on cybercrime under the Ministry of Home Affairs.

The government also funds cybersecurity research and development. The Centre for the Development of Advanced Computing (C-DAC), a part of MeitY, has always received a significant budget allocation—2,700 million rupees in the 2024–25 budget. This allocation indicates the government's desire not only to respond to cyber incidents but also to proactively undertake advanced research that can improve the country's response capabilities. C-DAC undertakes R&D on a range of cutting-edge technology fronts, including high-performance computing, software technology, and health informatics.³¹ In addition to funding specific institutions, the central government also funds specific deliverables such as cybercrime prevention against children and women, which was allocated 528.5 million rupees in the 2024–25 budget.

The increased budgetary allocation to cybersecurity acknowledges the augmented cyber risk that India's institutions must deal with and reaffirms

²⁹ Sharveya Parasnis, "Karnataka Unveils Cyber Security Policy with ₹100 Crore Budget," MediaNama, August 5, 2024  <https://www.medianama.com/2024/08/223-karnataka-unveils-cyber-security-policy-with-%E2%82%B9100-crore>.

³⁰ CERT-In, "Annual Report 2023."

³¹ Centre for Development of Advanced Computing (India)  <https://www.cdac.in>.


TABLE 1

Yearly Budget Allocations for Cybersecurity Institutions, 2018–25

Budget head and department/ ministry	2019–20	2020–21	2021–22
CERT-In <i>MeitY</i>	Budget • 420.0 million rupees (\$5.0 million) Revised • 350.0 million rupees (\$4.2 million) Actual • 299.8 million rupees (\$3.6 million)	Budget • 1,400.0 million rupees (\$16.7 million) Revised • 900.0 million rupees (\$10.7 million)	Budget • 2,160.0 million rupees (\$25.7 million) Revised • 2,133.0 million rupees (\$25.4 million) Actual • 1,936.9 million rupees (\$23.1 million)
Cybersecurity projects (National Cyber Coordination Centre and others) <i>MeitY</i>	Budget • 1,200.0 million rupees (\$14.3 million) Revised • 1,020.0 million rupees (\$12.2 million) Actual • 927.0 million rupees (\$11.0 million)	Budget • 1,700.0 million rupees (\$20.3 million) Revised • 800.0 million rupees (\$9.5 million) Actual • 3,105.1 million rupees (\$37.0 million)	Budget • 2,000.0 million rupees (\$23.8 million) Revised • 3,390.0 million rupees (\$40.4 million) Actual • 3,105.1 million rupees (\$37.0 million)
Indian Cyber Crime Coordination Centre <i>Police (Ministry of Home Affairs)</i>	Budget • 1,000.0 million rupees (\$11.9 million) Actual • 7.0 million rupees (\$0.8 million)	Budget • 798.0 million rupees (\$9.5 million) Revised • 440.0 million rupees (\$5.2 million) Actual • 5.9 million rupees (\$0.7 million)	Budget • 698.0 million rupees (\$8.2 million) Actual • 11.1 million rupees (\$0.1 million)

Table 1 continued

Budget head and department/ ministry	2022–23	2023–24	2024–25
CERT-In <i>MeitY</i>	Budget <ul style="list-style-type: none"> • 2,150.0 million rupees (\$25.6 million) Revised <ul style="list-style-type: none"> • 1,800.0 million rupees (\$21.4 million) Actual <ul style="list-style-type: none"> • 1,765.0 million rupees (\$21.0 million) 	Budget <ul style="list-style-type: none"> • 1,355.0 million rupees (\$16.1 million) Revised <ul style="list-style-type: none"> • 2,080.0 million rupees (\$24.8 million) 	Interim budget* <ul style="list-style-type: none"> • 2,400.0 million rupees (\$28.9 million) Final budget <ul style="list-style-type: none"> • 2,380.0 million rupees (\$28.3 million)
Cybersecurity projects (National Cyber Coordination Centre and others) <i>MeitY</i>	Budget <ul style="list-style-type: none"> • 3,000.0 million rupees (\$35.8 million) Revised <ul style="list-style-type: none"> • 1,000.0 million rupees (\$11.9 million) Actual <ul style="list-style-type: none"> • 301.1 million rupees (\$3.6 million) 	Budget <ul style="list-style-type: none"> • 4,000.0 million rupees (\$47.7 million) Revised <ul style="list-style-type: none"> • 4,000.0 million rupees (\$47.7 million) 	Interim budget* <ul style="list-style-type: none"> • 7,590.0 million rupees (\$90.5 million) Final budget <ul style="list-style-type: none"> • 7,590.0 million rupees (\$90.5 million)
Indian Cyber Crime Coordination Centre <i>Police (Ministry of Home Affairs)</i>	Budget <ul style="list-style-type: none"> • 590.0 million rupees (\$7.0 million) Revised <ul style="list-style-type: none"> • 250.0 million rupees (\$3.0 million) Actual <ul style="list-style-type: none"> • 188.0 million rupees (\$1.0 million) 	Budget <ul style="list-style-type: none"> • 940.0 million rupees (\$11.2 million) Revised <ul style="list-style-type: none"> • 869.4 million rupees (\$10.4 million) 	Not allocated

Source: Author's own compilation from union budget documents. See "Union Budget," Government of India  https://www.indiabudget.gov.in/previous_union_budget.php.

Note: The revised amount denotes a midyear review of the original amount provided in the annual budget. The actual amount denotes the actual amount spent. Asterisk indicates that, as the Indian general elections were held in May 2024, an interim budget was published in February 2024 and a final budget was published in July 2024 after the elections.

New Delhi's commitment to all aspects of cyber resilience, including response, mitigation, training, and research. Historically, there was a significant gap between the amount allocated and the amount utilized, which merits further investigation. However, the past financial year appears to have bucked this trend, with 79% of the allocated budget for cybersecurity projects being utilized.³² That said, published financial statements and public scrutiny would help prevent underutilization or misutilization in the future and promote accountable expenditure and allocation.

Engagement between cyber institutions and external stakeholders. The 2013 National Cyber Security Policy formally recognized the importance of public-private partnerships on cybersecurity issues and established a joint working group to serve as a platform for information sharing. The group later drafted holistic and specific recommendations for private-public collaboration. However, initial hesitation to share threat intelligence among government institutions stemming from a lack of institutional trust between the government and the private sector largely stymied the implementation of these proposals.³³

This trust deficit has been significantly reduced in the past ten years as cyber institutions began to collaborate more holistically with the private sector. CERT-In, for example, regularly participates in and organizes joint drills with private-sector firms. The institution has conducted cybersecurity exercises across several private-sector organizations as well as government departments, including in the finance, space, and oil sectors, to evaluate their ability to withstand cyberattacks.³⁴ CERT-In has also operationalized its own platform, the Threat Intelligence eXchange, to share enhanced intelligence on cyberthreats with a range of stakeholders.³⁵

In a departure from past reticence,³⁶ both the NCIIPC and CERT-In have started engaging more proactively with the security research community, including researchers working in security firms as well as independent researchers, to detect and disclose vulnerabilities in

³² Aditi Agrawal, "Reported Cybersecurity Incidents in Banking Sector Fell by 81% between 2021 and 2023: MoS," *Hindustan Times*, December 19, 2024 ~ <https://www.hindustantimes.com/india-news/reported-cybersecurity-incidents-in-banking-sector-fell-by-81-between-2021-and-2023-mos-101734595556314.html>.

³³ Ebert, "Hacked IT Superpower."

³⁴ CERT-In, "Annual Report 2023."

³⁵ *Ibid.*

³⁶ Karan Saini, Pranesh Prakash, and Elonnai Hickok, "Improving the Processes for Disclosing Security Vulnerabilities to Government Entities in India," Centre for Internet and Society, Policy Brief, March 2019.

existing software.³⁷ They have also organized joint closed-door workshops involving cyber institutions and security researchers from the private sector and offered incentives, such as rewards and recognition for researchers that report vulnerabilities.³⁸

Apart from reaching out to researchers, CERT-In has also started entering into memoranda of understanding (MoUs) with private-sector firms. Utilizing private-sector expertise to shore up institutional capacity is in line with global best practices and likely to enhance the overall cybersecurity awareness of individuals in both the public and private sectors. In 2024, CERT-In announced separate MoUs with Mastercard and Google Cloud to promote cooperation, information sharing, joint research, and capacity building in both the public and private sectors.³⁹

Coordination with international counterparts. Cybersecurity is a crucial strategic and diplomatic priority for India. This focus has led to a range of specific coordination mechanisms involving Indian cyber institutions with those of other states. First, the government, usually led by the National Cyber Security Coordinator, participates in a recurring strategic dialogue with a range of international partners that includes Australia, Japan, the United Kingdom, and the United States (i.e., the four Quad countries and the UK). At the minilateral level, the Quad Senior Cyber Group, which was established through the 2021 Quad Leaders Declaration, allows India to engage with its Quad counterparts on several cyber initiatives, such as the Joint Principles on Secure Software, Cybersecurity of Critical Infrastructure, and Supply Chain Resilience and Security.⁴⁰ Although these engagements have manifested in plans to solidify outcomes among the Quad partners, such as CERT-CERT cooperation and information sharing,⁴¹ specific instances of this cooperation remain unclear as no updates have been made public. India is also a member of other international groupings that address

³⁷ Author's telephone interview with Karan Saini, August 2, 2024.

³⁸ Ibid.

³⁹ "Google Cloud Partners with CERT-In to Train Govt Officials in Cybersecurity Skills," *Hindu*, September 7, 2024 ~ <https://www.thehindu.com/sci-tech/technology/internet/google-cloud-partners-cert-in-train-govt-officials-cybersecurity/article67280680.ece>; and Rajeswari Pillai Rajagopalan, "The Growing Tech Focus of the Quad," *Diplomat*, July 9, 2022 ~ <https://thediplomat.com/2022/07/the-growing-tech-focus-of-the-quad>.

⁴⁰ "Joint Press Release of the Quad Senior Cyber Group," Ministry of External Affairs (India), December 15, 2023 ~ https://www.mea.gov.in/press-releases.htm?dtl/37462/Joint_Press_Release_of_the_Quad_Senior_Cyber_Group.

⁴¹ "Quad Senior Cyber Group Joint Cybersecurity Statement," University of California Santa Barbara, American Presidency Project, February 2, 2023 ~ <https://www.presidency.ucsb.edu/documents/quad-senior-cyber-group-joint-cybersecurity-statement>.

cyber issues, such as the U.S.-led International Counter Ransomware Initiative that aims to build collective resilience on ransomware.⁴²

CERT-In is a member of the global Forum of Incident Response Teams (FIRST) and an accredited member of the Task Force for Computer Security Incident Response Teams/Trusted Introducer. FIRST is the premier global organization promoting cooperation among national incident response teams.⁴³ At the regional level, CERT-In is also a member of the Asia-Pacific CERT and chairs its Information of Things working group.⁴⁴

Building on the high-level cooperation at the political and macro-strategic level, CERT-In undertakes several joint activities with its counterparts. CERT-In also participates in and organizes cybersecurity exercises that foster participation with other national CERTs as well as the private sector. One example of this was the Synergy Exercise organized by CERT-In in 2022.⁴⁵ This exercise, organized in collaboration with the Cyber Security Agency of Singapore, involved thirteen countries as part of the Counter Ransomware Initiative.⁴⁶ CERT-In also conducted a G-20 cybersecurity exercise and drill during India's G-20 presidency in 2023.⁴⁷

CERT-In has entered into MoUs with the CERTs of other countries to share information regarding cyberthreats and respond collaboratively to cyber incidents. In 2023, CERT-In signed MoUs with the Egyptian CERT and the National Cyber Security Centre of the United Kingdom.⁴⁸ A long-standing MoU was signed between CERT-In and its U.S. counterpart in 2017, building on a 2011 MoU signed between the two governments to cooperate on cyber issues.⁴⁹

India's diverse cybersecurity partnerships are a product of both existing security cooperation architecture brokered by the political leadership and autonomous initiatives led by cyber-specific institutions such as CERT-In.

⁴² International Counter Ransomware Initiative ~ <https://counter-ransomware.org>.

⁴³ Forum of Incident Response and Security Teams (FIRST) ~ <https://www.first.org>.

⁴⁴ "Client's/Citizen's Charter," CERT-In ~ <https://www.cert-in.org.in/s2cMainServlet?pageid=chartmission>.

⁴⁵ "CERT-In Hosts Cyber Security Exercise 'Synergy' for 13 Countries as Part of International Counter Ransomware Initiative-Resilience Working Group," Ministry of Electronics and Information Technology (India), Press Release, August 31, 2022 ~ <https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1855771>.

⁴⁶ Ibid.

⁴⁷ CERT-In, "Annual Report 2023."

⁴⁸ Ibid.

⁴⁹ "India CERT Signs an MOU with U.S. CERT," Ministry of Electronics and Information Technology (India), Press Release, January 11, 2017 ~ <https://pib.gov.in/newsite/PrintRelease.aspx?relid=156288>.

The Indian political and diplomatic leadership work in close concert with the cyber institutions when engaging with international partners. India has, thus far, refrained from adopting an explicit and consistent stance on the controversial fissures of global normative debates, such as the application of sovereignty or other tenets of international law to cyberspace.⁵⁰ This approach enables collaboration with a range of partners without tripping up on ideological spats and accordingly enables the government and its institutions to showcase India's profile as a responsible cyberpower. Collaborations also serve as ripe opportunities for India's cyber institutions to be exposed to and benefit from best practices elsewhere.

Conclusion

India has established institutions to enhance national cybersecurity, and the government has allocated increased amounts of funding and resources to these institutions. India's cyber institutions have prioritized streamlined incident-reporting and response processes and have also attempted to increase awareness and build capacity among the general population and those individuals who directly engage with digital infrastructure. The bridging of the trust deficit between India's cyber institutions and the private sector over the past ten years has brokered much-needed external cooperation. Greater collaboration with the private sector, independent security researchers, and international counterparts, including between CERTs, has improved the information, capacity, and overall resilience of India's cyber institutions. This augurs well for the resist, recover, and adapt planks of cyber resilience.

That said, a continued lack of public clarity dampens efforts on all three fronts. In particular, the absence of a cohesive and regularly updated public national strategy hampers the resist and adapt parameters. This gap prevents both internal stakeholders and other countries from understanding the present threats and opportunities in India's cyber landscape and predicting its cyber behavior over the medium to long term. Disclosing the government's strategic thinking and overarching approach on issues such as cyber partnerships, the debates over global cyber norms, present and future cybersecurity financing, and the conduct of cyberoperations would

⁵⁰ Arindrajit Basu, "India's 'Passive' Multistakeholder Cyber Diplomacy," in *Building an International Cybersecurity Regime*, ed. Ian Johnstone, Arun Sukumar, and Joel Trachtman (Cheltenham: Edward Elgar Publishing, 2023), 201–19; and Arindrajit Basu and Karthik Nachiappan, "Will India Negotiate?" in *Hybridity, Conflict, and the Global Politics of Cybersecurity*, ed. Fabio Cristiano and Bibi Van Den Berg (London: Rowman and Littlefield, 2023), 189.

go a long way toward cementing India's global and domestic reputation on cyber issues. CERT-In's annual reports, which list various achievements and collaborations, are a useful starting point, but they stop short of articulating a broader strategic framework that can explain India's approach to cyber resistance and adaptation.

The lack of clarity also dampens recovery, though to a lesser extent. A continued lack of transparency in investigation processes and a reluctance to disclose clearly the steps taken in an investigation hamper accountability and collaboration. Further, the continued reticence to attribute cyberattacks remains a missed opportunity for India to reap significant strategic dividends.

India has taken impressive steps to make cybersecurity a core national security and domestic priority. Greater clarity in articulating its approach to the domain will enhance the country's cyber resilience. The future of India's quest to digitize, in a bid to further its national economic, security, and developmental goals, hangs in the balance. ♦

Indonesia's Cybersecurity Resilience

Gatra Priyandita

Indonesia is one of the world's most digitally connected countries. An estimated 212 million people (or 77% of its population) are online, and the digital economy is expected to contribute \$130 billion to its GDP by 2025.¹ Aiming to make Indonesia an advanced economy by 2045, the government of Joko Widodo (Jokowi) sought to use the transformative powers of digital technology to spur economic growth, enhance public services, and tackle socioeconomic challenges. This vision has also been adopted by the government of Prabowo Subianto, which took office in October 2024.² These ambitions, however, are threatened by cyber-enabled threats, including high rates of cybercrime and state-sponsored cyberoperations.

This essay maps and analyzes Indonesia's cyber resilience. Its capacity to resist, recover, and adapt to cyber challenges remains broadly mixed. Despite efforts to bolster cyber resilience, Indonesia's approach to cybersecurity is hampered by several challenges, including under-resourcing, limited political support, and legal ambiguities. The scarcity of human capital and financial resources has weakened the government's capacity to combat malicious cyberthreats, while cyberspace governance is undermined by the absence of clear legal frameworks that effectively empower agencies to enforce cybersecurity standards across all organizations, particularly in government. These factors undermine the country's cyber resilience, particularly its ability to recover from and adapt sufficiently to cyber-enabled threats.

To outline the argument, this essay is divided into five sections. The first section examines the emergence of cybersecurity as a national policy priority, highlighting how a series of considerations helped transform it from a technical issue to one of major policy attention. The second section considers measures the Indonesian government has employed to resist cyber-enabled threats. The third section examines measures to recover

GATRA PRIYANDITA is a Senior Analyst in the Cyber, Technology, and Security Program at the Australian Strategic Policy Institute (Australia). His primary research areas are cyber diplomacy and the military applications of emerging technology. He can be reached at <gatrapiyandita@aspi.org.au>.

¹ "Survei Internet APJII 2024" [Internet Survey APJII 2024], Association of Indonesian Internet Providers, 2024 ~ <https://survei.apjii.or.id>; and "e-Economy: SEA 2023," Google, Temasek, and Bain and Company, 2023, 86.

² Samaya Dharmaraj, "Komdigi: Driving Indonesia's Digital Future and Economic Growth," Open Gov, October 23, 2024 ~ <https://opengovasia.com/2024/10/23/komdigi-driving-indonesias-digital-future-and-economic-growth>.

from these threats by looking into how cyberattacks can be detected. The fourth section assesses how the country adapts to cyber-enabled threats by studying the measures for national and international collaboration. The final section highlights the challenges that undermine Indonesia's efforts to resist, recover, and adapt to cyberthreats—ultimately undermining its cyber resilience.

Emergence of Cybersecurity as a National Priority

Indonesia has grown increasingly vulnerable to cyber-enabled threats. The National Cyber and Crypto Agency (Badan Siber dan Sandi Negara, or BSSN) estimated that cybercrime cost the Indonesian economy around 14.5 trillion rupiah (nearly \$1.0 billion) in 2022. The BSSN further recorded that the country had 361 million cyber traffic anomalies from January to late October in 2023.³ With the country experiencing rapid digital transformation, numbers of high-profile cyber incidents have been increasing, resulting in unprecedented levels of data leakage and theft (see **Table 1**). Based on 2022 data from the Indonesian chapter of the Honeynet Project, a cybersecurity NGO, government agencies suffered most traffic anomalies (141.9 million), followed by energy and resource firms (122.0 million), finance firms (81.0 million), health organizations (49.9 million), and the information technology and communications (ICT) sector (47.0 million).⁴

From 2002 until the early 2010s, Indonesia consistently ranked among the top five countries hosting malicious cyberattacks; in fact, it briefly surpassed China as the world's largest source of cyberattacks in 2013.⁵ Indonesia's cyberspace was also vulnerable to information operations, misinformation and disinformation activities (especially from terrorist organizations), and foreign state actors. Terrorist organizations' use of the rapid proliferation of ICT and social media to spread propaganda and recruitment made cybersecurity—particularly content and information

³ Mahinda Arkyasa, "BSSN Records 361 Million Cyber Attacks in Indonesia," *Tempo*, November 17, 2023 ~ <https://en.tempo.co/read/1797753/bsn-records-361-million-cyber-attacks-in-indonesia>.

⁴ "Laporan Tahunan Honeynet Project Tahun 2022" [Honeynet Project Annual Report 2022], Badan Siber dan Sandi Negara (BSSN) [National Cyber and Crypto Agency] (Indonesia), 2023 ~ <https://cloud.bssn.go.id/s/qSJenLAmr2ooF2Q>.

⁵ "Indonesia Overtakes China as Top Source of Cyber Attack Traffic," ABC News (Australia), October 18, 2013 ~ <http://www.abc.net.au/news/2013-10-18/an-indonesia-overtakes-china-as-top-source-ofcyber-attack-traf/5032428>.

TABLE 1

Recent Major Cyberattacks in Indonesia

Date	Incident
March 2020	Tokopedia, one of Indonesia's largest e-commerce businesses, suffered a data breach that led to the leak of data on 15 million users.
May 2021	A breach in Badan Penyelenggara Jaminan Sosial Kesehatan, the National Healthcare and Social Security Agency, led to the leak of data on 222.5 million users, about 82% of Indonesia's overall population (though only via 100,002 records).
December 2021	Bank Indonesia suffered a ransomware attack, possibly by the notorious Conti Group, that threatened to leak 13.88 gigabytes of data.
August 2022	A series of high-profile data breaches and leaks occurred in Indonesia, attributed to a hacker or group of hackers operating under the pseudonym "Bjorka." This incident gained significant attention in 2022 when Bjorka exposed sensitive personal data of Indonesian citizens, including information related to government officials and agencies.
May 2023	Bank Syariah Indonesia, the largest Islamic bank in Indonesia, saw its services disrupted for several days. The hacking group Lockbit claimed responsibility for the attack and reportedly released a 1.5 terabyte trove of customer data.
June 2024	A ransomware attack extracted personal data from Indonesia's National Data Centre, exposing millions of Indonesians' personal data, including names, family information, and biometric data. The cybercriminal organization taking control of the data, possibly the Lockbit ransomware gang, demanded \$8 million in payment.
November 2024	The Directorate-General of Taxes suffered a major data breach by Bjorka, with six million taxpayer identification numbers, including that of President Joko Widodo, and other data leaked and sold on the Breach Forum website for \$10,000.

Source: Compiled by the author, 2024.

security—a national security risk.⁶ Furthermore, Jakarta was concerned that it could not protect network systems from state-sponsored attacks. This issue resurfaced in 2013 following revelations that members of the Indonesian political elite, including former president Susilo Bambang Yudhoyono and the first lady, had their phones wiretapped by the Australian government.⁷

⁶ Andyala Waluyo, "Penyebaran paham radikal melalui internet kembali marak" [The Spread of Radical Ideas via the Internet Is Becoming Widespread Again], Voice of America, September 26, 2013 ~ <https://www.voaindonesia.com/a/penyebaran-paham-radikal-di-internet-kembali-marak/1757520.html>.

⁷ Ewen MacAskill and Lenore Taylor, "Australia's Spy Agencies Targeted Indonesian President's Mobile Phone," *Guardian*, November 18, 2013 ~ <https://www.theguardian.com/world/2013/nov/18/australia-tried-to-monitor-indonesian-presidents-phone>.

To address these challenges, throughout its duration the Jokowi government moved to formally establish legal and institutional foundations to improve the country's ability to respond to cyber-enabled threats. Specifically, it focused on empowering incident-response capabilities, setting minimum cybersecurity standards, and building awareness about cyber-enabled threats.

Resistance

While cybersecurity has emerged as an issue of public and national security policy, the Indonesian government has yet to develop a cybersecurity strategy.⁸ Instead, Indonesia's response to cybersecurity challenges has centered on a series of legal and institutional measures.

Legal measures. Since the late 2000s, Indonesia has adopted several regulatory measures and developed the organizational capacity to strengthen its cyberdefenses. The foundational legal framework for regulating cyberspace is the Electronic Information and Transactions Law, which was enacted in 2008. This law empowers the government to prosecute various offences, including unauthorized access to computer systems and illegal wiretapping. In 2016, it was revised to include mandatory breach notifications and the "right to be forgotten."

Building on this law, additional regulations have been since introduced. A government directive empowered the Ministry of Defense to oversee cyberdefense, while Government Regulation No. 71/2019 addressed securing critical information infrastructure. Although the defense ministry regulation authorized the military to protect military infrastructure, the protection of critical civilian information infrastructure remained ambiguous. To address this gap, in 2022, President Jokowi issued Presidential Regulation No. 82/2022 that identifies and protects the country's vital information infrastructure. Another presidential regulation further assigned the BSSN to execute a national cybersecurity action plan for protecting critical infrastructure.

In October 2022 the Personal Data Protection Law was enacted, introducing stringent regulations on data protection following the leakage and sale on the dark web of millions of Indonesian taxpayer-identification

⁸ A strategy has been designed but as of the time of this writing has yet to be signed off on.

numbers and their personal data in what was termed the Bjorka case.⁹ The law concluded a two-year grace period in October 2024, with the government now able to start imposing sanctions on organizations that fail to protect the personal data under their control. However, an independent institution to review cases of noncompliance has yet to be established.

Institutional measures. The BSSN was established in 2017 to oversee cyber affairs and is responsible for creating, implementing, overseeing, and evaluating technical policies on cybersecurity. The agency has focused on raising awareness of cybersecurity's importance within government and the public at large, setting cybersecurity standards across government agencies, and supporting organizations experiencing cyberattacks. The BSSN has also organized regular cyber drills and is working to establish computer emergency response teams (also known as computer security incident response teams, or CSIRTs) across various government agencies and ministries.

Although Indonesia lacks a whole-of-government cybersecurity strategy, the BSSN developed its own national medium-term strategy, which outlined the agency's vision to build cybersecurity awareness, enhance the government's capacity to mitigate internal cybersecurity threats, protect critical infrastructure, and develop human capital.¹⁰ Other government agencies also maintain responsibilities over Indonesian cyberspace. The Ministry of Communication and Informatics handles content security and controls, while the National Police enforce laws in cyberspace, including prosecuting unauthorized intrusions and criminal activities online, such as gambling and child pornography. The Ministry of Defense oversees cyberdefense and the cybersecurity of the military's critical infrastructure, with specific cyber units attached to each of the three services. In September 2024 the Jokowi government also announced steps toward establishing a new cyber force, which may function as the fourth branch of the military.¹¹

Despite its important role in formulating minimum cybersecurity standards, the BSSN lacks the legal authority to coordinate among the

⁹ Yanuar Nugroho, "The #Bjorka Case and Ratification of Indonesia's PDP Law: Confronting Digitalisation," Fulcrum, September 29, 2022 ~ <https://fulcrum.sg/the-bjorka-case-and-ratification-of-indonesias-pdp-law-confronting-digitalisation>.

¹⁰ BSSN, *Rencana strategis Badan Siber dan Sandi Negara tahun 2020–2024* [National Cyber and Crypto Agency Strategic Plan for 2020–2024] (Jakarta, July 2020) ~ <https://peraturan.bpk.go.id/Details/174282/peraturan-bssn-no-5-tahun-2020>.

¹¹ "New 'Cyber Force': Indonesia to Launch Fourth Military Branch to Combat Online Threats and Attacks," Channel News Asia, September 24, 2024 ~ <https://www.channelnewsasia.com/asia/indonesia-cyber-force-military-4627456>.

various government units administering cyberspace. This diminishes its powers when enforcing standards across government bodies.

Recovery

Since 2016 the Indonesian government has drafted several measures to improve its response to cyber incidents. In 2018 the BSSN absorbed the powers of the Indonesia Security Incident Response Team on Internet and Infrastructure (ID-SIRTII), a unit established in 2007 to monitor cyberthreats and coordinate security incident response. The BSSN has since worked closely across government agencies to establish CSIRTs to help monitor and quickly respond to cyberthreats. The BSSN aimed to establish CSIRTs across 121 government agencies by 2024.¹² However, progress has been slowed by resource constraints.

This effort has been bolstered by attempts to address a lack of legal and regulatory clarity about national responsibility concerning incident response. In September 2023, President Jokowi issued Presidential Regulation No. 47/2023 on national cybersecurity strategy and cyber crisis management, focused on establishing CSIRTs and frameworks for managing cyber crises. Fundamentally, this regulation made the BSSN the primary coordinating agency during management of any cyber crisis. Thereafter, the BSSN issued several regulations requiring operators of critical information infrastructure to design frameworks for managing cyber crises, report incidents to the BSSN and other relevant parties, and disseminate information that would help prevent or mitigate future incidents.

Reporting procedures. BSSN Regulation No. 1 of 2024 outlines reporting procedures for cyber incidents involving both critical information infrastructure (CII) and non-CII electronic system providers (ESPs). When a cyber incident occurs, the organizational CSIRT must report it to the CSIRT at the next higher level. For CII ESPs, it is mandatory to report any cyber incidents that disrupt the continuity of electronic systems and services. Within 24 hours, the organizational CSIRT must report each incident to the sectoral CSIRT, with a copy appended to the national CSIRT. Non-CII ESPs must report cyber incidents that affect the continuity of their electronic system services, though the regulation does not specify a reporting deadline. Each report of a cyber incident must include the reporting party's contact information, a description of the incident, a chronology of events, and the

¹² BSSN, *Rencana strategis badan siber dan sandi negara tahun 2020–2024*.

incident's impact. These structured reporting procedures ensure that cyber incidents are promptly addressed and that information is disseminated to prevent future occurrences.

Adaptation

Indonesia is adapting to cybersecurity challenges through collaboration, capacity building, and international diplomacy. Recognizing the dynamic nature of cyberthreats, Jakarta is enhancing resilience by engaging multiple public and private stakeholders.

The Indonesian government has dedicated a small portion of the national budget to improve the security of government computer systems. However, the BSSN—the agency tasked to train government cybersecurity professionals and set cybersecurity standards—remains severely underfunded, limiting its ability to procure necessary equipment and recruit talent that would allow it to secure government and critical infrastructure networks. In 2024 the government allocated 771 billion rupiah (almost \$500 million) to the BSSN. Although this is an increase from 2022, it is still far below the peak allocation of over 2.2 trillion rupiah (\$1.4 billion) in 2019.¹³

Government agencies collaborate closely with the private sector and civil society to raise awareness, share expertise, and exchange information. A notable example is the recent establishment of the Indonesian chapter of the HoneyNet Project, a U.S.-based nonprofit cybersecurity organization investigating cyberattacks and developing open-source tools to enhance internet security. Through this project, the BSSN has partnered with a community of independent experts to create a comprehensive picture of cybersecurity threats in Indonesia. Industry and government agencies also collaborate to build technical capacity. Major ICT firms, including Cisco, Microsoft, and Huawei, have worked closely with government agencies to enhance cybersecurity capacity and share threat information.

Additionally, Indonesia is collaborating diplomatically to address growing cyber vulnerabilities.¹⁴ Within international forums, the country advocates for the peaceful use of ICT, discourages the development of “cyber weapons,” and seeks support for capacity building. Indonesia also

¹³ The allocation of \$1.4 billion in 2019 can be attributed to the need to both establish initial infrastructure development and improve the nation's cyberdefenses around the 2019 general election.

¹⁴ For an overview of Indonesia's approach to the world of cyber diplomacy, see Gatra Priyandita, “Indonesia,” in *Indo-Pacific Perspectives on Responsible Cyber Behaviour*, ed. Gatra Priyandita and Louise Marie Hurel (Canberra: Australian Strategic Policy Institute, forthcoming 2025).

actively promotes cyber capacity-building in major multilateral forums, including the United Nations and the Association of Southeast Asian Nations (ASEAN). The government, particularly through the BSSN, has engaged foreign governments and companies to facilitate training. Cyber cooperation has emerged as a dimension of overall security collaboration between Indonesia and other countries, such as South Korea and Australia. Bilateral cybersecurity cooperation most often covers capacity building, cooperation on cybercrime and cyberterrorism, and the establishment of points of contact for incident handling. International cooperation and cyber capacity-building are perceived as pathways to support Indonesia's relatively weak capacity in responding to cyberspace challenges.

Beyond capacity building, Indonesia's cyber diplomacy is most active when addressing the threat of cyberterrorism. Facing a flurry of problems involving the spread of Islamic fundamentalism and hate crimes, Indonesian documents highlight the threat that cyberspace could be hijacked to "spread hatred and racial ideology."¹⁵ Demonstrating its commitment to combat cyberterrorism, Indonesia signed up for the 2019 Christchurch Call initiated by the New Zealand government to encourage governments and online service providers to make voluntary commitments to stop terrorist and violent online content.

Despite Indonesia being one of the largest digital economies, its presence in international cyber summitry remains limited. In part, this can be attributed to limited expertise and relatively few diplomatic officials covering this subject. Indonesia's international cyber engagements are largely spread between two agencies—the BSSN, which manages bilateral cyber engagement at the technical level, and the Ministry of Foreign Affairs, which manages Indonesia's cyber engagements in international summits, such as at the UN Open-Ended Working Group on ICT. Within the foreign ministry, cyber diplomacy is managed by a few individuals working under the Directorate of International Security, a unit that also covers nonproliferation and arms control. With few officials focused on cyber diplomacy, there remains little capacity for the country to adopt a proactive attitude in international cyber summits.¹⁶

¹⁵ "Indonesia's Statements at the First and Second Substantive Sessions of the OEWG on ICT," United Nations TV, 2020.

¹⁶ For instance, see Indonesia's relative silence on the Pall Mall Process, initiated by the United Kingdom and France, that aims to mitigate proliferation and irresponsible use of commercial cyber intrusion tools and services. Gatra Priyandita and Arindrajit Basu, "Why Haven't India and Indonesia Signed Up for Anti-Spyware Dialogue?" Royal United Services Institute, RUSI Commentary, April 10, 2024 ~ <https://www.rusi.org/explore-our-research/publications/commentary/why-havent-india-and-indonesia-signed-anti-spyware-dialogue>.

Furthermore, Indonesia's relative reticence on cyber-related diplomatic matters may also be attributed to deepening strategic competition in cyberspace. With more issues now entangled in strategic competition between the major powers, Indonesia might adopt middle-of-the-road positions that allow it to avoid entanglement. Deepening strategic competition has thus far not undermined the quality or forms of cyber capacity-building. However, Indonesia's exposure to Chinese technologies, including its wide use of Huawei and ZTE equipment, could weaken the prospects of receiving valuable cyber intelligence and information from Western partners, such as the United States and Australia.¹⁷

Challenges

Indonesia has the legal and institutional foundations to protect its cyberspace from malign threats. That said, three core challenges undermine the country's cyber resilience.

The first problem is awareness, pertaining to the complexity of threats online. To be sure, there is growing public awareness about cyberattacks. For instance, commercial entities appear to be taking cybersecurity seriously, and the cybersecurity market was estimated to be worth about \$2.05 billion in 2023.¹⁸ Yet, Indonesia's cyberspace remains highly vulnerable, with relatively lower levels of IT security program utilization, such as virus protection software. Some government agencies also at times use pirated software, given budget constraints, which, unpatched, makes computer systems more vulnerable.¹⁹ Consequently, many computers in Indonesia are easily exploitable. Furthermore, there are diverging threat perceptions among the public and in industry over the economic and security implications of cyberattacks on organizations and society. This divergence generates inconsistencies in risk assessments and complicates mitigation efforts between organizations.

Organizations generally possess different risk appetites and perceptions when facing cyber-enabled threats. However, this constraint may pose a long-term problem for Indonesia's security and economic development.

¹⁷ On Huawei and ZTE in Indonesia, see Gatra Priyandita, Dirk van der Kley, and Benjamin Herscovitch, "Localization and China's Tech Success in Indonesia," Carnegie Endowment for International Peace, July 11, 2022 \approx <https://carnegieendowment.org/research/2022/07/localization-and-chinas-tech-success-in-indonesia?lang=en>.

¹⁸ "Indonesia Cybersecurity," U.S. International Trade Administration, Market Intelligence, July 3, 2023 \approx <https://www.trade.gov/market-intelligence/indonesiacybersecurity>.

¹⁹ Author's interview with a senior Indonesian official, Jakarta, June 20, 2024.

Indonesia is becoming wealthier, with more organizations increasingly producing valuable intellectual property. Thus, protecting information of commercial and knowledge security value is important. As of now, not all innovative industries maintain high standards for cybersecurity; only the financial sector maintains robust standards. The banking sector is the only industry that must submit annual cybersecurity assessments and enforce effective cybersecurity risk management, including incident management.²⁰ This disparity in requirements undermines the ability of industry writ large to recover and adapt from cyberattacks.

The second problem is resourcing. The BSSN and other government units responsible for cybersecurity consistently lack the funds and human capital required to maintain security in cyberspace. Funding was further reduced amid the Covid-19 pandemic, despite the growing use of the internet for communication and commerce during and after that period. However, failing to restore past budget levels amid growing cyberthreats will undermine the BSSN's ability to function effectively, procure essential cyberdefense equipment and infrastructure, and adequately train cybersecurity specialists.

The third problem concerns the absence of an overarching regulatory and legal framework for cybersecurity. Indonesia relies on a patchwork of regulations and legislation that cover a wide range of issues, including cybersecurity, data privacy, and content-related crimes (e.g., disinformation and intellectual property theft). Indonesia has no national cybersecurity strategy. This lack of a cybersecurity law or strategy specifying clear responsibilities and definitions does not make Indonesia's approach to cybersecurity unique—most ASEAN states currently lack such a law or strategy. However, this absence weakens governance and resourcing, particularly given Indonesia's authoritarian past and prevailing intra-bureaucratic conflicts. Without a national cybersecurity law, the BSSN's authority atop a diffuse cyber architecture remains ambiguous, impeding governance, enforcement, and resource allocation.

Collectively, these challenges undermine Indonesia's resilience as cyber-enabled threats rise. Although it has sufficient capacity to resist cyber-enabled threats, Indonesia struggles to recover and adapt, leaving its cyberspace vulnerable to exploitation. ♦

²⁰ "Ketahanan dan keamanan siber bagi bank umum" [Cyber Resilience and Security for Commercial Banks], Otoritas Jasa Keuangan [Financial Services Authority] (Indonesia), December 27, 2022 ~ <https://ojk.go.id/id/regulasi/Pages/Ketahanan-dan-Keamanan-Siber-Bagi-Bank-Umum.aspx>.

Japan's Shift in the Cyber Domain toward a Proactive Defense Posture

Dai Mochinaga

Cyberspace has emerged as a critical domain of conflict and competition in the 21st century. Japan has not been immune to these changes. Since the 2000s, Tokyo's approach to cybersecurity has evolved, reflecting broader shifts in the global security environment and in Japan's own strategic priorities. In the early 2000s, Japan's cybersecurity efforts primarily focused on protecting civilian infrastructure and government networks from potential disruptions. Cyberattacks on government agencies in 2000 served as a wake-up call, prompting the establishment of an organization responsible for cybersecurity and the formulation of basic cybersecurity strategies. However, these initial efforts were largely reactive and lacked a comprehensive national security perspective.

As cyberthreats grew more sophisticated and state-sponsored cyberattacks more prevalent, the Japanese government began to recognize cybersecurity as a critical national security issue. This shift was marked by the release of Japan's first National Security Strategy in 2013, which explicitly highlighted the importance of the cyber domain.¹ In 2013, Tokyo established a government-wide and international strategy for cybersecurity.² This strategy defined the basic principles of Japan's cybersecurity policy: ensuring the free flow of information, responding to increasingly serious risks, enhancing the risk-based approach, and supporting cooperation between the public and private sectors as well as international partnerships. The strategy also defined priority areas of collaboration such as incident response, information sharing, countering cybercrime, and international security. Subsequently, prompted by a rising number of cyber incidents,

DAI MOCHINAGA is an Associate Professor at the Department of Systems Engineering and Science at Shibaura Institute of Technology (Japan). Prior to this, he was a researcher at Mitsubishi Research Institute and an analyst at the Japan Computer Emergency Response Team (JPCERT) Coordination Center. His analysis focuses on global cybersecurity, technology policy, and regulatory issues. He can be reached at <mochidai@shibaura-it.ac.jp>.

¹ Cabinet Secretariat (Japan), *National Security Strategy* (Tokyo, December 2013) ~ <https://www.cas.go.jp/jp/siryou/131217/anzenhoshou/nss-e.pdf>.

² Information Policy Council (Japan), *Cybersecurity Strategy: Towards a World-Leading, Resilient and Vigorous Cyberspace* (Tokyo, June 2013) ~ <https://www.nisc.go.jp/eng/pdf/cybersecuritystrategy-en.pdf>; and Information Security Policy Council, *International Strategy on Cybersecurity Cooperation: Initiative for Cybersecurity* (Tokyo, October 2013) ~ https://www.nisc.go.jp/eng/pdf/InternationalStrategyonCybersecurityCooperation_e.pdf.

Japan moved to enhance its cyber capabilities, adopting an active cyberdefense (ACD) concept in the 2022 National Security Strategy.³ Cyberattacks on the Japanese government numbered 233 in 2023, 266 in 2022, and 207 in 2021.⁴ In the private sector, the Japan Computer Emergency Response Team Coordination Center (JPCERT/CC) received 65,669 incident reports in 2023, 58,389 in 2022, and 44,242 in 2021.⁵ The Japanese national police agency and other government agencies filed 6,312 cybercrime cases in 2023, 2,200 in 2022, and 1,516 in 2021.⁶

By tracing Japan's cybersecurity evolution and exploring the challenges and implications of its new ACD approach, this essay examines how Japan is adapting to the realities of cybersecurity in the 21st century and enhancing its cyber resilience. The essay also offers insights into the broader trends in national cyber strategies and the impact of international cooperation on cybersecurity policies.

The Evolution of Japan's Cybersecurity Strategy

Japan's cybersecurity strategy has evolved significantly since 2000, with a strong emphasis on protecting civilian infrastructure and government networks. This evolution has spanned three distinct phases, each marked by key policy developments and shifts in strategic thinking.

The first phase, 2000–2004, was characterized by trial and error. Following government-wide cyberattacks in 2000, Prime Minister Junichiro Koizumi established the IT Security Office (ITSO) in the Cabinet Secretariat. ITSO's primary tasks included building a government-wide framework for cybersecurity, developing an action plan for critical infrastructure protection, setting up guidelines for information security, and conducting assessments of government computer systems. During this phase, Japan's approach was predominantly civilian-oriented and reactive, focusing on protecting critical infrastructure and government networks.

³ Cabinet Secretariat (Japan), *National Security Strategy* (Tokyo, December 2022) ~ <https://www.cas.go.jp/jp/siryou/221216anzenhoshou/nss-e.pdf>.

⁴ National Center of Incident Readiness and Strategy for Cybersecurity (Japan), "Saiba sekyuriti 2024 (2023-nendo nenji hokoku/2024-nendo nenji keikaku)" [Cybersecurity 2024 (Annual Report for 2023/Annual Plan for 2024)], July 10, 2024 ~ <https://www.nisc.go.jp/pdf/policy/kihon-s/cs2024.pdf>.

⁵ Japan Computer Emergency Response Team Coordination Center (JPCERT/CC), "Incident Handling Quarterly Report" ~ <https://www.jpcert.or.jp/english/ir/report.html>.

⁶ "Fusei akusesu koi no hassei jokyo oyobi akusesu seigyo kino ni kansuru gijutsu no kenkyu kaihatsu no jokyo" [Cases of Unauthorized Accesses and Status of R&D Related to Access Control], National Police Agency (Japan), Press Release, March 14, 2024 ~ <https://www.npa.go.jp/news/release/2024/20240314.pdf>.

The second phase, 2005–14, saw the Japanese government build institutional frameworks, strategies, and legislative systems for cybersecurity. During this period the government established the Information Security Policy Council and reorganized the ITSO into the National Information Security Center (NISC, now the National Center of Incident Readiness and Strategy for Cybersecurity). The NISC served as the central government body for cybersecurity, focusing on intergovernmental coordination. It led the establishment of a government-wide strategy for information security and planning for critical infrastructure protection. The Ministry of Economy, Trade and Industry and the Ministry of Internal Affairs and Communications took leading roles in shaping policies for the private sector and telecommunications security, and the National Police Agency worked toward strengthening law enforcement in the cyber realm.

The 2014 Basic Act on Cybersecurity established a legal framework for Japan’s cybersecurity efforts.⁷ It aimed to build the legal basis of cybersecurity policies and to clarify responsibilities of the government agencies. During this period, the scope of Japan’s cybersecurity policy expanded to include national security, public security, and international cooperation. In 2013, Japan adopted its first comprehensive cybersecurity strategy, recognizing cyberattacks as a national security issue.

The third phase began in 2015 with the enforcement of the Basic Act on Cybersecurity and the adoption of a new cybersecurity strategy.⁸ This phase has been characterized by the establishment of a legal basis for cybersecurity policies, clarification of government agencies’ responsibilities, enhanced authority for the NISC (including audit powers), and an increased focus on the national security aspects of cybersecurity. The 2018 Cybersecurity Strategy marked a significant shift in approach by introducing the concept of deterrence in the cyber domain and emphasizing the strengthening of capabilities for defense, deterrence, and situational awareness across both public and private sectors.⁹ It underscored the need to develop capabilities to disrupt adversaries’ use of cyberspace and to strengthen Japan’s overall cyberdefense posture.

⁷ “The Basic Act on Cybersecurity,” Ministry of Justice (Japan), trans. Japanese Law Translation, November 12, 2014 \approx <https://www.japaneselawtranslation.go.jp/en/laws/view/3677/en>.

⁸ Government of Japan, *Cybersecurity Strategy* (Tokyo, September 2015) \approx <https://www.nisc.go.jp/eng/pdf/cs-strategy-en.pdf>.

⁹ Government of Japan, *Cybersecurity Strategy* (Tokyo, July 2018) \approx <https://www.nisc.go.jp/eng/pdf/cs-senryaku2018-en.pdf>.

In 2021 the Japanese government released its latest cybersecurity strategy emphasizing three pillars: advancing digital transformation and cybersecurity simultaneously, enhancing cyber initiatives from the perspective of national security, and contributing to the peace and stability of the international community. This strategy also recognizes the increasing importance of cybersecurity in the context of rapid digitalization, especially considering the implications of the Covid-19 pandemic; moreover, it emphasizes the need for a risk-based approach to cybersecurity throughout the supply chain.

The shift toward ACD came with the 2022 National Security Strategy, which introduced Japan's version of the concept. This ACD concept includes measures to preemptively neutralize adversary computers in peacetime to address serious cyberattacks. Given that cyberattacks consist of multiple phases, such as reconnaissance, initial access, and materialization, Japan's approach is to aim to mitigate the impact of attacks in the early phases. It represents a significant departure from Japan's previous defensive posture and aligns more closely with the approaches of the country's Western allies.

In 2024 the Japanese government intensified discussions on the development of ACD capabilities. A panel of experts established by the government convened to examine the challenges and conceptual details of ACD, and it concluded with the publication of a comprehensive set of recommendations in November.¹⁰ The panel's recommendations emphasized the need for enhanced public-private partnerships, communication analysis under a dedicated independent auditing authority, mechanisms for neutralizing cyberthreats, and reorganization of the NISC.

Under the leadership of Prime Minister Shigeru Ishiba, efforts to advance ACD capabilities have gained momentum. The government's 2025 budget underpinned this strategic direction. The 2025 budget allocation for the NISC doubled compared to the 2024 budget, and its personnel increased from 188 to 233. These developments, along with the expert panel's recommendations, provided the government with a strong mandate to draft new legislation. The government submitted the draft legislation to

¹⁰ "Expert Panel toward Improving Response Capabilities in the Field of Cybersecurity," Prime Minister's Office (Japan), June 7, 2024 ~ https://japan.kantei.go.jp/101_kishida/actions/202406/07cyber.html; and "Saiba anzen hoshō bun'ya de no taio noryoku no kōjo ni muketa yūshikisha kaigi" [Expert Panel toward Improving Response Capabilities in the Field of Cybersecurity], Cabinet Secretariat (Japan) ~ https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo/index.html.

the regular parliamentary session on February 7, 2025, accompanied by documents that detailed its concept and background.¹¹

Through these phases, Japan has prioritized public-private partnerships and information sharing. Initiatives like CISTA (Collective Intelligence Station for Trusted Advocates) and the Cybersecurity Information Sharing Partnership have promoted collaboration between government and industry.¹² Furthermore, the cybersecurity council operated by the NISC and JPCERT/CC have shared cyberthreat information with government agencies and private organizations under strict confidentiality as stipulated in the Basic Act on Cybersecurity.¹³ The NISC is a governmental computer emergency response team (CERT) and JPCERT/CC is a CERT covering private entities. Both work together as national CERTs. JPCERT/CC has served as a point of contact for incident reports from Japanese organizations since 1996. In this function, it has supported incident response work, assessed situations, analyzed methods used, and considered and proposed recurrence prevention measures. Also, the utilization of information held by telecommunications carriers is a Ministry of Internal Affairs and Communications effort related to proactive cybersecurity measures.

International cooperation has been a key aspect of Japan's strategy, with JPCERT/CC playing a crucial role in incident coordination and capacity building in the Asia-Pacific region. Japan has contributed to regional capacity development for over twenty years. Its community-based approach has led to collective power by sharing threat information and best practices. Engagement in capacity building stems from Japan's "free and open" Indo-Pacific vision aimed at pursuing economic prosperity and securing peace and stability. Japan has conducted cybersecurity capacity building with other countries by deepening understanding and training. For example, in 2020 the Japan International Cooperation Agency conducted a technical cooperation project with Southeast Asian states and Association of Southeast Asian Nations officials focused on cybersecurity under the Japan-ASEAN Technical Cooperation Agreement. JPCERT/CC helped form the Asia Pacific CERT (APCERT) and provides a secretariat function for

¹¹ "Saiba anzen hoshō ni kansuru torikumi (nodoteki saiba bogyo no jitsugen ni muketa kento nado)" [National Cybersecurity Initiatives (Considerations for the Implementation of Active Cyberdefense, etc.)], Cabinet Secretariat (Japan) ~ https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo_torikumi/index.html.

¹² JPCERT/CC, "About JPCERT/CC," https://www.jpcert.or.jp/english/about/06_2.html; and Information Promotion Agency (Japan), "J-CSIP & J-CRAT" ~ <https://www.ipa.go.jp/en/about/activities/jcsip-jcrat.html>.

¹³ National Center of Incident Readiness and Strategy for Cybersecurity (Japan), "Enhancement of Information Sharing" ~ <https://www.nisc.go.jp/eng/index.html#sec6>.

the group. Globally, as a member of the Forum of Incident Response and Security Teams (FIRST), JPCERT/CC cooperates with other CERTs in a trusted network. Furthermore, Japan, Australia, India, and the United States, operating through the Quad minilateral, have held Quad Senior Cyber Group meetings since March 2022. This group has reaffirmed its members' commitment to an Indo-Pacific that is resilient and equipped to detect and deter cyberattacks.¹⁴

Although Japan's cybersecurity strategy has evolved, shaped by national security considerations, the protection of civilian infrastructure and the promotion of public-private partnerships have remained a cornerstone of its approach, while also addressing new security challenges such as emerging technologies like artificial intelligence and the Internet of Things. As such, budgetary allocations for cybersecurity have increased. The government's cybersecurity budget grew substantially from approximately 56.7 billion yen (\$378 million) in FY2014 to 212.9 billion yen (\$1.419 billion) in FY2024.¹⁵ As cyberthreats evolve, Japan's challenge will be to maintain this balanced, collaborative approach while developing the capabilities necessary to mitigate sophisticated threats in an increasingly complex digital landscape.

The Shift to Proactive Defense Posture in the Cyber Domain

Japan's cyberdefense strategy has undergone a profound transformation in the nearly past quarter century. Beginning with a focus on protecting civilian infrastructure, it has evolved into a comprehensive approach that integrates cybersecurity into national defense strategy and includes elements of active defense. This evolution reflects Japan's growing recognition of cyberthreats as a critical national security issue, the influence of its alliance with the United States, and its ambition to play a more proactive role in international security.

The early 2010s saw a significant shift in Japan's perception of cyberthreats. Cyberattacks increasingly became recognized not just as a technical issue but as a matter of national security. This shift was reflected in the 2011 joint statement of the Japan-U.S. Security Consultative Committee,

¹⁴ "Joint Press Release of the Quad Senior Cyber Group," Ministry of Foreign Affairs (Japan), Press Release, December 14, 2023 ~ https://www.mofa.go.jp/tp/es/pageite_000001_00045.html.

¹⁵ "Seifu no cybersecurity ni kansuru yosan" [Government's Budget on Cybersecurity], National Center of Incident Readiness and Strategy for Cybersecurity (Japan), July 10, 2024 ~ <https://www.nisc.go.jp/pdf/council/cs/dai41/41shiryoku03.pdf>.

which referred to the threat in cyberspace for the first time and declared that the two countries would consider how to deal with it.¹⁶

The release of Japan's first National Security Strategy in 2013 marked a crucial turning point. This document explicitly recognized the importance of the cyber domain in security policy and set the direction for strengthening Japan's defense capabilities in cyberspace. Importantly, it emphasized the Japan-U.S. alliance as a pillar in this domain, explicitly stating cyberdefense cooperation as part of bilateral security and defense cooperation. The period from 2013 to 2018 saw intensive efforts to deepen cyber cooperation. In February 2013, Prime Minister Shinzo Abe and President Barack Obama agreed to launch the Japan-U.S. Cyber Dialogue, which brings together various relevant governmental authorities from both countries.¹⁷

Japan's cyberdefense strategy continued to evolve rapidly in the latter half of the 2010s. These included the establishment of the Cyber Defense Group under the Self-Defense Forces C4 Systems Command in 2014, the creation of the Cyber Defense Command directly under the Minister of Defense in 2022, and the establishment of various cyber-related divisions within the Ministry of Defense, including the Cyber Policy Section in 2015 and the position of Special Analyst for Cybersecurity in 2022. The 2018 National Defense Program Guidelines positioned the cyber domain as vital for Japan's multi-domain defense capability and cross-domain operations.¹⁸ It expanded the scope of protection to include private critical infrastructure, reflecting the growing recognition of the interconnected nature of cyberthreats.

The 2019 Japan-U.S. Security Consultative Committee meeting marked another significant step in bilateral cyberdefense cooperation, with the two countries confirming that cyberattacks could constitute an armed attack under the provisions of Article V of the Japan-U.S. Security Treaty.¹⁹ This agreement enhanced the feasibility of the treaty in the cyber domain and demonstrated the alliance's adaptation to new security challenges. Japan's cyberdefense capabilities in this period were significantly influenced by U.S.

¹⁶ "Joint Statement of the Security Consultative Committee: Toward a Deeper and Broader U.S.-Japan Alliance: Building on 50 Years of Partnership," Ministry of Foreign Affairs (Japan), June 21, 2011 ~ https://www.mofa.go.jp/region/n-america/us/security/pdfs/joint1106_01.pdf.

¹⁷ "Joint Statement Japan-U.S. Cyber Dialogue," Ministry of Foreign Affairs (Japan), May 10, 2013 ~ https://www.mofa.go.jp/region/page22e_000001.html.

¹⁸ Cabinet Secretariat (Japan), "National Defense Program Guidelines for FY 2019 and Beyond," December 18, 2018 ~ https://www.cas.go.jp/jp/siryou/pdf/2019boueikeikaku_e.pdf.

¹⁹ "Joint Statement of the Security Consultative Committee," Ministry of Foreign Affairs (Japan), April 19, 2019 ~ <https://www.mofa.go.jp/files/000470738.pdf>.

pressure and support. Washington consistently urged Tokyo to strengthen its cyber capabilities, reflecting the alliance's need for more balanced contributions in emerging security domains. This pressure was evident in critiques from U.S. officials and experts who expressed concerns about Japan's cybersecurity efforts.²⁰

The introduction of Japan's ACD concept in the 2022 National Security Strategy represents the culmination of this evolutionary process. The ACD concept, which includes measures to preemptively neutralize adversary computers in peacetime to address serious cyberattacks, aligns more closely with U.S. approaches to cyberdefense. It demonstrates Japan's move toward a more assertive posture in cyberspace and its intention to play a role equivalent to its allies and other like-minded countries.

Japan's evolving cyber strategy has also been accompanied by budgetary changes. The increase in the Ministry of Defense's cyber-related budget, from 34.2 billion yen (\$244.0 million) in FY 2022 to 236.3 billion yen (\$1.7 billion) in FY 2023, further demonstrates Japan's commitment to enhancing its cyber capabilities. When considering these budgets as a percentage of GDP, the comparison is striking. In FY 2023, the United States' budget request for cyberdefense represented 0.0493% of its GDP, while Japan's spending reached 0.0443%. This near parity in GDP-relative spending indicates that Japan's FY 2023 budget allocation for cyberdefense has achieved a level comparable to that of the United States—a significant development in Japan's cyberdefense posture.

Although the U.S.-Japan alliance is central to Japan's cyberdefense, Tokyo has also expanded its cooperation with other partners. Since 2014, Japan has engaged in bilateral cybersecurity meetings with multiple countries and participated in multinational cyber exercises. This expanded international cooperation reflects Japan's recognition that effective cyberdefense requires collaboration with a diverse array of partners and aligns with its broader strategic objective of playing a more active role in international security affairs. The introduction of a security clearance system in 2024 marked another significant development in facilitating information sharing and addressing a key aspect of alliance cooperation—intelligence

²⁰ See, for example, "Defense Perspective: Proposals / Cybersecurity Command Post Urgently Needed to Direct Active Cyber Defense," *Yomiuri shimbun*, November 22, 2022 ~ <https://japannews.yomiuri.co.jp/politics/political-series/20221122-72394>; and James Andrew Lewis "U.S.-Japan Cooperation in Cybersecurity," Center for Strategic and International Studies, November 5, 2015 ~ https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/151105_Lewis_USJapanCyber_Web.pdf.

sharing and joint threat assessment. This development should further U.S.-Japan cyber cooperation.

As Japan continues to develop and implement its ACD concept, it faces several challenges. These include legal constraints, the need for enhanced coordination across government agencies and with the private sector, and the complexities of operating in the rapidly changing cyber domain. The integration of Japan's ACD capabilities with U.S. cyberoperations, particularly in scenarios involving the defense of U.S. bases in Japan, presents both opportunities and challenges for the alliance.

Moving forward, Japan's cyberdefense strategy will likely continue to grow, adapting to new threats and technological advancements. The U.S.-Japan alliance will undoubtedly play a crucial role in this evolution, shaping Japan's capabilities, strategic thinking, and operational approaches in cyberspace. As both nations face common cyberthreats from actors such as China, Russia, and North Korea, their collaboration in this domain is becoming increasingly vital to their shared security interests in the Indo-Pacific region.

The trajectory of Japan's cyberdefense from 2000 to 2025 demonstrates a clear shift toward a more proactive and comprehensive approach, heavily influenced by its alliance with the United States. This evolution reflects not only Japan's growing recognition of cyberthreats as a critical national security issue but also the country's ambition to play a more significant role in international security. As cyberthreats develop and proliferate, the dynamics of the U.S.-Japan alliance in cyberspace will likely remain a key factor shaping regional cybersecurity efforts and strategies.

Implications and Future Challenges

Japan's evolution in cyberdefense strategy, in particular adopting its ACD concept, carries significant implications for regional security dynamics and presents a host of challenges for implementation. As Japan navigates this new digital frontier, it must balance its more assertive posture with legal, operational, and diplomatic considerations.

One of the primary implications of Japan's new cyber strategy is its potential impact on regional security dynamics. By developing deep cyber capabilities, Japan is positioning itself as a more robust security partner in the Indo-Pacific region. This shift could alter the strategic calculus of potential adversaries and may influence the cyber policies of other regional actors. However, it also raises questions about how Japan's neighbors,

particularly China and North Korea, might perceive and respond to this more assertive stance.

The implementation of the ACD concept presents several challenges. Legally, Japan must navigate complex domestic and international legal frameworks. Amendments to existing laws, such as the Act on Prohibition of Unauthorized Computer Access, may be necessary. Moreover, Japan must carefully consider how its ACD activities align with international law, particularly in cases where operations might affect systems in other countries.

Operationally, the ACD concept demands enhanced coordination across government agencies and the private sector. The proposed reorganization of the NISC is a step in this direction, but establishing effective cross-sectoral information sharing and rapid-response mechanisms remains a significant challenge. Japan must also develop the technical capabilities and human resources necessary to implement its more proactive cyber strategy. The protection of critical infrastructure, a key component of the ACD concept, requires close collaboration with the private sector. Establishing effective public-private partnerships while respecting corporate autonomy and addressing privacy concerns will be crucial.

Looking ahead, Japan must also consider how its ACD concept will evolve in response to rapidly advancing technologies. The rise of artificial intelligence, quantum computing, and other emerging technologies will likely present new challenges and opportunities in cyberspace, requiring continuous adaptation of Japan's cyber strategy. Furthermore, the country's proactive cyber posture may have implications for its broader foreign policy and diplomatic relations. As Japan engages in more assertive cyberoperations, it must carefully manage perceptions and maintain its commitment to international norms and a rules-based order in cyberspace.

Conclusion

Japan's cybersecurity strategy has evolved, transitioning from a defensive, civilian-focused approach to a comprehensive, proactive posture integrated into the country's national security framework. The adoption of the ACD concept in 2022 marks a pivotal shift, aligning Japan more closely with its Western allies and reflecting its ambition to play a larger role in international security.

This evolution, driven by growing cyberthreats and influenced by the U.S.-Japan alliance, has important implications for regional security dynamics. However, implementation challenges remain, with legal,

operational, and diplomatic considerations. Japan's commitment to enhancing its cyber capabilities is evident in its increased budget allocation and the introduction of a security clearance system. These developments position the country as a more robust security partner in the Indo-Pacific. As Japan further develops its cyber policies, it must balance its assertive posture with its commitment to international norms and a rules-based order. Japan will need to remain agile to meet evolving threats and emerging technologies. ◆

Cyber Resilience in South Korea

Dongyoun Cho

The Republic of Korea (ROK, or South Korea) has emerged as a digital powerhouse in the dynamic Indo-Pacific region. The country's rapid and successful digital transformation is underpinned by a robust infrastructure, widespread internet penetration, and a thriving technology sector. In this context, cybersecurity plays a vital role in sustaining South Korea's economic growth.

The Global Cybersecurity Index 2020, launched by the International Telecommunication Union in 2015 to measure the commitment of states to cybersecurity, ranks South Korea fourth globally and first in the Asia-Pacific, exemplifying Seoul's robust commitment.¹ However, cybersecurity is a dynamic field with evolving risks, shifting priorities, and variable resource allocations. South Korea has continuously adapted to these changes and reinforced its cybersecurity posture. This essay evaluates South Korea's cyber resilience by examining the country's capabilities to resist, recover, and adapt to adverse cyber events. The evaluation focuses on national cybersecurity strategies, incident-response mechanisms, and international coordination.

This essay argues that the ROK's cyber resilience is robust, shaped by a fractious environment marked by threats from the Democratic People's Republic of Korea (DPRK, or North Korea), Russia, and China. Moreover, this resilience is characterized by a heavy emphasis on resistance and adaptation, buttressed by a comprehensive domestic cybersecurity strategy and strong international partnerships on cyber issues. The findings provide insights into South Korea's cybersecurity strengths and areas for improvement, which are crucial for enhancing its ability to withstand and recover from cyberattacks and contribute to a more secure and resilient digital environment.

DONGYOUN CHO is an Assistant Professor in the Department of Military Studies at Seokyeong University in Seoul (Republic of Korea). She can be reached at <dongyoun@skuniv.ac.kr>.

¹ The Global Cybersecurity Index serves as a crucial benchmark for assessing the cybersecurity commitments of its member states and Palestine. The index evaluates 82 points across five key pillars: legal measures, technical measures, organizational measures, capacity development, and cooperation. It assists countries in identifying areas for improvement and encourages proactive measures. See International Telecommunication Union (ITU), *Global Cybersecurity Index 2020* (Geneva: ITU, 2020) ≈ <https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E>.


The Evolving Cyberthreat Landscape in South Korea

South Korea's digital landscape is characterized by an advanced broadband infrastructure, leading technology companies, and a tech-savvy population. With nearly 95% of its population online, the country boasts one of the highest internet penetration rates globally. Its rate is comparable to that of nine other Organisation for Economic Co-operation and Development (OECD) countries—Denmark, Finland, Iceland, Luxembourg, the Netherlands, Norway, Sweden, Switzerland, and the United Kingdom—where more than 97% of the population used the internet in the past three months.² However, this extensive digital connectivity also increases exposure to significant cyberthreats, ranging from espionage to ransomware. This is evidenced by the rising number of cyberattacks, which affect both the public and private sectors.

The cyberthreat landscape in South Korea is multifaceted and complex. While the DPRK poses a major concern with its sophisticated cyber campaigns that focus on espionage and financial gain, threats from cybercriminals and hacktivist groups also persist. Moreover, South Korea's increasing interconnectivity and dependence on digital systems make the country increasingly vulnerable to disruptions that could affect critical infrastructure and economic stability.

Constant cyberthreats from the DPRK. Between 2017 and 2023, the Panel of Experts, established under the UN Security Council Resolution 1874 in 2009, has investigated 58 suspected cyberattacks attributed to the DPRK that target cryptocurrency-related companies. These attacks are estimated to have yielded approximately \$3 billion to North Korea, helping fund the country's development of weapons of mass destruction. Carried out by hacking groups such as Kimsuky, the Lazarus Group, Andariel, and BlueNoroff, the cyberattacks have reportedly continued at a high volume. These attacks target defense companies and supply chains, often using increasingly shared infrastructure and tools. The attack methodologies employed by the country include spear phishing, vulnerability exploits, social engineering, and watering holes.³

The panel has identified several trends in malicious cyberactivity by the DPRK during 2023, including its continued targeting of the cryptocurrency industry. These trends are detailed in **Table 1**.

² OECD, *OECD Digital Economy Outlook 2024 (Volume 1): Embracing the Technology Frontier* (Paris: OECD Publishing, 2024)  <https://doi.org/10.1787/a1689dc5-en>.


³ "Note by the President of the Security Council," UN Security Council, UN Doc S/2024/215, March 7, 2024  <https://documents.un.org/doc/undoc/gen/n24/032/68/pdf/n2403268.pdf>.

TABLE 1

Summary of Cyberthreats from the DPRK

Target	Purpose	Content
Defense industrial bases	To obtain intellectual property or other information, such as designs and blueprints, that can advance the country's weapons of mass destruction and ballistic missile programs. Such information could also be sold to generate revenue for these programs.	The Lazarus Group attacked defense sector companies around the globe. In 2022, it compromised a Spanish aerospace company, obtaining initial access to its network through a spear-phishing campaign. In this campaign, DPRK actors posed as recruiters on LinkedIn, Telegram, and WhatsApp, convincing targets to execute malware as part of the fraudulent hiring process.
		Between December 2022 and March 2023, Andariel targeted telecommunications companies, research institutions, universities and information technology companies, the defense industry, and financial companies in the ROK, stealing 1.2 terabytes of data, including sensitive information on surface-to-air laser weapon systems.
Supply chain attacks (e.g., on software providers)	To access multiple networks in sectors of interest through a single intrusion, utilizing multiple attack vectors, including spear phishing, public open-source code repository "poisoning," and manipulation of profiles on industry-specific platforms.	In July 2024 the software-as-a-service provider JumpCloud was compromised by DPRK actors associated with cryptocurrency heists. The intrusion was likely achieved through a sophisticated spear-phishing campaign. This compromise might have resulted in at least two cryptocurrency heists with a combined value of \$147.5 million.
		The Lazarus Group and Andariel exploited a remote-code execution vulnerability affecting the JetBrains TeamCity server, a widely used application for software development.
Global enterprises (e.g., manufacturing, agricultural, and physical security companies)	To infiltrate and exploit large-scale organizations across critical industries for financial gain, intelligence gathering, and supply chain disruption. DPRK-affiliated threat actors employ various attack vectors, including spear phishing, Trojanized software, and watering-hole attacks, to gain persistent access to enterprise networks and exfiltrate sensitive data.	The Lazarus Group has employed at least three new DLang-based malware families, including two remote-access Trojans. One of these Trojans used Telegram bots and channels for command and control. The group is increasingly using open-source tools and frameworks in the initial access phase of its attacks to avoid profiling and prevent raising early red flags.

Table 1 continued

<p>Neighboring countries (e.g., government agencies, companies, and individuals in China and Russia)</p>	<p>To gather intelligence, monitor geopolitical developments, and exploit economic and technological resources through cyber espionage and financially motivated attacks. DPRK-affiliated threat actors conduct persistent cyberoperations against government institutions, financial entities, media organizations, and technology firms in neighboring countries to support strategic objectives, including sanctions evasion, diplomatic maneuvering, and military advancements. These operations also establish footholds within critical infrastructure for potential future exploitation.</p>	<p>In 2023 the Lazarus Group ranked seventh in attacks targeting China, focusing particularly on the government and financial sectors. The group controlled 6% of Chinese Internet Protocol addresses and 9% of Chinese command and control servers. Kimsuky ranked ninth in attacks targeting China, focusing on the government, media, education, and finance sectors, and controlled 3% of Chinese Internet Protocol addresses and 4% of Chinese command and control servers. The Lazarus Group is still reportedly active in Russia.</p>
<p>Mobile applications</p>	<p>To steal information from infected devices.</p>	<p>Kimsuky continues to create malicious Android mobile applications disguised as legitimate apps, including a popular e-commerce service, a security plug-in Google Authenticator, an anti-virus program, and a payment service app. The fake applications reportedly mimic the legitimate ones in icons, features, and size. The malicious applications were likely distributed via spear phishing or smishing.</p>
<p>Artificial intelligence</p>	<p>To leverage artificial intelligence models to accelerate malicious software development and identify systems to exploit.</p>	<p>Kimsuky has shown interest in using generative artificial intelligence, including large language models, potentially for coding or writing phishing emails. Kimsuky has been observed using ChatGPT.</p>

Source: “Note by the President of the Security Council”; Peter Kálnai, “Lazarus Luring Employees with Trojanized Coding Challenges: The Case of a Spanish Aerospace Company,” WeLiveSecurity, September 29, 2023 ~ <https://www.welivesecurity.com/en/eset-research/lazarus-luring-employees-trojanized-coding-challenges-case-spanish-aerospace-company>; Insikt Group, “North Korea-Aligned TAG-71 Spoofs Financial Institutions in Asia and U.S.,” Recorded Future, June 6, 2023 ~ <https://www.recordedfuture.com/research/north-korea-aligned-tag-71-spoofs-financial-institutions>; Microsoft Threat Intelligence, “Multiple North Korean Threat Actors Exploiting the TeamCity CVE-2023-42793 Vulnerability,” Microsoft, October 18, 2023 ~ <https://www.microsoft.com/en-us/security/blog/2023/10/18/multiple-north-korean-threat-actors-exploiting-the-teamcity-cve-2023-42793-vulnerability>; Jonathan Greig, “New Malware from North Korea’s Lazarus Used Against Healthcare Industry,” Record, August 25, 2023 ~ <https://therecord.media/lazarus-new-malware-manageengine-open-source>; and Song Sang-ho, “N. Korea Tries to Use Artificial Intelligence to Write Malicious Software: U.S. Official,” Yonhap News, October 19, 2023 ~ <https://en.yna.co.kr/view/AEN20231019000600315?input=tw>.

Cybersecurity concerns arising from the Russia-Ukraine conflict. At the outset of the Russia-Ukraine war, a major cyberoperation targeted U.S. firm Viasat's KA-SAT satellite network, causing significant disruptions in network connectivity across Ukraine, France, and Germany. This incident highlighted how cyberthreats can transcend geographic boundaries, affecting countries not directly involved in a conflict and emphasizing the interconnection between cybersecurity and the security of outer space. Although this essay does not explicitly evaluate the effectiveness of cyberwarfare, it is crucial to address the growing concerns about Russia's cyber capabilities and their potential ramifications for neighboring countries.

The deterioration of diplomatic relations between the ROK and Russia has heightened concerns regarding potential cyberattacks on South Korea, particularly following Russian president Vladimir Putin's 2024 visit to North Korea. Russia also has a history of cyberoperations against South Korea, notably during the Pyeongchang Winter Olympics in February 2018.⁴ Despite the absence of Russian teams from the events, Russian cyberattackers conducted disruptive attacks and attempted to obfuscate their involvement by mimicking methods associated with the DPRK.

In June 2024, a series of distributed denial-of-service attacks targeted 22 sites in South Korea, including key government ministries such as the Presidential Office, the Ministry of Industry, the Ministry of Foreign Affairs, the National Police Agency, and the National Tax Service, along with other institutions and companies. These attacks could have significantly disrupted the operations of critical government ministries and institutions, highlighting the vulnerability of critical infrastructure to cyberthreats. A Russian hacker group claimed responsibility for these attacks, citing as the motive dissatisfaction with South Korea's support for Ukraine.⁵ Such incidents raise concerns about the possibility of future cyberattacks targeting the ROK, especially if Seoul decides to extend military support to Ukraine. This evolving cyberthreat landscape necessitates a robust and proactive cybersecurity posture to safeguard national security and critical infrastructure.

⁴ Ellen Nakashima, "Russian Spies Hacked the Olympics and Tried to Make It Look Like North Korea Did It, U.S. Officials Say," *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.

⁵ Kim Kyung-ae, "Hanguk jeongbu saiteu 22gae tagiteuro DDoS gonggyeok sido pochak...Reosia haekeo sohaeng jujang" [Attempted DDoS Attack Targeting 22 South Korean Government Websites Detected...Claims of Russian Hacker Involvement], *Boan News*, June 18, 2024 ~ https://m.boannews.com/html/detail.html?tab_type=1&idx=130643.

China's cyberthreat. Concerns are growing about the potential for cyberattacks from China, particularly in the context of rising anti-Korean sentiment and tensions related to the issue of Taiwan. In January 2023 a Chinese cyberattack group, Xiaoshiying, publicly announced plans to target entities in South Korea. Following this declaration, the group targeted websites with relatively weak security measures, including those of domestic research institutes and academic societies. On February 19, Xiaoshiying unexpectedly posted a message on Telegram stating, "Our action ends here without any follow-up."⁶ The motivations behind the cyberattacks remain unclear but are believed to have been fueled by anti-Korean sentiment.

Despite this announcement, Xiaoshiying re-emerged on April 22, attacking the website of Infra Information Technology Co., a major infrastructure construction company.⁷ The Korea Internet and Security Agency's investigation revealed that the group had employed various cyberattack techniques, such as exploiting vulnerabilities and falsifying webpages. After the attack, Xiaoshiying claimed on Telegram to have stolen sensitive data, including employee emails and contacts from Korean infrastructure firms. A subsequent post suggested a plan to manipulate the stock market by launching cyberattacks to inflate the stock prices of Korean security companies.⁸ This strategy likely involved purchasing stocks in advance, expecting public awareness of the cyberattacks to increase demand for security services, thereby increasing stock prices.

The continuous rise in cyberattacks from North Korea, alongside the emerging threats from Russia and China, underscores the growing cybersecurity challenges facing South Korea. As geopolitical tensions persist, the threat of cyberoperations as a tool of statecraft or political expression remains a significant concern. This necessitates robust defensive measures and international cooperation to mitigate these threats. How well does South Korea perform in terms of cyber resilience?

⁶ "Cyber Security Reports," NTT Security Japan, February 2023 \approx <https://www.security.ntt/reports/Cyber-Security-Reports-2023-02-2.pdf>.

⁷ Park Eun-ju, "Jungguk haekinggeurup Syaochiing, guknae gieop tto dashi haeking gonggyeok" [Chinese Hacking Group Xiaoshiying Launches Another Cyberattack on a South Korean Company], Boan News, April 22, 2023 \approx <https://m.boannews.com/html/detail.html?idx=117388>.

⁸ Kim Hye-kyung, "'Juga oreul teni maesu-hara' jung haekedeul-ui hwangdanghan 'saibeo gonggyeok'" ["Stock Prices Will Rise, So Buy": Hackers' Absurd Cyberattack], iNews24, April 24, 2023 \approx <https://www.inews24.com/view/1588143>.

Resist: South Korea's National Cybersecurity Strategy in 2019 and 2024

Recognizing the critical need for a robust cybersecurity framework, the ROK government launched its first comprehensive National Cybersecurity Strategy in 2019.⁹ This strategy established cyberspace as an independent operational domain and underscored its significance for national defense. The strategy laid foundational goals to enhance domestic information protection capabilities and safeguard critical infrastructure. However, between 2019 and its second iteration in 2024, South Korea's cybersecurity strategy evolved significantly to address the increasingly complex landscape of cyberthreats and the demand for more sophisticated defense mechanisms.¹⁰ **Table 2** summarizes the evolution of South Korea's cybersecurity strategies and the changes in vision, objectives, principles, and strategic tasks between 2019 and 2024.

The 2024 strategy presents four key features that distinguish it from the 2019 strategy. First, it emphasizes the identification of cyberthreat actors and the development of offensive capabilities. Unlike the previous strategy, the 2024 iteration highlights international and state-sponsored hacking organizations. These include groups responsible for technology theft, election interference, infrastructure attacks, ransomware, and supply chain threats, with a focus on North Korea. The 2024 strategy argues that strengthening defensive capabilities alone is inadequate and outlines necessary response measures to address national security breaches.

Second, the strategy emphasizes global leadership and cooperation with international partners, particularly the United States, Japan, the UK, and like-minded Indo-Pacific countries. It commits South Korea to advocate for universal values in cyberspace, promote norms for responsible behavior, and contribute to a rules-based cyber order. The strategy details measures for conducting investigations, identifying attackers, and issuing joint security advisories. This marks a departure from the more domestically focused approach of the 2019 strategy and positions South Korea to lead international efforts against cyberthreats, especially from North Korea.

Third, the strategy aims to achieve a competitive edge in the technologies essential for cyberdefense. It specifically focuses on the industrialization of critical technologies. Additionally, it aims to establish a cyber

⁹ Office of the President of the Republic of Korea, *Gukga saibeo-anbo* [National Cybersecurity Strategy] (Seoul, 2019).

¹⁰ Office of the President of the Republic of Korea, *Gukga saibeo-anbo* [National Cybersecurity Strategy] (Seoul, 2024).

TABLE 2

Comparison of 2019 and 2024 National Cybersecurity Strategies

	2019 National Cybersecurity Strategy	2024 National Cybersecurity Strategy
Vision	Create a free and safe cyberspace to support national security, promote economic prosperity, and contribute to international peace	Create a global pivotal state that upholds the values of freedom, human rights, and the rule of law in cyberspace and fulfills its roles and responsibilities in the international community
Objectives	<ol style="list-style-type: none"> 1. Ensure stable operations of the state. 2. Respond to cyberattacks. 3. Build a strong cybersecurity foundation. 	<ol style="list-style-type: none"> 1. Create an offensive cyberdefense and attack response system. 2. Expand global leadership. 3. Secure robust cyber resilience.
Principles	<ol style="list-style-type: none"> 1. Balance individual rights with cybersecurity. 2. Conduct security activities based on the rule of law. 3. Build a system of participation and cooperation. 	<ol style="list-style-type: none"> 1. Prioritize balancing the importance of national core values with the economic interests of the citizens in conducting cybersecurity activities. 2. Ensure all stakeholders, including the government, industry, and academia, collaborate to recognize the importance of cybersecurity and jointly respond to threats. 3. Protect the fundamental rights of citizens from concerns such as privacy infringements resulting from cybersecurity activities by performing duties with legitimate purposes and lawful means based on established norms.
Strategic tasks	<ol style="list-style-type: none"> 1. Increase the safety of the national core infrastructure. 2. Enhance cyberattack response capabilities. 3. Establish governance based on trust and cooperation. 4. Build foundations for cybersecurity industry growth. 5. Foster a cybersecurity culture. 6. Lead international cooperation in cybersecurity. 	<ol style="list-style-type: none"> 1. Strengthen offensive cyberdefense activities. 2. Establish a global cyber cooperation framework. 3. Enhance cyber resilience of critical infrastructure. 4. Secure a competitive edge in critical and emerging technologies. 5. Strengthen the operational foundation.

Source: Office of the President of the Republic of Korea, *Gukga saibeo-anbo* [National Cybersecurity Strategy] (Seoul, 2019); and Office of the President of the Republic of Korea, *Gukga saibeo-anbo* [National Cybersecurity Strategy] (Seoul, 2024).

risk-management system to monitor vulnerabilities related to emerging technologies. Rather than listing specific new technologies crucial for cyberdefense, the strategy calls for a collaborative effort among government, industry, and academia to identify and review relevant industrial policy. However, the framework acknowledges the disruptive potential of artificial intelligence and quantum technologies for cybersecurity. Furthermore, it calls for developing a quantum-resistant encryption system and adopting new cryptography standards.¹¹

Last, the strategy outlines a comprehensive national cybersecurity governance framework and defines the roles of the National Security Office (NSO). It includes the establishment of the National Cybersecurity Committee and a cyber governance system centered in the National Intelligence Service (NIS) as the lead operational agency. The 2024 strategy calls for enacting and revising relevant laws, including the National Cybersecurity Basic Act, to support cybersecurity measures.¹²

Recover: The National Cybersecurity Council and National Cyber Risk Management Unit

Since the 2015 creation of the post of secretary to the president for cybersecurity within the cabinet-level NSO, this office has been the highest national authority involved in planning and coordinating cybersecurity issues at a whole-of-governmental level.¹³ The recent establishment of the National Cybersecurity Council, chaired by the third deputy director of the NSO, is a critical initiative to further enhance South Korea's cybersecurity coordination and effectiveness.¹⁴ Comprising officials from fourteen government agencies, including the NIS and the Ministry of National

¹¹ Natasha Wood, "South Korea's 2024 Cyber Strategy: A Primer," Center for Strategic and International Studies August 2, 2024 ~ <https://www.csis.org/blogs/strategic-technologies-blog/south-koreas-2024-cyber-strategy-primer>.

¹² So-jeong Kim, "Gukga saibeo-anbo jeollyak gaejeong-ui teukjing-gwa sisajeom" [Characteristics and Implications of the Revision of the National Cybersecurity Strategy], Institute for National Security Strategy, Issue Brief, no. 512, February 2024.

¹³ Sungbaek Cho, "National Cybersecurity Organization: Republic of Korea," NATO Cooperative Cyber Defence Centre of Excellence, National Cybersecurity Governance Series, 2022 ~ <https://ccdcoc.org/uploads/2022/12/ROK-Country-report.pdf>.

¹⁴ The NSO and the National Cybersecurity Council have distinct functions. The NSO operates under the Office of the President and is responsible for overseeing national security and foreign policy, including cybersecurity at a high level. The National Cybersecurity Council is a specialized body focused on coordinating national cybersecurity policies and strategies across agencies. It plays a key role in shaping South Korea's cybersecurity framework, addressing cyberthreats, and enhancing resilience.

Defense, the council serves as a central body for addressing cybersecurity policies and issues.¹⁵

As the lead cyber crisis-management agency, the NIS coordinates incident responses and serves as the council's secretariat. The council aims to protect national infrastructure and citizens from persistent cyberthreats. It has plans to establish a joint response system with allied nations, reinforcing South Korea's leadership in global cybersecurity affairs. This initiative highlights the government's commitment to resilience and readiness in an evolving cyberthreat landscape.

The council's primary function is to oversee the implementation of the National Cybersecurity Basic Plan and its one hundred action items that operationalize the National Cybersecurity Strategy. Key tasks include bolstering defenses against state-sponsored hacking actions, participating in international cyber norm discussions, establishing cloud security certification, developing quantum-resistant encryption, and expanding cybersecurity training.

Another significant aspect of the council's strategy is fostering cooperation between government agencies and the private sector to combat increasingly sophisticated cyberattacks. To this end, the council aims to facilitate the swift sharing of policies as well as discussions on relevant issues to ensure a unified national response to evolving cyberthreats. However, it has not yet specified its methods to accomplish this.

On May 17, 2023, the NIS and the NSO established the National Cyber Risk Management Unit (NCRMU). This marked the start of full-scale operations for an integrated risk-response team to combat increasingly sophisticated cyberthreats. The NCRMU builds on the foundation of the Civil/Public/Military Joint Response Team established in 2012, expanding its size and functions. It serves as a platform for experts from the NIS, government, public sector, and private sector to collaboratively address national cyber crises under the guidance of the NSO. This approach aligns with the revised "Basic Guidelines for National Crisis Management" introduced in 2023. The NCRMU is staffed with officers from various government ministries, public institutes, and private entities, creating a new

¹⁵ These institutions are the Financial Services Commission; Korea Communications Commission; Ministry of Education; Ministry of the Interior and Safety; Ministry of Foreign Affairs; Ministry of Justice; Ministry of National Defense; Ministry of Oceans and Fisheries; Ministry of Science and ICT; Ministry of Trade, Industry and Energy; Ministry of Unification; Supreme Prosecutors' Office; National Intelligence Service; and National Police Agency. "Daehanminguk daetongryeongsil, gugka saibeo-anbo hyeobuihoe chulbeom" [Launch of the National Cybersecurity Council], Office of the President of the Republic of Korea, Press Release, July 31, 2024 ~ <https://www.president.go.kr/newsroom/press/VMLJwadN>.

public-private partnership model to centralize national cyber risk response efforts under one entity.¹⁶

Adapt: International Coordination in Cybersecurity

South Korea's active coordination with international counterparts has significantly enhanced its cyber resilience, particularly given the transnational nature of cyberthreats. The country participates in various global forums and bilateral partnerships. These include the UN Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace, which addresses the global security context, and the Asia-Pacific Economic Cooperation Telecommunications and Information Working Group, which focuses on regional cooperation. Key institutions such as NIS and the Korea Internet and Security Agency engage in regular information exchanges and collaborative efforts with international organizations to combat cybercrime and cyberespionage. These agencies have established memoranda of understanding with numerous global cybersecurity bodies to facilitate swift responses to cross-border incidents.

South Korea's cybersecurity strategy includes robust bilateral engagements, particularly with the United States, Japan, and the European Union, for sharing advanced technological knowledge and enhancing mutual defense capabilities. Notably, the seventh U.S.-ROK Cyber Policy Consultations, held in January 2024, highlighted the strategic partnership and shared commitment to advancing cybersecurity measures.¹⁷ Further exemplifying South Korea's commitment to international cooperation, the Republic of Korea-UK Strategic Cyber Partnership emphasizes cybersecurity research, policy development, and critical infrastructure protection, reflecting the two governments' shared dedication to democratic values and secure cyberspace.¹⁸

In addition to bilateral relations, the ROK participated in the inaugural U.S.-Japan-ROK Trilateral Diplomatic Working Group Meeting on DPRK

¹⁶ "2023 gukga saibeo-anbo senteo yeollye bogoseo" [National Cyber Security Center 2023 Annual Report], National Cyber Security Center, March 4, 2024 ~ https://www.ncsc.go.kr:4018/main/cop/bbs/selectBoardArticle.do?bbsId=Publish_main&nttId=121713&pageIndex=1&searchCnd2=연례보고서.

¹⁷ U.S. Mission Korea, "7th U.S.-ROK Cyber Policy Consultations," U.S. Embassy and Consulate in the Republic of Korea, Media Note, January 24, 2024 ~ <https://kr.usembassy.gov/012524-7th-u-s-rok-cyber-policy-consultations>.

¹⁸ "Republic of Korea-UK Strategic Cyber Partnership," Prime Minister's Office (UK), Policy Paper, November 23, 2023 ~ <https://www.gov.uk/government/publications/uk-republic-of-korea-strategic-cyber-partnership/republic-of-korea-uk-strategic-cyber-partnership>.

Cyber Activities, which focused on countering North Korean cyberthreats. This trilateral initiative aims to enhance collective cyberdefense through joint threat assessments and synchronized response strategies.¹⁹

South Korea actively participates in international, regional, and bilateral cyber policy dialogues and partnerships, underscoring the importance it places on international cooperation in developing robust cyberdefenses. These collaborations enhance South Korea's cyber resilience and reinforce its role in global cybersecurity initiatives. Despite these efforts, however, challenges to closer integration persist resulting from differences in legal frameworks and varying levels of cybersecurity maturity among partner nations.

Conclusion: Challenges Ahead and Areas for Improvement in South Korea's Cyber Resilience

South Korea's robust cybersecurity approach enables it to resist, recover, and adapt to imminent and evolving cyberthreats. A challenging cyber landscape—characterized by persistent attacks from China, Russia, and North Korea—has compelled ROK officials to institute an ambitious and comprehensive cybersecurity strategy. This strategy emphasizes efficient incident-response mechanisms and international partnerships to bolster cyber resilience.

Nevertheless, the increasing sophistication and persistence of cyberthreats demand ongoing vigilance and strategic foresight. To sustain its resilience, South Korea must address governance challenges, foster innovation, and deepen collaborative efforts through targeted actions in three key areas: governance, resourcing, and talent development.

Fragmented governance. A key challenge lies in South Korea's fragmented governance model, which is built on a patchwork of sector-specific laws addressing information protection and cyberdefense across government, civil, and military domains. While this approach allows for tailored regulations for specific sectors—such as public institutions, telecommunications, critical infrastructure, finance, and military, among others—it lacks a unified, comprehensive foundational law. Existing legislative instruments, including the National Intelligence Service Korea

¹⁹ U.S. Mission Korea, "Inaugural United States–Japan–Republic of Korea Trilateral Diplomatic Working Group Meeting on DPRK Cyber Activities," U.S. Embassy and Consulate in the Republic of Korea, Media Note, December 7, 2023 ~ <https://kr.usembassy.gov/120823-inaugural-united-states-japan-republic-of-korea-trilateral-diplomatic-working-group-meeting-on-democratic-peoples-republic-of-korea-cyber-activities>.

Act and the National Cyber Security Management Regulation, address specific aspects of cybersecurity but fail to provide an overarching framework. The absence of such a law or legal framework hinders the creation of a cohesive national cybersecurity strategy and impedes cross-sectoral coordination. Efforts to enact the National Cybersecurity Basic Act, which aims to centralize cybersecurity governance, have stalled due to political discord, highlighting the difficulties of advancing critical legislation in a polarized environment.²⁰

Uneven financial prioritization. The second challenge is the uneven allocation of financial resources in the country's cybersecurity R&D budget. Despite the government's emphasis on cybersecurity, the 2025 R&D budget for cyberthreat response decreased to 104.9 billion won (\$71.3 million) from 114.1 billion won (\$77.6 million) in 2024. While funding for cryptography-based technologies saw a modest increase, key initiatives such as the Cybersecurity Challenge and Global Data Privacy R&D were eliminated, reflecting inconsistencies in prioritization.²¹ These reductions disproportionately affect smaller firms and critical infrastructure sectors that face challenges in implementing comprehensive cybersecurity measures. This underscores the urgent need for equitable and strategic resource allocation to help ensure holistic national resilience.

A shortage of skilled cybersecurity professionals. The third challenge is South Korea's shortage of skilled cybersecurity professionals, which diminishes the nation's capacity to respond effectively to emerging threats. While the ROK boasts a strong technological base, its cybersecurity workforce has not kept pace with the increasing complexity and volume of cyberthreats. This skills gap is particularly evident in critical sectors such as healthcare and manufacturing, where cybersecurity expertise is less developed. The lack of trained professionals limits the implementation of robust security measures and the development of innovative solutions to address advanced cyberthreats.

This shortage is compounded by insufficient educational programs and professional training opportunities tailored to cybersecurity.

²⁰ Kang Jin-gyu, "Bisang geyeom-tanhaek satae-e...gukga saibeo-anbo gibonbeop jejeong angaetsok" [Martial Law, Impeachment Crisis...The Uncertainty Surrounding the Enactment of the National Cybersecurity Framework Act], Digital Today, December 26, 2024 ~ <https://www.digitaltoday.co.kr/news/articleView.html?idxno=547156>.

²¹ Kim Young-myeong, "Choegeun 5nyeongan gwagijeongtongbu-ui 'saibeo wiheom daeung' gwanryeon R&D yesan salpyeoboni" [Reviewing the R&D Budget for "Cyberthreat Response" by the Ministry of Science and ICT over the Past Five Years], Boan News, September 23, 2024 ~ <https://m.boannews.com/html/detail.html?idx=133018>.

Many universities and technical institutes focus on general information technology education and offer only limited emphasis on specialized cybersecurity disciplines. Additionally, high costs often make private-sector-led training initiatives inaccessible to small and medium-sized enterprises. Addressing this challenge will require a multifaceted approach, including government-funded training programs, public-private partnerships to establish certification standards, and incentives to encourage young professionals to enter cybersecurity. Moreover, regional cooperation could help address the talent shortage. Collaborating with neighboring countries in the Indo-Pacific region could enable South Korea to exchange knowledge and expertise while promoting cross-border training initiatives to build a regional pool of cybersecurity professionals.

Cyber resilience is not a static goal but a dynamic and ongoing process. Progress cannot be taken for granted in an increasingly interconnected and vulnerable digital world. This underscores the urgency of addressing governance challenges to achieve cyber resilience. By embracing a holistic strategy encompassing resistance, recovery, and adaptation, South Korea can safeguard its digital assets and protect its critical infrastructure. Such an approach will also strengthen its leadership role in fostering a secure and resilient cyber environment throughout the Indo-Pacific region. ◆

