CYBER RESILIENCE IN THE INDO-PACIFIC

NUS National University of Singapore

iSAS Institute of South Asian Studies

KONRAD ADENAUER STIFTUNG

About the Institute of South Asian Studies

The Institute of South Asian Studies (ISAS) is dedicated to research on contemporary South Asia. It was established in July 2004 as an autonomous research institute at the National University of Singapore (NUS). The establishment of ISAS reflects South Asia's increasing economic and political importance and the strong historical links between South Asia and Southeast Asia.

The Institute seeks to promote understanding of this vital region of the world and communicate knowledge and insights about it to policymakers, the business community, academia and civil society in Singapore and beyond.

About the Konrad Adenauer Stiftung

The Konrad Adenauer Stiftung (KAS) is a political foundation of the Federal Republic of Germany. Founded in 1964, it was named after the first Chancellor of the Federal Republic of Germany, Konrad Adenauer. KAS offers political and social training activities, conducts research, grants scholarships to students and supports and encourages international understanding and economic development. In addition to the activities of the local KAS offices in many Asian countries, the regional programme "Political Dialogue Asia" organises and sponsors international conferences and seminars. Its numerous events and diverse projects focus on political and social development, political parties and civil society, social market economy, regional security, international cooperation and Asia-Europe relations.

ISAS-KAS Workshop
Cyber Resilience in the Indo-Pacific
Authored by Karthik Nachiappan and Mriganika Singh Tanwar

Cover photographs courtesy of Wikimedia Commons
Printed in Singapore by Oxford Graphic Printers Pte Ltd

Institute of South Asian Studies
National University of Singapore
29 Heng Mui Keng Terrace
#08-06 (Block B)
Singapore 119620
Tel (65) 6516 4239
Fax (65) 6776 7505
URL www.isas.nus.edu.sg

Konrad Adenauer Stiftung
380 Jalan Besar
#11-01 Arc 380
Singapore 209000
Tel (65) 6603 6160
Fax (65) 6227 8343
URL www.kas.de/web/politikdialog-asien

CYBER RESILIENCE IN THE INDO-PACIFIC

Institute of South Asian Studies
Konrad Adenauer Stiftung (Singapore)

May 2025

Karthik Nachiappan
Mriganika Singh Tanwar

Special Report Issue No. 34

CONTENTS

Foreword

The Indo-Pacific is at the heart of global digital transformation. With an expanding digital economy, increasing interconnectivity and the proliferation of emerging technologies, the region is poised for significant economic and societal advancements. However, this rapid digital growth also exposes countries to evolving cyber threats – ranging from cybercrime and espionage to misinformation campaigns and hybrid warfare.

With an expanding digital economy, increasing interconnectivity and the proliferation of emerging technologies, the region is poised for significant economic and societal advancements.

As nations in the Indo-Pacific strive to enhance their cyber resilience, the lessons they learn and the strategies they adopt are of great relevance to Germany, Europe and beyond. This initial thought led to the conceptualisation of a joint project between the Institute of South Asian Studies (ISAS) at the National University of Singapore and the Konrad Adenauer Foundation's (KAS) Regional Programme Political Dialogue Asia at the beginning of 2024, culminating with a ISAS-KAS workshop on 'Cyber Resilience in the Indo-Pacific' in October 2024.

The now finalised publication, *Cyber Resilience in the Indo-Pacific*, provides critical insights into the region's cybersecurity landscape, examining how key players – India, Japan, Indonesia and South Korea – are addressing these challenges. By analysing their approaches to resisting, recovering from and adapting to cyber threats, this study sheds light on regional best practices and offers valuable takeaways for European cybersecurity policy.

In Europe, hybrid threats have become an increasing concern for its security. State-sponsored cyber operations, misinformation campaigns and digital espionage are being used as strategic tools by authoritarian regimes to undermine democracies and destabilise critical infrastructure. For instance, Russia's cyber interference in democratic processes, Chinese-linked cyber espionage and cyberattacks on German and European Union (EU) institutions serve as stark reminders of the need for robust cyber resilience.

The KAS Regional Programme Political Dialogue Asia, within its 'Security Policy' portfolio, is dedicated to providing a dialogue and cooperation platform on these pressing security challenges. Through initiatives like the Asia-Pacific Roundtable in Kuala Lumpur, closed-door workshops, book launches and expert discussions with visiting delegations to Asia, KAS facilitates the exchange between its European and Indo-Pacific partners. This publication is a continuation of that effort, offering a great starting point to look for an informed discussion on the future of cyber resilience.

We now invite policymakers, scholars and cybersecurity professionals to explore the findings in this publication and consider their implications for both regional and global security. Cyber resilience is not just a technical challenge but a strategic imperative (as we have seen repeatedly) — one that demands cooperation, innovation and sustained engagement across borders.

Cyber resilience is not just a technical challenge but a strategic imperative (as we have seen repeatedly) — one that demands cooperation, innovation and sustained engagement across borders.

I would also like to invite readers to have a closer look at KAS' work on domestic security and cybersecurity in Germany, exploring links and parallels between the Indo-Pacific and Europe at www.kas.de/en/domestic-security-and-cyber-security.

We hope this publication provides valuable perspectives and sparks further dialogue on strengthening cyber resilience in an increasingly complex digital world.

Wishing you an insightful and engaging read!

Andreas Klein
Director
Regional Programme Political Dialogue Asia
Konrad Adenauer Stiftung (Singapore)

Executive Summary

Cyber threats have increased in frequency and complexity, creating governance and security challenges for all Asian countries.

The Indo-Pacific region is undergoing profound digital transformation. This shift intersects with intense security competition that exacerbates vulnerabilities in cyberspace. Cyber threats have increased in frequency and complexity, creating governance and security challenges for all Asian countries. This special report maps and analyses the cybersecurity landscape of four Indo-Pacific countries – Indonesia, Japan, South Korea and India. It focuses on and assesses the resilience of these countries facing heightened cyber risks.

The report reveals that these four countries have different cybersecurity challenges and conditions that affect their capacity to mitigate and deter rising cyber risks. There is a variation in how these four Asian countries are handling various cyber threats and incidents, largely shaped by their distinct cyber challenges. India and Indonesia have seen a surge in digital transactions epitomised by the rapid proliferation of e-commerce and financial technology (fintech) in their digital economies while Japan and South Korea face cyberattacks from adversaries keen to exploit their gaps and asymmetries.

Cyber resilience is measured through three key dimensions: *Resistance*, *Recovery* and *Adaptation*. The report underlines that while these four countries benefit from digital innovation, they are becoming targets for nefarious cybercriminals and state-sponsored threat actors seeking to exploit cybersecurity and digital governance gaps. Cybercrimes, data theft, misinformation and disinformation campaigns have become prevalent.

While all four countries have made progressive strides to defend and immediately respond to cyberattacks, differences exist in terms of adaptation or how they protect their cyber architectures over the long term. The report's findings also emphasise the need for a multifaceted, whole-of-government approach when dealing with increasingly sophisticated cyber threats. There is an urgent need to foster collaboration among the Indo-Pacific states to improve the regional cybersecurity infrastructure.

Introduction

During the COVID-19 pandemic, digitalisation accelerated across Asia, making all the sectors in the growing economies heavily reliant on digital technologies.

The Indo-Pacific is characterised by intense security competition. The security dynamics in the region are bound by global and regional interdependencies and interstate rivalries. These rivalries are also intersecting with profound digital transformation. During the COVID-19 pandemic, digitalisation accelerated across Asia, making all the sectors in the growing economies heavily reliant on digital technologies. Citizens, governments and businesses adopted a 'digital first'[1] outlook for new products, services and business models. For instance, India recorded some of the highest volumes of digital transactions globally, and the pandemic propelled the growth of digital infrastructure further.

Similarly, in Indonesia, e-commerce services and fintech dominated the digital economy. Countries like Japan and South Korea, which were technologically advanced even before the pandemic, attracted rapid investment in critical and emerging technologies like artificial intelligence (AI), quantum engineering and the Internet of Things (IoT), among others. Thus, a secure, trusted and inclusive digital infrastructure is pivotal in supporting Asia's economic and social development.

Asia's digital transformation accompanies risks. The intense security competition, intersecting with pervasive digitalisation, is creating new cybersecurity threats and vulnerabilities that undermine Asia's growth trajectory. The digital arena, in effect, becomes a space, tool and weapon through which countries jostle for more influence and balance in the Indo-Pacific. However, nefarious cyber incidents, developments and disruptions – driven by state or non-state actors – continue to manifest.

[1] Lu Qilin and Victor Kim, 'Digital First Economy: ICT Infrastructure drives economic evolution for sustainable, inclusive growth', *Huawei*, September 2022, https://www-file.huawei.com/-/media/corp2020/pdf/tech-insights/1/huawei_dfe_whitepaper_asia_pacific.pdf?la=en.

Some Asian countries are being used as popular sites for cybercriminals to launch attacks as hotspots with vulnerable infrastructures or as highly connected hubs that can initiate and execute attacks. Malware attacks have been launched from Indonesia, Malaysia and Vietnam.[2] These disruptions have cast a shadow over regulation, management and mitigation of cyber vulnerabilities. If these vulnerabilities persist, they could undermine digital economic growth, which could add up to US$1 trillion (S$1.35 trillion) to the region's gross domestic product by 2030.[3]

Cybersecurity is particularly challenging for countries like India and Indonesia, which lack adequate cyber capacity to defend themselves against such threats. Other countries like Japan and South Korea that are digitally well-connected and have adopted national cybersecurity strategies, face threats that require greater and sustained policy action and coordination. The need to close digital divides and advance digital transformations versus the lack of a strong cybersecurity posture is a risk to achieving safe, secure and rights-respecting online environments.

The need to close digital divides and advance digital transformations versus the lack of a strong cybersecurity posture is a risk to achieving safe, secure and rights-respecting online environments.

Other cybersecurity threats like cybercrimes, hacking, disinformation and misinformation and data fraud are becoming pervasive. Advancements in AI and mainstreaming of generative AI further complicates cybersecurity.

Thus, cyber resilience is critical to the economic security of the Indo-Pacific.[4] It is defined as the country's ability to resist, recover and adapt against cyber threats. By effectively protecting their digital infrastructures from cyber threats, the countries will be able to secure their digital and economic transformation and the lives and livelihoods of millions of people that use digital technologies.

[2] Arief Subhan, 'Southeast Asia's cybersecurity an emerging concern', *The ASEAN Post*, 20 May 2018, https://theaseanpost.com/article/southeast-asias-cybersecurity-emerging-concern·

[3] Keith Detros, 'Towards a Resilient Cyberspace in Southeast Asia', Tech For Good Institute, May 2023, https://techforgoodinstitute.org/wp-content/uploads/2023/07/TFGI_Cybersecurity_Report_Digital_report.pdf.

[4] Igor Linkov and Alexander Kott. 'Fundamental concepts of cyber resilience: Introduction and overview', *Cyber Resilience of Systems and Networks* (Cham: Springer, 2019), pp 1-25.

The report assesses the cyber resilience of these countries based on three parameters – Resistance, Recovery and Adaptation.

This report explores the pivotal question – what is the state of cyber resilience in the Indo-Pacific? This report outlines the existing cybersecurity landscape of four countries in the Indo-Pacific, namely, Indonesia, Japan, South Korea and India. The report assesses the cyber resilience of these countries based on three parameters – Resistance, Recovery and Adaptation. Substantial gaps exist in understanding and assessment of how specific countries deal with cyber threats domestically, that is, instituting necessary institutional changes to bolster their cyber capacities, and internationally through cybersecurity partnerships and governance.

There is a variation in the Indo-Pacific countries' capacity to resist cyberattacks, recover rapidly and adapt to emerging cybersecurity threats. There is a need to analyse cyber architectures across specific Indo-Pacific countries to ascertain how they deal with cybersecurity challenges and what specific aspects they should focus on to resist cyberattacks, recover rapidly and adapt to emerging cybersecurity threats.

Regional Cyber Landscape

Cybersecurity broadly refers to the actions taken by countries, firms and organisations to protect their networks, systems, infrastructures and data from attacks and unauthorised access.[5] It involves the practice of ensuring the security, accessibility and confidentiality of information. With rapid digitalisation, the ways in which individuals acquire and store information have grown, increasing digital risks. Cyberattacks are rising. There has been a growing reliance on malware or malicious software like spyware and ransomware. Consumers online are more aware of where and how their data is treated.

Governments are drafting laws to protect user data, expecting firms and organisations to eschew cybercrime and theft. Such risks, however, are dynamic, compelling countries and companies to monitor and mitigate disruptions. The rapid shift towards mobile platforms and remote work only increased the risks with more data consumed online. Although users and firms can protect themselves through better password protection and augmenting network security, government intervention is important to bolster national cyber defences against an ever-growing array of threats.

The rapid shift towards mobile platforms and remote work only increased the risks with more data consumed online.

The future cyber landscape in the Indo-Pacific could be dominated by AI-driven attacks, with cybercriminals possibly using generative AI to sow havoc. Social media and generative AI could enable highly targeted scams and impersonations, making it harder to distinguish between real and artificial interactions. Ransomware will evolve, targeting supply chains and critical infrastructure. Increasing cloud adoption will likely expose vulnerable cloud environments and insecure APIs. Supply chain complexities in hardware continue to pose challenges through tampering devices and IoT infrastructure. Fake applications, especially in the fintech and e-commerce areas,

[5] Dan Craigen, Nadia Diakun-Thibault, and Randy Purse, 'Defining cybersecurity', *Technology Innovation Management Review 4*, no. 10 (2014).

are a growing concern. The demographic and social differences in the internet user base also determine how vulnerable the users are to cyber risks.

The majority of attacks targeted financial firms and cryptocurrency businesses to generate revenue.

Additionally, the challenging geopolitical situation could precipitate cyberattacks against critical public infrastructures. State-sponsored cyberattacks are on the rise in the region. Japan and South Korea, in a joint statement with the United States (US), expressed concern regarding the massive influx of malicious cyber activity attributed to North Korea.[6] The majority of attacks targeted financial firms and cryptocurrency businesses to generate revenue. Recently, a cryptocurrency platform in India named WazirX was also targeted by North Korean hackers leading to a loss of more than US$230 million (S$310.2 million).[7]

With such malicious cyber activities increasing, there is a growing need to map the cybersecurity landscape and situation in the region comprehensively. Some countries face a larger number of malware threats and advanced persistent threats (APT) attacks to their critical digital infrastructure like South Korea and Japan while others like India and Indonesia are targeted by spear-phishing campaigns, data breaches, cyber-terrorism and disinformation.

[6] 'Joint Statement of Japan, the Republic of Korea, and The United States', U.S. Mission Korea, 15 November 2024, https://kr.usembassy.gov/111924-joint-statement-of-japan-the-republic-of-korea-and-the-united-states/#:~:text=We%20express%20grave%20concern%20over,destruction%20and%20ballistic%20missile%20programs.

[7] 'WazirX hack and $235 million loss attributed to North Korea', *The Hindu*, 15 January 2025, https://www.thehindu.com/sci-tech/technology/wazirx-hack-and-235-million-loss-attributed-to-north-korea/article69099267.ece.

Cyber Resilience

The Indo-Pacific cannot escape the complexities of emergent cybersecurity challenges. Cyberattacks do not occur in a vacuum. The transnational nature of the cybersecurity problem needs a collaborative solution. *Cyber resilience*, which refers to the ability of an organisation, system or country to prepare for, respond to, recover from and adapt to cyber incidents, is crucial to ensure existing and emerging cyber challenges are addressed effectively. It involves a comprehensive approach that encompasses preventive measures to protect against cyber threats, effective response strategies during incidents and recovery processes to restore operations and data integrity.

This section critically analyses the existing cybersecurity architecture, measures and frameworks in Indonesia, Japan, South Korea and India to ascertain their level of cyber preparedness. These four countries are at the centre of regional security competition and digitalisation. Cybersecurity for these countries is more than a cyber issue. Their cybersecurity is shaped by broader institutional and political conditions. Cyber resilience, therefore, is critical to economic development and security. Simply put, how effectively countries resist, recover and adapt their digital space from evolving cyber threats will determine their socioeconomic development and secure their digital transformation. This report focuses on three aspects of cyber resilience, namely, resistance, recovery and adaptation of the digital infrastructure of Indonesia, Japan, South Korea and India.

Their cybersecurity is shaped by broader institutional and political conditions.

First, resisting cyberattacks on digital systems and infrastructure is of primary importance to business firms and organisations. To defend against cyberattacks, individuals, civil societies and organisations usually follow various measures, legal frameworks and guidelines to manage their information security. Resistance is assessed by measures that firms adopt to identify and manage cybersecurity risks. In a world where over 61 per cent of industry and social interactions occur online, mapping cyber risks and securing online space is a high-

Having a cybersecurity strategy allows states to establish a whole-of-government approach, institutional division of labour and cybersecurity priorities of the state.

priority agenda of countries.[8] Lately, countries, as well as international organisations, have fixed their attention towards drafting and releasing national cybersecurity strategies. Having a cybersecurity strategy allows states to establish a whole-of-government approach, institutional division of labour and cybersecurity priorities of the state. Japan and South Korea have established cybersecurity strategies that have been majorly influenced by their security calculations in the Indo-Pacific. The two countries are more focused on developing offensive cyber capabilities for cyber resilience. On the other hand, India and Indonesia do not possess codified cybersecurity strategies. Instead, they have established regulatory measures to manage cybersecurity challenges.

Second, recovery focuses on the institutions and mechanisms in place to recover from malicious cyber incidents. Countries adopt measures to ascertain the nature of the cyber disruption by sharing relevant information on the event and moving to address it systemically. These mechanisms are vital to not just track and repel cyberattacks but also ensure systems are operating sufficiently during and after the attack. Recovery generally involves computer emergency response teams (CERT) and their operations domestically and regionally. Incident response holds priority for countries. There is a greater synergy in recovery measures between Indonesia, Japan, South Korea and India. A major difference persists in terms of the attribution of cybersecurity incidents. While the governments in Japan and South Korea practise public attribution of cyberattacks and threat actors as part of their response, India and Indonesia rarely release information of attacks to avoid public unrest and panic.

Finally, adaptation assesses a country's willingness to engage with the private sector and international partners and focuses on cyber investment and public spending. It also emphasises coordination between relevant domestic and international partners on cyber

[8] Wasyihun Sema Admass et.al., 'Cyber security: State of the art, challenges and future directions', *Cyber Security and Applications*, Vol. 2, 2024, https://www.sciencedirect.com/science/article/pii/S2772918423000188#bib0004.

risks. Adaptation covers the financing and resource allocation for cybersecurity strategy.

The cyber threats are transnational in nature. The Indo-Pacific countries are fostering international cooperation in cyber resilience. For example, India and Japan have been collaborating on cybersecurity through the Quadrilateral Security Dialogue (Quad). Japan and South Korea have well established security partnerships with the US and closely cooperate on cybersecurity issues. Indonesia, on the other hand, has limited cyber partnerships in the region. A greater focus on adaptation is necessary to ensure sustainable cyber policies in the long run.

The Indo-Pacific countries are fostering international cooperation in cyber resilience.

Table 1: Cyber Resilience Framework – Resistance, Recovery and Adaptation

Countries	RESISTANCE	RECOVERY	ADAPTATION
	Measures adopted to identify and mitigate cyber risks	**Mechanisms to recover from cyberattacks**	**Engagement with private sector and international counterparts to cyber threats**
Indonesia	No codified cybersecurity strategy	Computer Security Incident Response Teams (CSIRTs)[9]	Multilateral cybersecurity collaboration *For example: the Association of Southeast Asian Nations' cybersecurity cooperation strategy; United Kingdom-Indonesia memorandum of understanding on cyber security cooperation; US-Indonesia maritime cybersecurity exercises in the Indo-Pacific*
		No public attribution	Private sector partnerships *For example: Indonesia's National Cyber and Crypto Agency partnership with Honeynet Project*
Japan	Cybersecurity Strategy 2021[10]	Japan Computer Emergency Response Team (JPCERT)[11]	International information sharing mechanism *For example: JPCERT's early warning information sharing system with global CSIRT communities*
		Public attribution of cyberattacks	Regional cyber cooperation *For example: Development of counter cyberattack grid for the Indo-Pacific; the Quad cybersecurity partnership*
India	No codified Cybersecurity Strategy	Computer Emergency Response Teams (CERT-IN)[12]	Regional cyber cooperation *For example, the Quad cybersecurity partnership; US-led Counter ransomware initiative*
		No public attribution	International information sharing mechanism *For example: CERT-IN's cybersecurity exercise with the G20 countries*
South Korea	National Cybersecurity Strategy 2024[13]	Korean Computer Emergency Response Team (KrCERT)[14]	International information sharing mechanism *For example: KrCERT chairing the Asia Pacific Computer Emergency Response Team to expand international cybersecurity incident response*
		Public attribution of cyberattacks	Private sector engagement *For example: Korea Internet & Security Agency's cyber threat analysis system to support cyber threat assessment and management in private sector; Comprehensive Plan for Information Security in Private Sector (2019)*
			Multilateral cybersecurity collaboration *For example, UK-South Korea strategic cyber partnership; US-South Korea cyber dialogue; US-Japan-South Korea trilateral diplomatic working group on North Korea's cyber activities*

Source: Authors' own computations based on various sources

[9] Computer Security Incident Response Team Indonesia, [Update 2025], https://csirt.or.id/c/pengetahuan-dasar.

[10] 'Cybersecurity Strategy 2021', Government of Japan, 28 September 2021, https://www.nisc.go.jp/eng/pdf/cs-senryaku2021-en.pdf.

[11] Japan Computer Emergency response Team Coordination Center, [Update 2025], https://www.jpcert.or.jp/english/.

[12] Indian Computer Emergency Response Team, Ministry of Electronics and Information Technology, Government of India, [Update 2025], https://www.cert-in.org.in/.

[13] 'National Cybersecurity Strategy 2024', Government of Republic of Korea, 2024, https://www.president.go.kr/newsroom/press/gdXzwtKB.

[14] Korean Computer Emergency Response Team, Korea Internet & Security Agency, [Update 2023], https://www.krcert.or.kr/en/main.do.

Indonesia

Indonesia is rapidly digitalising. In recent years, the archipelagic state has become a hub of e-commerce and fintech. It is forecasted to be the fastest growing market for the digital payments industry with a penetration rate of 69 per cent by 2028.[15] Indonesia's digital transactions amount to 40 per cent (US$77 billion [S$104 billion]) of Southeast Asia's total.[16] The number of Indonesians connected online increased from 88.1 million in 2014 to 221.5 million in 2024.[17] It has been estimated that Indonesia's digital economy will be US$360 billion (S$489.6 billion) in 2030.[18] Indonesia has fostered a healthy start-up ecosystem, dense with e-commerce, technology start-ups and fintech firms. It has a booming AI market and has been making steady progress in innovation, engineering and research and development (R&D) of critical technologies. Increased digitalisation, however, makes Indonesia more susceptible to cyber threats.

Indonesia has fostered a healthy start-up ecosystem, dense with e-commerce, technology start-ups and fintech firms.

Cyber incidents are targeting various sectors, including government, defence, energy, telecommunications and finance. This increase in incidents is characterised by both the density and sophistication of cyberattacks, such as botnet infestation, data breaches, hacktivism, cyber-terrorism, disinformation campaigns, phishing schemes, ransomware attacks and cyber fraud. There has been an increase in state-sponsored cyber operations. Indonesia's cybersecurity agency identified over 4.4 million activities by hacking groups known to be APTs.[19]

Indonesia is also experiencing increasing cybercrime that manifests through stolen data, credentials and unsolicited access to digital

[15] 'Penetration rate of the digital payments market in Indonesia from 2018 to 2028', *Statista*, 9 February 2024, https://www.statista.com/forecasts/1326599/indonesia-digital-payments-market-penetration-rate.

[16] Kartina Sury, 'Indonesia's Cyber Resilience: At the Epicenter of ASEAN Digital Economy Growth', Tech For Good Institute, https://techforgoodinstitute.org/blog/expert-opinion/indonesias-cyber-resilience-at-the-epicenter-of-asean-digital-economy-growth/.

[17] 'Survei Internet APJII 2024, Association of Indonesian Internet Providers, https://survei.apjii.or.id/.

[18] 'e-Conomy: SEA 2023: Reaching New Heights – Navigating the Path to Profitable Growth', Google, Temasek, Bain & Company, 2023, p 86, https://www.temasek.com.sg/content/dam/temasek-corporate/news-and-views/resources/reports/google-temasek-bain-e-conomy-sea-2023-report.pdf.

[19] Prashant Singh Parihar, 'Indonesia's Growing Cyber Threats: Why Action is Urgent Now', *Linkedin Blog Post*, 21 November 2024, https://www.linkedin.com/pulse/indonesias-growing-cyber-threats-why-action-urgent-now-parihar-1gxhc/.

systems. In 2013, Indonesia became the largest source of online criminal activity, overtaking China.[20] There has been a marked rise in data fraud targeting Indonesian businesses and private companies, particularly concerning the sale of data like sensitive employees and customer information on dark web marketplaces. Cybercriminals often gain unauthorised access to financial and governmental systems, posing severe security and reputational risks to individuals and organisations. Data leaks and identity theft accounted for 88 per cent of cyberattacks.[21]

The volatile cybersecurity landscape raises concerns over Jakarta's cyber capabilities and readiness to deter and manage emerging threats.

Moreover, ransomware continues to rise as a threat, with several high-profile attacks on Indonesian firms. Jakarta is also particularly wary of cyberterrorism, weaponisation of the internet for recruitment in terrorist activities and political propaganda. The volatile cybersecurity landscape raises concerns over Jakarta's cyber capabilities and readiness to deter and manage emerging threats. Against this backdrop, there is a need for heightened vigilance, proactive security measures and continued investment in cybersecurity to close prevailing gaps.

Resistance

Indonesia's cybersecurity capacity to resist, recover and adapt remains broadly mixed. There is growing cybersecurity awareness in the public domain. However, the Indonesian government has yet to formalise a cybersecurity strategy. Instead, the Joko Widodo (Jokowi) government formally established a series of legal and institutional measures to defend itself against cyber threats. The Ministry of Communications and Digital Affairs (MCDA) rolled out its Strategic Plans 2020-2024, in which it divided the responsibilities of cyber defence and data protection between the National Cyber and Crypto Agency (BSSN) and the MCDA. The plan includes regulatory measures for emerging

[20] Lily Kuo, 'Indonesia just passed China as the world's top apparent source of cyber attacks', *Quartz*, 16 October 2013, https://qz.com/135984/indonesia-just-passed-china-as-the-worlds-top-apparent-source-of-cyber-attacks.

[21] Kartina Sury, 'Indonesia's Cyber Resilience: At the Epicenter of ASEAN Digital Economy Growth', Tech for Good Institute, https://techforgoodinstitute.org/blog/expert-opinion/indonesias-cyber-resilience-at-the-epicenter-of-asean-digital-economy-growth/.

technology like AI and machine learning and the importance of digital government services. The BSSN provides recommendations on industry standards for cybersecurity, builds awareness of cyber threats and ensures cyber hygiene through capacity building and training.

There are legal frameworks such as the Law on Electronic Information and Transactions (2008) which form the basis of regulating cyberspace by criminalising computer intrusions and illegal wiretapping.[22] Building on this law, the Data Protection Act (2022) was introduced after the Bjorka data leaks incident which exposed a massive amount of personal data onto the dark web.[23] This law provides stringent regulations against data breaches in the public and private sector. It also obliges the institutions under a cyberattack to notify data subjects within 72 hours of data breach. Major information and communications technology (ICT) firms like CISCO, Microsoft and Huawei have worked closely on cybersecurity capacity development and information sharing. However, the lack of coordination and trust between the government and industry still persists. In fact, a cybersecurity strategy could narrow such gaps but the lack of support from the business community and bureaucratic rivalry have delayed the progress on the bill.[24]

In fact, a cybersecurity strategy could narrow such gaps but the lack of support from the business community and bureaucratic rivalry have delayed the progress on the bill.

Recovery

The Indonesian government has taken persistent measures to improve cyber incident response. In 2022, the BSSN became responsible for cyber crisis management, involving the deployment of digital forensics during cyberattacks, supporting post-attack recovery measures and setting up the Computer Security Incident Response Teams (CSIRTs) across government agencies. Besides the BSSN, the national police

[22] Gatra Priyandita, 'Indonesia's Cybersecurity Woes: Reflections for the Next Government', Centre for Strategic and International Studies (CSIS), 12 February 2024, https://s3-csis-web.s3.ap-southeast-1.amazonaws.com/doc/CSIS_Commentaries_CSISCOM00624.pdf?download=1.

[23] Yanuar Nugroho, 'The #Bjorka Case and Ratification of Indonesia's PDP Law: Confronting Digitalisation', *Fulcrum*, 29 September 2022, https://fulcrum.sg/the-bjorka-case-and-ratification-of-indonesias-pdp-law-confrontingdigitalisation/.

[24] Gatra Priyandita, 'Indonesia's Cybersecurity Woes: Reflections for the Next Government', Centre for Strategic and International Studies (CSIS), 12 February 2024, https://s3-csis-web.s3.ap-southeast-1.amazonaws.com/doc/CSIS_Commentaries_CSISCOM00624.pdf?download=1.

have their own cybercrime unit responsible for the investigation of cyber threats. In 2024, Jakarta announced plans to establish a cyber force.[25] Additionally, the MCDA is developing a national digital firewall to safeguard the country's cyberspace from malicious attacks.[26]

This law could strengthen the cybersecurity infrastructure to detect threats, allocate responsibilities to existing institutions and establish penalties for violations.

After the BSSN absorbed the powers of the Indonesia Security Incident Response Team on Internet and Infrastructure in 2018, it issued several regulations requiring critical information infrastructure operators to design frameworks to defend against cyberattacks in real-time, report incidents to the BSSN and other parties and disseminate information for effective prevention and mitigation of future incidents. However, Indonesia is yet to pass a cybersecurity bill, which was proposed in 2019. This law could strengthen the cybersecurity infrastructure to detect threats, allocate responsibilities to existing institutions and establish penalties for violations. It would facilitate organisational discipline in managing and safeguarding data.

Adaptation

Indonesia has adapted to its cybersecurity challenges by actively engaging in cyber diplomacy and multilateral collaborations. Indonesia has been involved with the United Nations (UN) and the Association of Southeast Asian Nations as a 'bridge builder' in defining and defending cyber norms. Indonesian officials have emphasised advocacy of two issues multilaterally. These include deterrence of use of cyber weapons by state actors and cyber terrorism. Indonesia has also developed bilateral relationships with countries including Australia, China, South Korea and the US, focusing on cyber information sharing and capacity building to protect its critical infrastructure and draft international legal frameworks to advance cybersecurity.

[25] 'New 'Cyber Force': Indonesia to launch fourth military branch to combat online threats and attacks', *Channel News Asia*, 24 September 2024, https://www.channelnewsasia.com/asia/indonesia-cyber-force-military-4627456.

[26] Samaya Dharmaraj, 'Indonesia Accelerates Cybersecurity to Support Digital Transformations', Open Gov, 14 December 2024, https://opengovasia.com/2024/12/14/indonesia-accelerates-cybersecurity-to-support-digital-transformation/.

The BSSN is collaborating with the Honeynet Project, an American initiative of cybersecurity professionals working closely with Indonesian government agencies to detect the cyber threat landscape of the state, investigate cyberattacks and develop open-source security tools for internet security. Adaptation also requires close coordination with the private sector and civil societies. Here, the BSSN has been working with the industry on cyber capacity building and information-sharing mechanisms. Jakarta has also dedicated a small portion of its budget to improving the security of the government computer systems. However, for the BSSN, which is tasked with training cyber professionals, under-resourcing and underfunding are major challenges. Compliance is another key challenge. Despite the regulatory standards and reporting mechanisms in place, the industry is cautious of reporting cyber incidents, fearing reputational damages and potential public backlash.

Despite the regulatory standards and reporting mechanisms in place, the industry is cautious of reporting cyber incidents, fearing reputational damages and potential public backlash.

Cybersecurity is not an immediate priority for the Indonesian government. Even though the Jokowi government launched initiatives for digital talent development and digital literacy, human capital, in terms of cybersecurity expertise, is not at par with rapidly evolving cyber threats. Under President Prabowo Subianto, there is speculation on whether the BSSN will exist. Furthermore, contradictions in laws and regulations, inter-agency rivalries and weak authority to enforce cyber standards dent cyber resilience.

Japan

This digital transformation has exposed Japan's digital infrastructure to sophisticated cyber threats like APT attacks, state-sponsored cyberattacks, data breaches and phishing attacks.

Japan is a pioneer in information technologies. Growing digital strides have been accompanied with widespread internet penetration in Japanese society. Over 86.2 per cent of the Japanese population are internet users, including the growing use of IoT, AI, 5G and cloud services.[27] This digital transformation has exposed Japan's digital infrastructure to sophisticated cyber threats like APT attacks, state-sponsored cyberattacks, data breaches and phishing attacks. Japan contends with an array of cyber threats varying in type and intensity. Tokyo has recorded a noticeable rise in cyberattacks, with a 35-fold jump in the last 10 years.[28] For example, distributed denial-of-service (DDoS) attacks are increasing in Japan. The number of DDoS attacks identified and reported in 2024 are 15 times higher than in 2023.

Tokyo was prodded to upgrade cybersecurity capabilities in January 2000 when Japanese government agencies, including the Science and Technology Agency and the Ministry of Internal Affairs and Communications, were under cyberattack.[29] In 2011, Tokyo's concerns regarding its cybersecurity capabilities were heightened when Japanese defence contractors namely, Mitsubishi Heavy Industries, IHI Corporation and Kawasaki Heavy Industries were targeted.[30]

Cyberattacks not only disrupt accessibility to websites but potentially threaten critical digital infrastructure like telecommunications, electricity grid, healthcare services and cashless payment systems, among others. Other cyber threats include spear-phishing campaigns and ransomware attacks. In 2023, a nefarious ransomware attack on the Port of Nagoya halted the cargo logistics for almost two days.[31]

[27] 'Internet penetration rate Japan 2014-2023', *Statista*, 31 July 2024, https://www.statista.com/statistics/255857/internet-penetration-in-japan/.

[28] Thisanka Siripala, 'Japan's Rush to Play Cyber Defence Catchup', *The Diplomat*, 14 June 2024, https://thediplomat.com/2024/06/japans-rush-to-play-cyber-defense-catchup/.

[29] Mihoko Matsubara, 'Japan's Cybersecurity Policies', Foundation Office Japan, Regional Economic Programme Asia (SOPAS), Konrad-Adenauer-Stiftung, https://www.kas.de/documents/287213/32541786/22.pdf/ac4775e9-3ef5-4f26-aaee-d852c53650a0?version=1.1&t=1728528033126.

[30] 'Japan defence firm Mitsubishi Heavy in cyberattack', *British Broadcasting Corporation (BBC) News*, 20 September 2011, https://www.bbc.com/news/world-asia-pacific-14982906.

[31] Jiwon Ma, 'Ransomware Attack on Japanese Port is a Warning to US Shipping', Foundation for Defense of Democracies, 18 July 2023, https://www.fdd.org/analysis/2023/07/18/ransomware-attack-on-japanese-port-is-a-warning-to-u-s-shipping/.

Japanese companies and institutions with weak cybersecurity capabilities are becoming easier targets for theft and ransomware attacks. Such security breaches are dangerous and can cause significant monetary and reputational damage.

Resistance

Japan has a sophisticated yet complicated cybersecurity policy. In 2000, the Japanese government acknowledged cybersecurity as a critical domain in its Action Plan for Building Foundations of Information System Protection from Hackers and Other Cyberthreats.[32] Japan recognised cyber as an issue of national security in 2013 which spurred a series of initiatives over the years to bolster cyber defence. Since then, Japan has established safeguards for information privacy and intelligence capabilities that further complement its cybersecurity policy. It has also outlined a clear cybersecurity strategy to defend itself from emerging cyber threats. Tokyo initially focused on protecting civilian infrastructure and government networks from cyberattacks. However, after the adoption of the National Cyber Security Strategy, Japan moved from reactive to proactive cyber defence. The 2021 Cyber Security Strategy outlines basic cybersecurity policies like the Critical Infrastructure Protection and General Framework for Secure IoT Systems, and establishes management, safety and technical standards for government agencies.[33] Tokyo's cybersecurity strategy focuses on strong R&D to understand the complexities of cyber threats. The strategy aims to resist cyberattacks by early detection and defence mechanisms.

Japan recognised cyber as an issue of national security in 2013 which spurred a series of initiatives over the years to bolster cyber defence.

Recovery

Japan's cybersecurity posture changed in 2022 after the announcement of the National Security Strategy and the Defense Buildup Programme. It introduced the Active Cyber Defence Bill to

[32] Erkeley Ukhanova, 'Cybersecurity and cyber defence strategies of Japan', Euro-Asian Law Congress, 2021, https://www.shs-conferences.org/articles/shsconf/pdf/2022/04/shsconf_eac-law2021_00159.pdf.

[33] 'Cybersecurity Strategy 2021', Government of Japan, 28 September 2021, https://www.nisc.go.jp/eng/pdf/cs-senryaku2021-en.pdf.

Persistent cyberattacks on critical infrastructure accelerated the need for preemptive action against cyber adversaries.

augment cyber and information warfare capabilities. This shift was the result of an extended cyberattack campaign by China since 2019.[34] The Chinese hacker group, MirrorFace has repeatedly engaged in cyber espionage and intrusion against critical infrastructure in Japan.[35] Japan's National Police Agency (NPA) attributed 200 cyber incidents between 2019 and 2024 to MirrorFace across government agencies, defence organisations, space research centres and private firms.[36] These organisations contain critical information on government officials, technologies and national security. Persistent cyberattacks on critical infrastructure accelerated the need for preemptive action against cyber adversaries.

The Active Cyber Defence Bill has three objectives – reinforcement of public-private cooperation, monitoring and collection of online communication data from domestic telecommunication providers and implementation of measures for preemptive strike on an attacker's server.[37] The law mandates companies to report cyberattacks to the government, which, in turn, will advise them on how to manage cyber incidents. The legislation also allows the government to monitor cross-border communications channels if a cyberattack is suspected.[38] Preemptive actions will be conducted by the NPA to neutralise cyber threats.[39] The Japanese government has also attributed and sanctioned malicious cyber actors and joined internationally coordinated public attribution. These measures increase Japan's potential to identify and respond to cyber threats timely.

Two key institutions are responsible for cybersecurity – the National Center of Incident Readiness and Strategy for Cybersecurity (NISC) that focuses on protecting critical infrastructure and the National

[34] Abhishek Sharma, 'Japan's cybersecurity shift: Adoption of Active Cyber Defence Posture', Observer Research Foundation, 21 March 2025, https://www.orfonline.org/expert-speak/japan-s-cybersecurity-shift-adoption-of-active-cyber-defence-posture.

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

[36] Ibid.

[37] Daisuke Akimoto, 'Japan Is Ready to Legalize 'Active Cyber Defense'', *The Diplomat*, 24 January 2025, https://thediplomat.com/2025/01/japan-is-ready-to-legalize-active-cyber-defense/.

[38] Ibid.

[39] Ibid.

Security Secretariat, which oversees national security issues, including cyber threats. The NISC's cybersecurity strategies require it to work closely with the private sector, which is regulated by government agencies through industry-specific acts, laws and standards. These regulations ensure effective identification and timely reporting of cyber incidents. Government agencies such as the National Police Agency or the Japan Computer Emergency Response Team (JPCERT) Coordination Center reports the incident to the NISC, which manages all incident responses. The NISC then shares this information with international partners to organise cybersecurity responses. Through its early warning information sharing system, the JPCERT is crucial in coordinating with the CERTs of partner countries, private sector entities and global CSIRT communities. The JPCERT has also been involved in regional cyber capacity initiatives.

Adaptation

Japan has been actively engaging its Indo-Pacific counterparts to advance regional cybersecurity. Japan has proposed the development of a counter-cyberattack grid for the Indo-Pacific region to defend itself and its allies from cyber threats.[40] The Japanese foreign ministry has allocated US$75 billion (S$101.6 billion) in its 2024 draft budget to strengthen cybersecurity cooperation with South and Southeast Asian countries.[41] At the 2021 Quad Leaders' Summit, the Quad Senior Cyber Group (QSCG) was created in line with the commitment of the members to collaborate on cybersecurity matters. The QSCG met in 2023 to advance a positive and ambitious cyber agenda, outlining regional cooperation on secure cyberspace and fostering an international digital economy. The Quad Cybersecurity Partnership prioritises capacity building and regional supply chain resilience in its agenda. In 2020, Japan signed the Individual Partnership and Cooperation Programme with the North Atlantic Treaty Organization

Japan has proposed the development of a counter-cyberattack grid for the Indo-Pacific region to defend itself and its allies from cyber threats.

[40] Inder Singh Bisht, 'Japan Plans Counter-Cyber Attack Grid for Indo-Pacific', *The Defence Post*, 30 August 2023, https://thedefensepost.com/2023/08/30/japan-counter-cyber-attack/.

[41] Pratnashree Basu, 'From reactive to proactive: Japan's advances in cybersecurity and cyber defence strategies', Observer Research Foundation, India, 27 March 2024, https://www.orfonline.org/expert-speak/from-reactive-to-proactive-japan-s-advances-in-cybersecurity-and-cyber-defence-strategies.

to deepen its collaboration over cyber defence. Japan's growing cybersecurity budget, regional capacity-building initiatives, robust incident reporting mechanisms and public-private partnerships are leading its intent to become a leading 'cyber power'. However, Japan's cybersecurity strategy has been primarily shaped and conditioned by the US' security agenda.

Recently, Tokyo increased investments in the cyber domain, covering human capital and capacity development.

Japan suffers from understaffed cybersecurity units. The NISC had 191 personnel in 2018 with most working for the NISC being part-timers (civilians) or primary employees of other government agencies. Recently, Tokyo increased investments in the cyber domain, covering human capital and capacity development. In 2020, around US$237.1 million (S$320.7 million) was allocated to cyber capacity development, including AI-driven systems.[42] The primary beneficiary is the Ministry of Defense – receiving almost 70 per cent for cyber defence. The Council for Science, Technology and Innovation has pioneered capacity development by promoting industry-academia-public coordination to navigate the changing threat landscape. Significant legal and implementation barriers exist, especially since Tokyo's shift towards offensive cyber capabilities. The operationalisation of active cyber defence remains a major challenge.

[42] Ibid.

South Korea

South Korea's digital situation is characterised by an advanced broadband infrastructure, leading technology companies and a technology savvy population. South Korea is hyper-connected, with an internet penetration rate of 97.4 per cent of its population.[43] Seoul has made the digital sector a high priority and has become a world leader in semiconductors, crucial for advances in critical and emerging technologies.

However, South Korea has become more vulnerable to digital disruptions. Cyber espionage, ransomware attacks and hacktivist groups are rising. Besides cyberattacks, other threats include cyberattacks on supply chains, financial theft and AI-powered spear phishing campaigns. Threat actors use advanced computing, large language models and AI technologies like ChatGPT for cyberattacks.

South Korea's location deeply affects its cybersecurity. North Korea has long been a severe cyber threat to South Korea, targeting critical infrastructure through its state-sponsored cyberespionage and financial theft. North Korea uses increasingly sophisticated cyber capabilities to conduct its operations. Pyongyang's hacking operations have steadily increased over the past 10 years. The attacks target a wide range of institutions, including defence industries and private enterprises, some of which do not actively track cyberattacks. The country's cyber operations have focused mainly on financial gain and sanction evasion. The theft of virtual assets has become a lucrative avenue. North Korean hackers have been suspected of injecting malware into software supply chains to stage ransomware attacks.[44]

North Korea has long been a severe cyber threat to South Korea, targeting critical infrastructure through its state-sponsored cyberespionage and financial theft.

North Korea aside, deteriorating diplomatic ties with Russia have heightened cyberattacks on South Korea government agencies and

[43] 'South Korea: internet penetration 2000-2023', *Statista*, 6 November 2024, https://www.statista.com/statistics/255859/internet-penetration-in-south-korea/.

[44] Tae Yeon Eom, 'AI and Cybersecurity in Digital Warfare on the Korean Peninsula', *Georgetown Journal of International Affairs*, 10 July 2024, https://gjia.georgetown.edu/2024/07/10/ai-and-cybersecurity-in-digital-warfare-on-the-korean-peninsula/.

firms. These attacks are generally seen as retaliation for South Korea's support of Ukraine. There are growing concerns about potential cyberattacks fueled by anti-Korean sentiment in China, given tensions in the Taiwan Strait. The use of AI for mass malware creation and phishing campaigns has drastically reduced the time required to launch large-scale cyberattacks.

Resistance

Seoul launched its first comprehensive National Cybersecurity Strategy in 2019 to better resist cybersecurity risks. The National Cybersecurity Strategy was revised in 2024 to transition from a defensive to an offensive cybersecurity posture. It highlighted the creation of an offensive cyber defence and attack response system.[45] The 2024 strategy emphasises the identification of cyber threat actors and strengthening cyber offensive defence capabilities. An important feature of the strategy was the identification of international state-sponsored hacking organisations responsible for technological theft, election interference, infrastructure attacks, ransomware attacks and supply chain thefts, with a particular focus on North Korea.

That said, the 2024 strategy has gaps in terms of how South Korea pursues offensive cyber operations.

The 2024 strategy outlines necessary response measures for national security breaches and emphasises cooperation with international partners. The 2024 strategy also details measures for cyber investigations, assessing the cyber threat landscape and issuing joint security advisories, a departure from 2019. Furthermore, the updated strategy provides a competitive edge by inculcating emerging technologies in cyber defence. It also emphasises the importance of attribution. That said, the 2024 strategy has gaps in terms of how South Korea pursues offensive cyber operations.

South Korea's cybersecurity strategy appears committed to boosting cyber resilience. The framework demands strengthening the existing information system, creating minimum-security requirements for

[45] Natasha Wood, 'South Korea's 2024 Cyber Strategy: A Primer', Centre for Strategic and International Studies (CSIS), 2 August 2024, https://www.csis.org/blogs/strategic-technologies-blog/south-koreas-2024-cyber-strategy-primer.

digital infrastructure operations and delivering rapid response in case of system failure. It also proposes the creation of a classification mechanism to assess the severity of cyberattacks. The framework iterates the importance of ICT supply chain security, for which it intends to designate trustworthy product suppliers in the market.

Recovery

Regarding recovery, South Korea recently established a National Cyber Security Council (NCSC) to enhance cybersecurity coordination and effectiveness. It will serve as the central body for addressing cybersecurity challenges and overseeing the implementation of the national cybersecurity strategy. However, the NCSC is a relatively new body and its deliverables are unclear. In 2009, the Korea Internet & Security Agency (KISA) was established under the Ministry of Science and ICT to ensure the digital safety of citizens and businesses through advanced detection and response systems for cybersecurity threats. The KISA operates the Korean Computer Emergency Response Team (KrCERT) for coordinating cyber incident response in the private sector. The KrCERT has a 24-hour cyber incidents and vulnerabilities monitoring system, based on which it provides cybersecurity recommendations and support to businesses. The KISA uses an automated threat information-sharing system called the Cyber Threats Analysis System, through which it circulates updated data on cyber threats to the private sector and academia.[46]

It will serve as the central body for addressing cybersecurity challenges and overseeing the implementation of the national cybersecurity strategy.

Additionally, the 2024 strategy is set to industrialise critical technologies to establish a cyber risk management system to monitor vulnerabilities around the development and application of emerging technologies. The disruptive potential and risks of AI and quantum technologies for cybersecurity have been identified in the strategy to caution against emerging risks. A unique feature of South Korea's cybersecurity strategy is that sector-specific laws ensure tailor-made

[46] Sungbaek Cho, 'National Security Organisation: Republic of Korea', NATO Cooperative Cyber Defence Center for Excellence, 15 December 2022, p. 18, https://ccdcoe.org/uploads/2022/12/ROK-Country-report.pdf.

mechanisms for information protection and cyber defence across the public sector, private sector and society.

Adaptation

Seoul engages in regular information exchange to combat cybercrimes and cyber espionage. South Korea has been increasing its budget for cybersecurity R&D. The government has been persistently pushing for the training of cybersecurity experts in both the public and private sectors. South Korea's National Intelligence Service and the KISA actively coordinate with international counterparts on cybersecurity, including the UN Group of Governmental Experts on Information Security, the Open-ended Working Group and the Asia Pacific Economic Cooperation. In 2023, South Korea was selected as the Chair for the Asia Pacific Computer Emergency Response Team (APCERT).[47] The KrCERT has been proactively involved in the APCERT to expand international cybersecurity incident response in the region.

South Korea also works with the US (US-South Korea Cyber Policy Consultations), Japan (US-Japan-South Korea trilateral diplomatic working group on North Korea cyber activities) and the United Kingdom (UK) [UK-South Korea Strategic Cyber Partnership]. Notably, the US and South Korea have been proactively advancing their cyber defence cooperation through diplomatic mechanisms like the US-South Korea Cyber Dialogue and technical mechanisms like the Cybersecurity and Infrastructure Security Agency's Joint Cyber Defence Collaboration. However, the Mutual Defence Treaty signed between the US and South Korea in 1953 presents a challenge for coordinating cyber defence. As cybersecurity risks become increasingly hybrid in nature, an ongoing assessment of their defence partnership is crucial.

As cybersecurity risks become increasingly hybrid in nature, an ongoing assessment of their defence partnership is crucial.

[47] 'South Korea elected as the Chair to the Asia Pacific Computer Emergency Response Team (APCERT)', *Press Release*, Ministry of Science and ICT, Republic of Korea, 8 November 2023, https://www.msit.go.kr/eng/bbs/view.do?sCode=eng&nttSeqNo=909&pageIndex=&searchTxt=&searchOpt=ALL&bbsSeqNo=42&mId=4&mPid=2.

India

India's digital ecosystem has grown alongside digital penetration and use.[48] Rapid internet adoption across Indian society was facilitated by several digital infrastructure initiatives. India also accounts for a sizeable proportion of the global increase in digital payments, outperforming globally in the share of total real-time payments.[49] New Delhi is integrating the internet into other aspects of daily life, like businesses, education and the government sector. Small businesses like micro, small and medium enterprises and start-ups are seeking new opportunities through digitalisation.

Small businesses like micro, small and medium enterprises and start-ups are seeking new opportunities through digitalisation.

India's expanding digital footprint renders it vulnerable to cyber threats. India ranked second in terms of cyberattacks in Asia, second only to Taiwan.[50] It faces the second-highest encrypted cyberattacks globally.[51] The scale of cyberattacks on India is staggering, demonstrating the relentlessness of emerging cyber threats on India's digital infrastructures. One key cybersecurity threat in India is malware attacks that have evolved to evade signature-based detection methods. Low cyber awareness amongst the Indian population makes them easy targets for malware infections. Additionally, small businesses and start-ups are becoming easy targets of data theft.

Another common cyber threat is data breaches, which occur when the customers' sensitive information is revealed. In 2023, approximately 83 per cent of organisations in India faced cyber incidents, ranging from web attacks, phishing attempts and supply chain infiltration.[52] Malicious software like Stuxnet, Flame and Black Shades present a

[48] 'Internet penetration rate in India 2014-2024', *Statista*, 15 May 2024, https://www.statista.com/statistics/792074/india-internet-penetration-rate/.

[49] 'India leads the world in real-time digital payments, says PM Modi', *India News*, 15 August 2022, https://www.business-standard.com/article/current-affairs/india-leads-the-world-in-real-time-digital-payments-says-pm-modi-122081500622_1.html.

[50] 'India second most targeted nations in terms of cyber attacks: CloudSEK', *The Economic Times*, 2 January 2025, https://economictimes.indiatimes.com/tech/technology/india-second-most-targeted-nation-in-terms-of-cyber-attacks-cloudsek/articleshow/116890873.cms?from=mdr.

[51] Vasudha Mukherjee, 'At 5.2 billion, India ranks 2nd globally in encrypted cyberattacks: Report', *Business Standard*, 12 December 2024, https://www.business-standard.com/technology/tech-news/at-5-2-billion-india-ranks-2nd-globally-in-encrypted-cyberattacks-report-124121200635_1.html#goog_rewarded.

[52] Shruti Sharma, 'Securing India's Digital Future: Cybersecurity Urgency and Opportunities', *The Diplomat*, 20 January 2024, https://thediplomat.com/2024/01/securing-indias-digital-future-cybersecurity-urgency-and-opportunities/.

critical security challenge for India's cyberspace. Cybercrimes like fraudulent calls and impersonation are also on the rise.

Cyberattacks on Indian government agencies also increased by 460 per cent and those on start-ups and small and medium enterprises increased by 508 per cent.

State-sponsored cyberattacks in India rose by almost 278 per cent between 2021 and 2023.[53] Cyberattacks on Indian government agencies also increased by 460 per cent and those on start-ups and small and medium enterprises increased by 508 per cent.[54] As per the India Threat Landscape report published by Cyfirma, a cybersecurity firm based in Singapore, India faces the most cybersecurity challenges from threat actors in Pakistan (6.4 per cent) and China (79 per cent).[55] India's healthcare industry was the most targeted sector, facing about 21.82 per cent of total cyberattacks.[56] The hospitality (19.57 per cent) and banking sectors (17.3 per cent) were also targeted increasingly, showcasing the attacker's interest in industries in charge of handling large volumes of personal and financial data.[57]

According to the CISCO Cybersecurity Readiness Index, only 24 per cent of Indian firms and organisations have the necessary capabilities to defend against cyberattacks.[58] Also contributing to this problem is the widespread accessibility and affordability of AI tools, the threat emerging from hybrid cybersecurity attacks like bot attacks, misinformation campaigns, spam emails and deep fakes.

Resistance

India has significantly improved its cybersecurity posture. It has instituted legislative and organisational measures to resist, recover and adapt to the evolving cyber threat landscape. In 2013, India's Ministry of Electronics and Information Technology (MEITY) unveiled

[53] Annapurna Roy, 'State-sponsored cyberattacks against India up 278% in three years', *The Economic Times*, 6 November 2023, https://economictimes.indiatimes.com/tech/technology/india-most-targeted-country-by-cyber-attackers-report/articleshow/104989856.cms.

[54] Ibid.

[55] 'India: Threat Landscape Report 2020', Cyfirma, 2020, https://www.cyfirma.com/media/2020/11/India-Threat-Landscape-Report_14-Oct-2020-compressed-1.pdf.

[56] Ibid.

[57] Ibid.

[58] 'Cisco Cybersecurity Readiness Index: Resilience in a Hybrid World', CISCO, March 2023, https://www.cisco.com/c/dam/m/en_us/products/security/cybersecurity-reports/cybersecurity-readiness-index/2023/cybersecurity-readiness-market-snapshot-india.pdf.

a cybersecurity policy. The policy was largely a vision and did not identify concrete outcomes. However, it facilitated the establishment of the National Critical Information Infrastructure Protection Center (NCIIPC). The Indian Army published a Joint Doctrine on Cyberspace Operations in 2024, but it is not publicly accessible yet. It deals with offensive cyber operations, use of cyber capabilities for the military and cyber warfare. The other legal frameworks in place to resist cyber threats are legislations like the Information Technology Act (2000) that imposes civil as well as criminal penalties on offensive cyber operations which are effective for managing cyber threats. As mentioned earlier, India does not publicly attribute cyberattacks to specific state or non-state actors.

Recovery

In terms of recovery, India focuses on incident response to cybersecurity challenges. The nodal agency for incident response is the Computer Emergency Response Teams (CERT-IN). The CERT-IN issued a detailed template for reporting cyber incidents in 2022.[59] It also released a Responsible Vulnerability Disclosure and Coordination Policy that carries contact information for reporting cybersecurity vulnerabilities to CERT-IN. The informant is guaranteed to receive a response within 72 hours. Another agency that manages the recovery from cyber incidents is the NCIIPC. In 2017, the NCIIPC published Standard Operating Procedures for Incident Response, which include guidelines on reporting procedures, incident mitigation and the dissemination of information. Additionally, MEITY established the National Cyber Coordination Centre to provide a macroscopic view of the cyber threats faced by India. Another agency called the Indian Cyber Crime Coordination Center (I4C) was set up under the Ministry of Home Affairs to tackle issues related to cybercrimes in India. The I4C provides a framework for law enforcement agencies to combat cybercrimes and improve citizen satisfaction. These measures are vital

The I4C provides a framework for law enforcement agencies to combat cybercrimes and improve citizen satisfaction.

[59] Information Technology Act 2000, Government of India, https://eprocure.gov.in/cppp/rulesandprocs/kbadqkdlcswfjdelrquehwuxcfmijmuixngudufgbuubgubfugbububjxcgfvsbdihbgfGhdfgFHytyhRtMjk4NzY=.

for generating situational awareness of India's cyber threat landscape in the broader Indo-Pacific region.

Adaptation

Interestingly, some states have also allocated their budget at the state level for cyber capacity development and awareness schemes.

The Indian government has increased the budget allocated to cybersecurity institutions and projects. The budget allocated to CERT-IN increased by six per cent to about US$29 million (S$39.15 million) for Financial Year 2025.[60] Interestingly, some states have also allocated their budget at the state level for cyber capacity development and awareness schemes. The majority of the share of the cybersecurity budget goes to MEITY. New Delhi also prioritises cybersecurity research by significantly investing in the Center for the Development of Advanced Computing (CDAC). The CDAC has undertaken several projects, including cyber forensics, biometrics and mobile and web security, among others.

These agencies in India are actively collaborating with their international counterparts through mechanisms like the Quad, the US-led counter ransomware initiative and cybersecurity exercises involving the CERTs of the G20 countries. In 2023, India and Japan engaged in pivotal talks regarding enhanced collaboration in the cyber domain, especially on cybersecurity and advanced technologies like 5G.[61] India and the US collaborated through the Joint Indo-US Quantum Coordination Mechanism to share expertise on critical and emerging technologies like quantum computing.[62] India, the US and Taiwan also forged critical ties in the domain of cybersecurity through organising a workshop in December 2023 under the Global

[60] Shravani Nag Lanka and Medha Garg, '2025 Budget and Digital Rights: Artificial Intelligence Takes Center Stage', Internet Freedom Foundation, 11 February 2025, https://internetfreedom.in/2025-budget-and-digital-rights-artificial-intelligence-takes-centre-stage/#:~:text=However%2C%20budget%20allocation%20for%20the,for%20FY25%20which%20could%20prove.

[61] 'India and Japan Forge Cybersecurity Collaboration and Set Future Course', *Financial Express*, 14 September 2023, https://www.financialexpress.com/business/defence-india-and-japan-forge-cybersecurity-collaboration-and-set-future-course-3243939/.

[62] Pravan Dixit, 'India, United States forge groundbreaking collaboration in AI and Quantum Computing', *Business Today*, 23 June 2023, https://www.businesstoday.in/technology/news/story/india-united-states-forge-groundbreaking-collaborations-in-ai-and-quantum-computing-386806-2023-06-23.

Cooperation and Training Framework.[63] These measures spur greater public-private collaboration and inter-agency interoperability. The Indian government is moving towards bolstering the nation's cybersecurity capabilities through capacity building, supply chain resilience and development of critical infrastructure.

[63] 'Tri-Nation cybersecurity summit marks milestone in global collaboration under GCTF', *Financial Express*, 11 December 2023, https://www.financialexpress.com/business/defence-tri-nation-cybersecurity-summit-marks-milestone-in-global-collaboration-under-gctf-3335651/.

Conclusion

The Indo-Pacific stands at a critical juncture. As countries rapidly digitalise, they have to grapple with a difficult and escalating cyber landscape filled with threats and risks that require robust and adaptive cyber strategies. This report examined the cybersecurity landscape and the domestic cyber resilience of Indonesia, Japan, South Korea and India to map and understand the domestic institutional changes made to bolster cybersecurity. It assesses the cybersecurity of these countries along three dimensions – resistance, recovery and adaptation.

Though they differ in terms of crafting and implementing a cybersecurity strategy, they are adopting measures to improve cybersecurity resistance and recovery as and when attacks occur.

The report reveals a region characterised by countries facing growing cyber challenges but united by a desire to address them domestically, notwithstanding capacity and strategic constraints. Each country in this report has made significant strides to enhance its cyber defense. Though they differ in terms of crafting and implementing a cybersecurity strategy, they are adopting measures to improve cybersecurity resistance and recovery as and when attacks occur. That said, these measures have to be constantly and consistently reformed and improved to defend and deter various cyber threats. Simply put, they have to remain adaptive.

These findings underscore the urgent need for a multifaceted, whole-of-government approach to cybersecurity. Addressing the unique challenges faced by each nation – from the surge in digital transactions in India and Indonesia to the targeted attacks on Japan and South Korea – requires tailored strategies and sustained policy responses. Going further, collaboration between countries could become essential as cybersecurity threats evolve. Ultimately, strengthening cyber resilience is not merely a technical exercise but a strategic choice and institutional shift, essential to safeguard security and prosperity in the Indo-Pacific.

Appendix
About the Authors

Dr Karthik Nachiappan is a Research Fellow at the Institute of South Asian Studies at the National University of Singapore. His research focuses on India's geo-economics and how issues like trade, technology and climate change affect India's foreign policy. He is the author of *Does India Negotiate?* (Oxford University Press, 2020).

Ms Mriganika Singh Tanwar is a Research Analyst at the Institute of South Asian Studies at the National University of Singapore. Her research interests lie at the intersection of international security, strategic technologies and climate change with a special focus on India's role in the Indo-Pacific region. She has previously been involved in research roles at S. Rajaratnam School of International Studies at the Nanyang Technological University, Singapore, Observer Research Foundation, India, and Warner Bros. Discovery.

Ms Tanwar's research was selected for the UNITAR Leaders' for Free and Open Indo-Pacific training programme (2024) by the United Nations Institute For Training and Research – Division of Prosperity – funded by the government and people of Japan.

INSTITUTE OF SOUTH ASIAN STUDIES
National University of Singapore
29 Heng Mui Keng Terrace
#08-06 (Block B)
Singapore 119620

Tel (65) 6516 4239
Fax (65) 6776 7505
URL www.isas.nus.edu.sg

KONRAD ADENAUER STIFTUNG
380 Jalan Besar
#11-01 Arc 380
Singapore 209000

Tel (65) 6603 6160
Fax (65) 6227 8343
URL https://www.kas.de/en/web/rspa