ORF OBSERVER RESEARCH FOUNDATION

STRENGTHENING THE QUAD'S REGULATORY DIPLOMACY ON CYBERSECURITY

Sameer Patil • Anirban Sarma • Basu Chandola

STRENGTHENING THE QUAD'S REGULATORY DIPLOMACY ON CYBERSECURITY

Attribution: Sameer Patil, Anirban Sarma, and Basu Chandola, *Strengthening the Quad's Regulatory Diplomacy on Cybersecurity,* March 2025, Observer Research Foundation.

ISBN: 978-93-49061-72-9
ISBN Digital: 978-93-49061-33-0

Editorial and Production Team: Vinia Mukherjee, *Editor and Producer;* Aswathy Gopinath and Monika Ahlawat, *Assistant Editors;* Rahil Miya Shaikh, *Design;* Simi Jaison, *Layout*

Contents

6

Introduction

10

The Quad's Cyber Threat Landscape

16

Assessing the Domestic Regulatory Landscape

26

Current Quad Efforts at Cybersecurity Cooperation

29

Regulatory Alignment: Potential Benefits and Challenges

36

Towards Stronger Quad Cooperation

1

Introduction

THE QUADRILATERAL SECURITY INITIATIVE (Quad) was established in 2007 following a senior official-level meeting between Australia, India, Japan, and the United States (US). However, the grouping unravelled soon after due to the flux in the regional security environments and each country's relationship with China. The grouping re-emerged a decade later, in 2017, after officials from the four countries met in Manila on the sidelines of the Asia-Pacific Economic Cooperation (APEC) summit.[1] The minilateral has since focused on issues like infrastructure development, counterterrorism, and security in the areas of maritime and cyberspace towards promoting peace, stability, and prosperity in the Indo-Pacific.

The collaboration has been undergirded by various initiatives in the technology sector. However, the Quad nations continue to face their biggest challenges in cyberspace. The four democracies have seen an unprecedented escalation since 2014 in cyber threats and malicious cyber activities, such as distributed denial-of-service attacks (DDoS), ransomware attacks, supply chain breaches, zero-day attacks, and cyber-enabled espionage campaigns.[a] These converging threats are fuelled by geopolitical tensions and polarisation in cyberspace approaches, risking the security and stability of not just the four democracies but also the larger Indo-Pacific region.

The four democracies have implemented a number of domestic measures to strengthen cybersecurity. In the US, the Biden administration issued Executive Order 14028 on Improving the Nation's Cybersecurity in May 2021, which emphasised the importance of public-private collaboration, information-sharing, and the adoption of best practices to mitigate cyber risks.[2] Likewise, India is establishing acts, advisories, and technical frameworks that focus on data protection, critical infrastructure protection, and information-sharing.[3]

---

a DDoS is an attack technique using multiple compromised systems or bots to flood a targeted server or network with excessive traffic, and render it inoperative.
A ransomware attack involves malicious software that either locks a device or encrypts files, then demands a ransom in exchange for restoring access to the compromised data or device.
A supply chain breach occurs when a cyber attacker exploits vulnerabilities in a third-party vendor or supplier to gain unauthorised access to an organisation's systems or data.
Zero-day attacks exploit software vulnerabilities unknown to developers or vendors, providing attackers an edge by launching attacks before a fix or defence is available, posing severe security threats.
A ransomware attack involves malicious software that either locks a device or encrypts files, then demands a ransom in exchange for restoring access to the compromised data or device.
A supply chain breach occurs when a cyber attacker exploits vulnerabilities in a third-party vendor or supplier to gain unauthorised access to an organisation's systems or data.
Zero-day attacks exploit software vulnerabilities unknown to developers or vendors, providing attackers an edge by launching attacks before a fix or defence is available, posing severe security threats.
Cyber-enabled espionage campaigns involve hacking into systems to gather sensitive information for political, economic, or strategic advantage, and are often conducted by state-sponsored groups or advanced persistent threats, aiming for long-term access and intelligence gathering.

Japan and Australia, too, are sharpening their focus on cyber resilience. At the Quad level, they have collectively taken steps to address cyber threats. In May 2022, the Quad leaders pledged to strengthen their respective capabilities in the defence of their government networks and critical infrastructure against cyber disruptions.[4]

The four democracies are therefore aligned on the need for polities and societies that are resilient to cyber threats. Despite being a shared threat, however, the nature, sources, and contexts of cyber threats differ across the four countries, and these differences have shaped their policy approaches. For instance, each country has different regulations vis-à-vis two specific aspects of cybersecurity: regulations governing critical infrastructure protection, and cyber-incident reporting norms. Unharmonised regulations can lead to compliance being prioritised over security imperatives.[5] Businesses may spend resources to comply with various breach regulations rather than protecting against breaches or innovating.[6] These regulations are necessary, but without harmonisation and reciprocity agreements, they can counter their objective of strengthening cybersecurity. Therefore, there is a need for regulatory alignment to boost the Quad's cyber resilience and enhance collective security in the Indo-Pacific.

Regulatory harmonisation refers to a spectrum of practices that can facilitate alignment across national regulatory frameworks. In the current context, harmonisation would mean minimising or eliminating differences[7] in critical infrastructure protection and cyber-incident reporting norms and developing reciprocity agreements. These approaches can improve cybersecurity outcomes while lowering costs for different stakeholders.[8]

Harmonising cybersecurity regulations among the Quad countries, especially those governing critical infrastructure protection and cyber-incident reporting, can enhance collective defence against cyber threats, streamline compliance efforts, improve incident response, and increase resilience. By aligning regulations and adopting common standards, the Quad countries can ensure a more cohesive and effective response to cyber incidents, reduce administrative burdens, and achieve better security outcomes at lower costs. Such regulatory alignment can foster international cooperation, creating a more resilient and secure digital environment that protects critical infrastructure and ensures swift and coordinated response to cyber incidents.

Standards play a crucial role in this process by providing a consistent and recognised baseline for cybersecurity practices, facilitating interoperability, and enabling more effective collaboration among nations.

This report evaluates the potential of regulatory alignment among the Quad democracies on critical infrastructure protection and cyber-incident reporting norms. It offers recommendations for strengthening the Quad's cyber cooperation.

II

The Quad's Cyber Threat Landscape

CYBERATTACKS HAVE GROWN in sophistication and impact, evolving from simple phishing and malware attacks targeting individuals and companies to DDoS attacks, large-scale state-sponsored attacks, and Advanced Persistent Threats (APTs).[b] The complexity and geographical spread of many of these attacks make them difficult to mitigate. This is true for the Quad countries. The Australian Signals Directorate (ASD), for example, responded to over 1,100 cybersecurity incidents in 2023-24.[9] India's Computer Emergency Response Team (CERT), meanwhile, handled 15,92,917 cyber incidents in 2023 (see Table 1).[10]

b An APT involves a sophisticated and prolonged cyberattack where an intruder secretly infiltrates a network and maintains an undetected presence over time.

Table 1: Cybersecurity Incidents Handled by CERT-In

Year	Total Incidents
2020	1,158,208
2021	1,402,809
2022	13,91,457
2023	1,592,917

Source: Data compiled from CERT-In[11]

Evolving trends include campaigns by Chinese threat actors, ransomware incidents targeting the healthcare sector, and breaches of election infrastructure.

Campaigns by Chinese Threat Actors

Globally, the number of cyberattacks on critical infrastructure doubled in 2023-24 as compared to the previous year.[12] These attacks are attributed to various threat actors, most prominently the hacking syndicates deployed by China as proxies in its grey-zone tactics against adversaries. Various cybersecurity reports and advisories have highlighted the role of actors such as Volt Typhoon,[13] RedEcho,[14] and BlackTech[15] in compromising networks to target critical infrastructure. This infrastructure spans state/public and private/commercial sectors and are expected to be operational around the clock, without disruptions. There are also intricate functional linkages among them. Therefore, any potential breach, disruption, or degradation of critical infrastructure in one sector has potential impact on others.[16]

Chinese state-sponsored threat actors are employing increasingly sophisticated techniques to target critical infrastructure, primarily for cyber espionage. In 2023, the ASD blamed China for targeting Australian businesses and critical infrastructure through Volt Typhoon.[17] It was alleged that Volt Typhoon used 'living-off-the-land' techniques[c] to blend in with the normal system and network activities and mask its presence.[18]

c A "living-off-the-land" technique is a cyberattack method where attackers utilise legitimate, native tools already present in the victim's system to maintain and escalate their malicious activities.

The US security establishment has also highlighted the threat posed by Volt Typhoon, which has conducted espionage and information-gathering campaigns targeted at US critical infrastructure since 2021.[19] US intelligence has also warned that the threat actor is pre-positioning in US critical infrastructure networks "to enable disruption or destruction of critical services in the event of increased geopolitical tensions and/or military conflict with the United States and its allies."[20]

China has deployed several such proxies to target critical infrastructure networks with an aim to establish long-term presence and evade detection.[21] In July 2024, the US, along with the Australian and Japanese cybersecurity agencies, blamed APT40, a threat actor linked to China's Ministry of State Security, for targeting Australian and other government and private-sector networks in the region.[22] Previously, Japanese authorities had linked several attacks in the country, including on its space agency and businesses, to APT40, which is known to target IP, trade secrets, and other high-value information from companies, universities, research institutes, and governmental entities.[23,24,25] Between 2019 and 2024, Japan's foreign and defence ministries alone faced more than 200 cyberattacks from Chinese state-sponsored threat actor MirrorFace.[26]

While India has not publicly attributed cyberattacks on its critical infrastructure to Chinese state-sponsored threat actors, it has also faced the consequences of their actions. Three instances highlight this: the persistent breaches of its power grids (attributed to the RedEcho threat actor); attacks on the IT networks of Indian biotech companies (attributed to Stone Panda); and the attack on the networks of the All India Institute of Medical Sciences (AIIMS) in December 2022 (attributed to the Chinese cyber-espionage group ChamelGang).[27,28,29] The power grid breaches also led to the disruption of electricity supply in Mumbai in October 2020, producing a cascading effect on other critical infrastructure such as railway transportation and traffic management systems.[30] These attacks have primarily been viewed as cyber-espionage campaigns, where the aim has been to obtain valuable information such as data about critical infrastructure (power grids), clinical trial data related to vaccines and confidential business plans (biotech companies), and sensitive health data of high-ranking government officials (AIIMS).[31]

Such cyber-espionage campaigns targeting critical infrastructure, which can compromise sensitive or confidential information, intellectual property, and trade secrets, can result in adverse impacts on future business opportunities, disruption of supply chains, decline in economic fortunes, business advantage to competitors, and reputation loss.

Ransomware Attacks and the Targeting of Healthcare Infrastructure

There has also been a surge in ransomware attacks targeting manufacturing, healthcare, and other critical infrastructure. According to the US Office of the Director of National Intelligence, the number of ransomware attack claims worldwide rose by 74 percent in 2023 from 2022.[32] Attacks against the agriculture, defence and government, energy, healthcare, IT, and transportation sectors increased by more than 50 percent from 2022.[33] The US witnessed 1,500 ransomware-related incidents in 2023 alone, involving over US$1.1 billion in ransom payments.[34] In Japan, ransomware attacks increased by 15 percent in 2023, whereas in India, these attacks doubled, as compared to 2022.[35]

Reports indicate that the healthcare and pharmaceuticals sector has consistently been the most vulnerable to cyberattacks, particularly to ransomware attacks, since the COVID-19 pandemic. This is especially concerning for the Quad countries, each of which has health-related industries and services as part of its critical infrastructure.[36] Table 2 shows the surge in ransomware attacks on the healthcare sector in the US.[d]

Table 2: Ransomware Attacks on the Healthcare Sector in the US (2020-23)

Year	Total Attacks
2020	116
2021	194
2022	128
2023	260

Source: Data compiled from the US Office of the Director of National Intelligence[37,38]

d The US was one of the countries most affected by the top four ransomware variants—Magniber, LockBit, BlackCat, and Hive. See: https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024

The findings of a US Department of Health and Human Services report draw attention to the extreme vulnerability of the healthcare sector.[39] Such attacks tend to disrupt operations and steal patient data. A ransomware attack on a hospital could encrypt patient records, making it difficult for healthcare providers to access critical information.[40] In India, too, the healthcare sector continues to be the most affected and most susceptible to cyberattacks.[41] Cybercrime syndicates have also begun transforming their ransomware into ransomware-as-a-service operations,[e] which is proving to be a profitable business model for these malicious actors.

Besides cybercrime syndicates, which have been the primary perpetrators of ransomware attacks, Chinese state-sponsored hacking syndicates use ransomware for espionage. The 2022 breach of AIIMS highlights this trend: Initially considered a ransomware attack, the breach was eventually revealed to be an espionage operation. There was no ransom demand; instead, the aim was to harvest sensitive health data of high-ranking government officials.[42] The attack was attributed to the Chinese cyber-espionage group ChamelGang, which has previously targeted organisations in the US and Japan.

Another notable threat actor is Russian cybercrime syndicates, which conduct ransomware attacks without facing punitive action from the Russian government. These groups have been responsible for incidents such as the May 2021 attack against the Colonial Pipeline in the US and the July 2023 LockBit ransomware attack at Japan's busiest port facility, the Port of Nagoya.[43,44] Both incidents caused disruptions: in the case of Nagoya port, the ransomware attack impacted cargo loading and unloading operations on more than 15,000 containers.[45]

North Korea, too, has emerged as another source of ransomware attacks targeting the healthcare and space sectors in the US.[46] North Korea-sponsored hacking syndicates conduct financially motivated attacks by using ransomware. APT45 is one group that has been linked to such activities, aligned with the priorities of Pyongyang.[47]

e 'Ransomware as a service' is a cybercrime business model in which ransomware developers sell ransomware code or malware to other hackers and cybercriminals, who then use the code to initiate their own ransomware attacks.

Breaches of Election Infrastructure

Election infrastructure has also been the target of penetrative cyberattacks from adversarial states. Manipulating elections and election results has become a common tactic for authoritarian governments to destabilise democracies. Since 2016, when malicious actors linked to the Russian government targeted the US election infrastructure during the presidential elections, the frequency and intensity of attacks have only surged.[48] Consequently, the US Department of Homeland Security designated election infrastructure as critical infrastructure in 2017.[49] According to Microsoft's *Digital Defense Report 2024,* election interference efforts were detected in 15 US states between July 2023 and June 2024, highlighting the ongoing threat to the integrity of the electoral process.[50]

In the Indo-Pacific, Chinese cyber interference in elections has been witnessed in Australia, Indonesia, Singapore, and Taiwan.[51] In the case of Indonesia, Russian threat actors were also involved. Beyond elections, parts of government systems have also witnessed breaches. In 2019, the Australian parliament was the target of a hack that resulted in data exfiltration.[52] Authorities determined that China's Ministry of State Security was responsible.[53] Accompanying these attacks are cyber-enabled foreign-influence operations that seek to capitalise on domestic political polarisation. Such cyberattacks and influence operations undermine citizens' trust in their countries' ability to protect the sanctity of their elections, and therefore, their democratic systems.

The Quad countries' cyber threat landscape has been made more complicated by persistent attacks on their critical infrastructure by adversaries, which have resulted in service disruptions and data harvesting. While China has been a primary source of these malicious activities, other countries like Russia and North Korea have also been involved. These malicious activities draw attention to the potential benefits of aligning Quad cyber regulations to implement joint countermeasures and the difficulties in identifying and operationalising areas for joint action. However, before examining these issues, it is necessary to evaluate the regulatory landscape of each Quad member state.

III

Assessing the Domestic Regulatory Landscape

THE QUAD COUNTRIES HAVE PUT IN PLACE their own cybersecurity laws and ecosystems, shaped by their respective national priorities, threat perceptions, and historical contexts. These countries have tailored the laws and policies governing cybersecurity to meet their specific technological, political, and economic environments.

Overview of the Regulatory Landscape

In November 2024, Australia introduced the Cyber Security Act 2024,[54] its first standalone law on cyber security.[55] The Act provides for mandatory security standards for products, reporting obligations for ransomware payments, voluntary information-

sharing of significant cybersecurity incidents, and the establishment of the Cyber Incident Review Board. The Act is an integral part of the Cyber Security Legislative Package,[56] designed to implement seven initiatives under the 2023-2030 Australian Cyber Security Strategy.[57] The Strategy marks a shift in Australia's approach to cybersecurity, making it more proactive and inclusive, not only responding to the current threat landscape but also preparing it against future challenges.[58]

In India, the Information Technology Act 2000 (IT Act 2000), as amended occasionally, is the primary legislation for the regulation of the use of computers, computer systems, and computer networks, as well as data and information in the electronic format. The IT Act 2000 addresses various offences, along with penalties and compensation.[59] In addition, the Digital Personal Data Protection Act, 2023 imposes duties on data principals and provides for penalties in case of breaches.[60] India has recognised "new age cybersecurity threats",[61] and the laws are aimed at ensuring "a secure and resilient cyberspace for citizens, businesses and Government".[62]

Japan's Basic Act on Cybersecurity provides a framework for the responsibilities and policies of the national and local governments to enhance cybersecurity in the country.[63] The Act aims to boost economic and social vitality and ensure a secure digital environment, while preserving the free flow of information and driving advancements in information and communications technology.[64] Further, the Act on the Prohibition of Unauthorised Computer Access, the Penal Code, and the Act on the Protection of Personal Information have cybersecurity implications.[65]

The US lacks a single federal law regulating cybersecurity, although several other laws have cybersecurity implications.[66] These include the Computer Fraud and Abuse Act, the Federal Trade Commission Act, the Fair Credit Reporting Act, Gramm-Leach-Bliley Act, the Cybersecurity and Infrastructure Security Agency Act, Cybersecurity Information Sharing Act of 2015, and the Cyber Incident Reporting for Critical Infrastructure Act of 2022. State-level laws, such as the California Consumer Privacy Act, also have cybersecurity implications. In 2021, then President Joe Biden issued Executive Order 14028 on Improving the Nation's Cybersecurity, aimed at modernising and enhancing the federal government's cybersecurity practices and establishing higher standards for software security across industries.[67]

Critical Infrastructure Protection

Safeguarding critical infrastructure is crucial for ensuring the continuity of essential services. Critical infrastructure is the cornerstone of modern economies, and any damage to them can result in economic losses and societal consequences.[68] Accordingly, the Quad countries have adopted policies to minimise vulnerabilities and to ensure that such systems are functional even during times of crisis.

Critical infrastructure protection in Australia is governed by the Security of Critical Infrastructure Act 2018, as amended occasionally, and most recently by the Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Act 2024.[69] The Security of Critical Infrastructure Act 2018 lists critical infrastructure sectors and critical infrastructure sector assets[70] and provides a detailed framework for managing risks relating to critical infrastructure. The Act requires entities responsible for critical infrastructure assets to identify and manage risks related to those assets and imposes enhanced cybersecurity obligations on such entities.

India defines "critical information infrastructure" as "computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety."[71] The government has the power to declare any computer resource that directly or indirectly affects the facility of critical information infrastructure to be a protected system.[72] Unauthorised access to protected systems is punishable under the Act. The Information Technology (Information Security Practices and Procedures for Protected System) Rules, 2018 expand on the provisions of the IT Act 2000.[73] The National Critical Information Infrastructure Protection Centre (NCIIPC) established under the Act has identified seven critical sectors: power and energy, banking, financial services and insurance, telecommunications, transport, government, strategic and public enterprises, and healthcare. Additionally, sector-specific policies, such as the Telecommunications (Critical Telecommunication Infrastructure) Rules, 2024, play a role in shaping the governance of critical infrastructure.[74]

Japan, for its part, has its Cybersecurity Policy for Critical Infrastructure Protection. It defines "critical infrastructure" as "sectors that comprise the

backbone of national life and economic activities formed by businesses providing services that are extremely difficult to be substituted; if the function of the services is suspended or deteriorates, it could have a significant impact on national life and economic activities."[75] Japan classifies 15 sectors as critical infrastructure. The policy specifies the purpose of critical infrastructure protection, the responsibilities of stakeholders, the basic concept of critical infrastructure, and the enhancement of incident response capabilities. Further, the Guideline for Establishing Safety Principles for Ensuring Cybersecurity of Critical Infrastructure provide standards or references for the decisions and actions taken by critical infrastructure operators to ensure cybersecurity.[76]

The US defines "critical infrastructure" as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[77] It considers 16 sectors as critical infrastructure.[78] The 2024 National Security Memorandum on Critical Infrastructure Security and Resilience aims to further advance efforts to strengthen and maintain secure, functioning, and resilient critical infrastructure and sets forth a revised framework for federal agency roles and responsibilities within the national critical infrastructure risk-management enterprise.[79]

Table 3: Laws Governing Critical Infrastructure

Country	Applicable Laws	Approach to Defining Critical Infrastructure	Number of Sectors Identified
Australia	The Security of Critical Infrastructure Act 2018	Lists various critical infrastructure sectors	11
India	The Information Technology Act 2000; Information Technology (Information Security Practices and Procedures for Protected System) Rules, 2018	Defines critical infrastructure	No sectors identified but seven sectors notified as critical infrastructure

Country	Applicable Laws	Approach to Defining Critical Infrastructure	Number of Sectors Identified
Japan	Cybersecurity Policy for Critical Infrastructure Protection; Guideline for Establishing Safety Principles for Ensuring Cybersecurity of Critical Infrastructure	Defines critical infrastructure	15
US	2024 National Security Memorandum on Critical Infrastructure Security and Resilience	Defines critical infrastructure	16

Source: Authors' own

Table 4 highlights the criteria adopted by India, Japan, and the US for assessing the criticality of a sector. Australia does not define critical infrastructure as a whole but defines the various critical sectors individually.

Table 4: Criteria for Assessing Criticality

Criteria for Assessing Criticality	India[80]	Japan[81]	US[82]
National Security	✓		✓
Economy	✓	✓	✓
Public Health	✓		✓
Safety	✓	✓	✓
National Life		✓	

Source: Adapted with modifications from Srishti Saxena and Kaushal Mahan[83]

Each of the Quad countries has identified a range of critical infrastructure sectors (see Table 5).

Table 5: Critical Infrastructure Sectors in the Quad Countries

	Critical Infrastructure Sector	Australia[84]	India[85]	Japan[86]	US[87]
1	Chemical			✓	✓
2	Commercial Facilities				✓
3	Communications / Telecommunications Services	✓	✓	✓	✓
4	Critical Manufacturing				✓
5	Dams				✓
6	Defence Industrial Base	✓			✓
7	Emergency Services				✓
8	Energy / Electric Power Supply Services	✓	✓	✓	✓
9	Financial Services Sector and Markets / Banking Services / Credit Card Services	✓	✓	✓	✓
10	Food and Agriculture	✓			✓
11	Gas Supply Services			✓	
12	Government Services and Facilities		✓	✓	✓
13	Healthcare and Public Health / Medical Services	✓	✓	✓	✓
14	Higher Education and Research	✓			
15	Information Technology / Data Storage or Processing	✓		✓	✓
16	Logistics Service			✓	
17	Nuclear Reactors, Materials, and Waste				✓
18	Petroleum Industries			✓	
19	Ports and Harbours			✓	
20	Space Technology	✓			
21	Strategic Entities		✓		
22	Transportation Systems / Airports / Railway Services	✓	✓	✓	✓
23	Water and Wastewater Systems	✓		✓	✓

Source: Adapted with modifications from Srishti Saxena and Kaushal Mahan[88]

Each country classifies critical sectors based on national priorities and contexts.[89] Certain sectors are common across all countries, such as communications/telecommunications, energy supply, financial services, healthcare, and transportation services. Additionally, while there could be agreement on broader sectors, there are differences at the level of sub-sectors or enterprises.[90]

Cyber-Incident Reporting Norms

The Quad countries have varying cyber incident reporting norms, as shown in Table 6.

Table 6: Cyber Incident Reporting Norms in the Quad Countries

Country	Cyber Incident Reporting Norms
Australia	• Critical cyber incident to be reported within 12 hours • Other cyber incidents to be reported no later than 72 hours • Ransom payment to be reported within 72 hours
India	• Cyber incidents to be reported to CERT-In within six hours • Security incidents on protected systems to be reported to the NCIIPC within no specific time. To be reported to CERT-In within six hours.
Japan	• No general requirements for reporting security breaches • Personal data security breach to be reported within three to five days
US	• Covered cyber incidents to be reported no later than 72 hours • Ransom payment to be reported within 24 hours

Source: Authors' own

Australia requires the reporting of a critical cyber incident within 12 hours of becoming aware of the incident, and if 'other' cyber incidents occur, they must be reported within 72 hours of incident awareness.[91] Additionally, the Cyber Security Act 2024 requires an entity to report ransomware payments within 72 hours of making the ransomware payment or becoming aware that the ransomware payment has been made.[92]

In India, under the Cyber Security Directions, all cyber incidents have to be reported to CERT-In within six hours of becoming aware of such incidents.[93] In addition, all organisations that have "protected systems" must report security incidents to the NCIIPC. However, there is no specific deadline for this.[94]

Japan has no general requirements for reporting security breaches.[95] The Act on the Protection of Personal Information requires business owners to report a personal data security breach to data-protection authorities within three to five days.[96]

The US, in 2022, took a significant step towards cohesive breach notifications with the Cyber Incident Reporting for Critical Infrastructure Act, which sets uniform cybersecurity incident reporting requirements for operators of critical infrastructure. The Act requires covered cyber incidents to be reported no later than 72 hours from the time that the entity reasonably believes that the incident occurred. Similarly, ransom payments made in response to a ransomware attack must be reported within 24 hours after the ransom payment has been made.

In addition, several sectoral laws mandate cyber incident reporting in Australia, India, and the US (Table 7). Beyond general incident reporting norms, which apply to organisations across sectors, these countries have developed specific regulatory frameworks that enforce additional reporting obligations for certain sectors. The financial sector is a key area where additional obligations are imposed.

Table 7: Sectoral Laws with Specific Reporting Requirements in Quad Countries (Illustrative)

Country	Sector	Law	Reporting Requirements
Australia	Financial Services	Australian Prudential Regulation Authority Prudential Standard CPS 234 Information Security[97]	"An APRA-regulated entity must notify APRA as soon as possible and, in any case, no later than 72 hours, after becoming aware of an information security incident that: (a) materially affected, or had the potential to materially affect, financially or non-financially, the entity or the interests of depositors, policyholders, beneficiaries or other customers; or (b) has been notified to other regulators, either in Australia or other jurisdictions."
India	Electricity	Central Electricity Authority (Cyber Security in Power Sector) Guidelines, 2021[98]	The Chief Information Security Officer needs to submit a report on every sabotage classified as cyber incidents(s) on "Protected System" within 24 hours of occurrence.
	Telecom	Telecommunications (Critical Telecommunication Infrastructure) Rules, 2024[99]	Every telecommunication entity needs to ensure intimation of security incident(s) to the Central Government no later than six hours from the occurrence of such incident.
	Finance	Cybersecurity and Cyber Resilience Framework (CSCRF) for SEBI Regulated Entities (REs)[100]	Any cyberattack, cybersecurity incident and/or breach falling under CERT-In Cybersecurity directions shall be notified to SEBI and CERT-In within six hours of noticing/detecting such incidents or being brought to notice about such incidents. Any cybersecurity incident(s) on Regulated Entities which have been identified as 'Protected systems' and/ or CII by NCIIPC shall be reported to NCIIPC within 24 hours.
	Banks	Reserve Bank of India's Cyber Security Framework in Banks[101]	Security incident reporting mandated to the Reserve Bank of India within 2-6 hours.

Country	Sector	Law	Reporting Requirements
USA	Securities Market	Securities and Exchange Commission's Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure[102]	Publicly traded companies are required to disclose material cybersecurity incidents in Form 8-K within four business days of determining materiality.
	Financial Services	New York Department of Financial Services (NYDFS) Cybersecurity Regulation[103]	Each covered entity shall notify the superintendent as promptly as possible but in no event later than 72 hours from the determination that a cybersecurity event has occurred.

Source: Authors' own

The Quad countries are investing heavily in cybersecurity and have established detailed frameworks to ensure that critical infrastructures are protected. The diverse legislative frameworks in these countries reflect their unique approaches to cybersecurity and governance. While the disparate cybersecurity frameworks present a fragmented landscape, these countries have entered into a number of international cooperation initiatives.

IV

Current Quad Efforts at Cybersecurity Cooperation

CYBERSECURITY HAS BEEN A KEY area of cooperation for the Quad, featuring prominently in Leaders' declarations across the years. In 2021,[104] they pledged to work together to combat cyber threats, promote resilience, and secure critical infrastructure. The Quad Senior Cyber Group was launched following the 2021 Quad Leaders' Summit to enhance collaboration on cybersecurity matters.[105]

In 2022,[106] the Leaders noted the need to take a collective approach to enhancing cybersecurity in light of the spike in sophisticated cyber threats. They committed to improving the defence of critical infrastructure by sharing threat information, and agreed to coordinate capacity-building programmes under the Quad Cybersecurity Partnership.

In 2023,[107] Quad Leaders committed to creating a more secure cyberspace by enhancing regional capacity and resilience to cyber threats. Further, they introduced the first-ever Quad Cyber Challenge, adopted the Quad Joint Principles for Secure Software and the Quad Joint Principles for Cybersecurity of Critical Infrastructure, and introduced a track 1.5 government-academia dialogue to promote the use of machine learning for bolstering cybersecurity.[108]

In 2024,[109] the Leaders discussed the need to enhance cybersecurity partnerships to counter common threats and malicious actors and agreed to undertake joint efforts to detect vulnerabilities and protect critical infrastructure and national security networks. They also committed to coordinate on developing policy responses to counter cyber threats impacting the Quad's shared priorities.

In addition to the efforts at the Quad level, the four countries are also part of other multilateral initiatives focusing on cybersecurity. Australia, Japan, and the US signed the Joint Statement on the Strategic Dialogue on Cybersecurity of Civil Society Under Threat of Transnational Repression[110] in March 2023. Similarly, Australia and the US issued a Joint Cybersecurity Advisory[111] along with the United Kingdom (UK) and issued Cybersecurity Best Practices for Smart Cities[112] with the UK and New Zealand. Australia, Japan, and the US are also parties to the Budapest Convention on Cybercrime.[113] Table 8 lists some bilateral initiatives between the Quad countries.

Table 8: Cooperation and Partnerships on Cybersecurity Between the Quad Countries (Illustrative)

Countries	Partnership Mechanisms
Australia-India[114]	• Australia-India Framework Arrangement on Cyber and Cyber Enabled Critical Technologies Cooperation 2020 • Australia-India Cyber and Critical Technology Partnership 2020
Australia-Japan	• Australia-Japan Joint Declaration on Security Cooperation 2022[115] • Japan-Australia Cyber Policy Dialogue[116] • Pacific Digital Development Initiative 2024[117]

Countries	Partnership Mechanisms
Australia-US	• Australia-US Cyber Security Dialogue[118] • Australia-US Cyber Training Capabilities Project Arrangement[119] • Joint Statement on Australia-US Ministerial Consultations (AUSMIN) 2024[120]
India-Japan	• Memorandum of Cooperation in the field of Cybersecurity 2020[121] • India-Japan Cyber Dialogue[122]
India-US	• Framework for the US-India Cyber Relationship 2016[123] • India-US Initiative on Critical and Emerging Technology[124] • India-US MoU on Cybercrime Investigations 2025[125]
Japan-US	• Japan-US Cyber Dialogue[126] • United States-Japan Joint Leaders' Statement 2025[127]

Source: Authors' own

Threat actors can be located across nations and geographies. Accordingly, the Quad countries have been increasing their coordination and partnerships to enhance cybersecurity and work towards creating a safe and secure cyberspace. These countries have bilateral agreements and bilateral cyber dialogues to enhance cybersecurity cooperation.

The Quad countries could also work towards aligning their cyber laws and policies to enhance the Indo-Pacific's cyber resilience. Such an alignment will foster greater information-sharing among the four countries and other regional like-minded partners, enhance coordination among concerned government line agencies, and ensure more effective responses against malicious cyber activities targeting the four countries and the broader region.

V

Regulatory Alignment: Potential Benefits and Challenges

ATTACKS ON CRITICAL INFRASTRUCTURE can have a transnational or supranational dimension.[128] Such attacks utilise digital technologies and are not limited by physical geopolitical borders. Accordingly, the preparation, commission, and effects of the attacks may all be in different jurisdictions. As a result, there is need for a cross-jurisdictional approach for critical infrastructure protection; a domestic response will not be able to effectively deal with such harms.

The International Chamber of Commerce Working Paper on the cybersecurity of critical infrastructures[129] notes that differences in the approach to critical infrastructure protection makes international cooperation and coordination difficult. It highlights

the shared dependencies between countries, which could result in spillover impacts.

Potential Benefits of Aligning Cyber-Reporting and Critical Infrastructure Protection Norms

More Uniform Legal and Regulatory Frameworks

Varying critical infrastructure protection and cyber-incident reporting norms cause inefficiencies for multinational technology companies when addressing cyber incidents and tend to weaken the potential agility of their cybersecurity responses.[130] Working towards a more uniform regulatory framework would reduce the complexity of operations and compliance for tech companies and other cybersecurity-oriented private players in multiple jurisdictions and enable adherence to a near-common set of standards.

Developing a baseline for critical infrastructure protection and minimum reporting and protection measures for cyber incidents[131] could help strengthen accountability mechanisms, streamline reporting processes, and reduce the administrative burden on government agencies, organisations, and multinational companies reporting or trying to mitigate the effects of security breaches and cyber incidents. For example, the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) in the US requires timely reporting of cyber incidents. If similar reporting requirements are adopted by other Quad countries, companies can streamline their compliance processes, ensuring that they meet regulatory requirements without unnecessary repetitions.

The lack of harmonisation of regulation and reciprocity agreements also creates the possibility of conflict and contradictions in laws, wherein a company operating in multiple jurisdictions may have to "pick which laws to violate and which to follow."[132]

Consistent standards across the Quad could lead to the more efficient enforcement of these standards, facilitate better information-sharing, further strengthen cybersecurity measures, and provide a common ground for holding malicious actors responsible. For instance, the National Institute of Standards and Technology (NIST) Cybersecurity Framework, widely used

in the US, can be adopted or adapted by other Quad countries to create a common baseline for cybersecurity practices. This alignment ensures that all member countries have robust defences against cyber threats targeting critical infrastructure like power grids, financial systems, and healthcare networks.

Greater Cost Efficiency and Increased Resilience

Ecabert et al.[133] noted that the increasing number of cybersecurity regulations has led to multinational organisations expending significant efforts to ensure compliance, stay updated about new laws, and train staff. The absence of harmonisation also leads to greater compliance costs and administrative burdens for businesses.[134] Aligning regulatory frameworks can help reduce this burden, thereby reducing compliance costs, which companies can invest instead in improving the security and functionality of their products.[135]

By harmonising regulatory frameworks and developing reciprocity agreements, compliance requirements will take less time and resources for companies operating in different jurisdictions.[136] Aligning on cybersecurity norms and practices could help streamline processes and create opportunities for sharing financial, human, and technological resources, which would lead to greater cost efficiencies in managing the protection of critical infrastructure and reporting cyber incidents. These synergies and convergences would also lead more organically to the design and cost-effective execution of joint capacity-building programmes, data-sharing exercises, cyber defence simulations, and tech-procurement activities. Joint capacity-building programmes, in particular, offer a real opportunity to enhance the cyber capabilities of Quad member states. It is this kind of initiative that the Quad Cybersecurity Partnership envisions as part of its mandate.[137]

Pooled Knowledge and Improved Trust

Increasing cyber threats make regulatory harmonisation even more crucial.[138] Like-minded states can develop a minimum standard for information transfer and promote cooperation on pooling knowledge.[139] One of the primary benefits of being able to share intelligence as a result

of aligned systems would be advancing trust between Quad partners and thereby strengthening the overall potential for Quad-level cooperation. Besides, standardised mechanisms for reporting on cyber incidents would help build a common pool of knowledge, allowing Quad members to better understand the emerging tactics, strategies, strengths, and weaknesses of the malicious actors and proactively manage cybersecurity responses.

Further, weaknesses in the critical infrastructure protection of one country can impact the system viability and sustainability of critical infrastructures in other countries.[140,141] Thus, building shared structured cooperation and information-sharing mechanism is necessary. Sharing important information for investigations and improving collaboration among agencies to absorb lessons learned can also help mutually strengthen cyber-response capacities and advance cyber cooperation.[142] At present, Quad countries share threat information and collaborate through the interventions of their respective CERTs, but other collaborative mechanisms could also be considered to strengthen and upscale cyber cooperation. For instance, the implementation of the NIST Cybersecurity Framework across all Quad countries can provide a consistent approach to identifying, protecting, detecting, responding to, and recovering from cyber incidents. This consistency can help ensure that critical infrastructure remains operational even in the face of sophisticated cyberattacks.

Public-Private Partnerships

The Quad has highlighted the importance of public-private partnerships (PPPs) for promoting cybersecurity and tech development. For instance, a 2021 joint statement by the Quad Leaders stated that the four nations would "work together to facilitate public-private cooperation and demonstrate… the scalability of open, standards-based technology".[143] Closer regulatory alignments among Quad partners are likely to result in increased ease of entering cross-border PPPs. Such alignments could also facilitate and simplify the work of the Quad Investors Network (QUIN), which was set up in 2023 to support public-private collaboration, accelerate investments in cyber resilience and critical and emerging technologies for the Quad, and bring together investors, corporations, and public institutions from the Quad nations for this purpose. Regulatory alignment would present a set of basic shared goals and priorities for the QUIN to build upon.

Enhanced International Cooperation

Regulatory alignment would foster international cooperation by creating a more resilient and secure digital environment. For instance, the Quad Cybersecurity Partnership, which includes initiatives like the Quad Cyber Challenge and the Joint Principles for Secure Software, promotes collaboration and information-sharing among member countries. This cooperation enhances the collective ability to defend against cyber threats and respond to incidents.

Potential Challenges to Closer Regulatory Alignment

Divergent Perceptions of Cyber Threats

Quad nations have differing perceptions about the primary cyber threats affecting them or likely to affect them.[144] While China is generally viewed as a common threat, Quad members also have divergent views about the state actors that pose the greatest cyber threat to them.[145] Taken together, these two issues could pose a challenge in agreeing on cybersecurity policies and processes as well as norms for incident reporting.[146]

The priorities for the Quad countries are adapted to their threat landscape and domestic needs. For instance, Australia introduced a new cybersecurity plan following increasing attacks to critical infrastructure, with major breaches including Latitude, Optus, and Medibank.[147]

Meanwhile, India announced the Digital India Act,[148] which aims to enhance cybersecurity provisions in response to more sophisticated cyber threats.[149] This proposed legislation seeks to expand cybersecurity provisions, particularly for the rapidly growing digital economy, and establish stricter frameworks for protecting data and critical systems. India's focus is on reinforcing the legal and regulatory structure to counter evolving cyber risks.

Similarly, Japan amended its laws to include seaports as a critical infrastructure.[150] Japan is also adopting a more proactive approach to cybersecurity following over 200 cyberattacks between 2019 and 2024 on its foreign and defence ministries by the Chinese threat actor MirrorFace.[151]

Varied Regulatory Environments

Every Quad country currently has its own set of cyber laws and regulations, with different points of emphasis and differences in the ways in which certain issues are defined and understood. Such policies have developed over time based on each country's historical and cultural contexts as well as their strategic interests and priorities.[152] The countries also have different kinds of data-protection regimes and approaches towards data sharing.[153] These differences may pose a challenge to establishing a consistent or uniform regulatory environment and common norms for sharing sensitive threat information and incident reporting.

While all four countries have Tier 1 status in the Global Cybersecurity Index 2024,[154] their areas of relative strength and potential growth differ (see Table 9), depending on the changing priorities of the countries over time.

Table 9: Areas of Relative Strength and Potential Growth for the Quad Countries

Country	Areas of Relative Strength[f]	Areas of Potential Growth
Australia	Organisational measures, Legal measures, Capacity development measures	Technical measures, Cooperation measures
India	Technical measures, Legal measures, Capacity development measures, Cooperation measures	Organisational measures
Japan	Technical measures, Organisational measures, Legal measures, Capacity development measures	Cooperation measures
US	Technical measures, Organisational measures, Legal measures, Cooperation measures	Capacity development measures

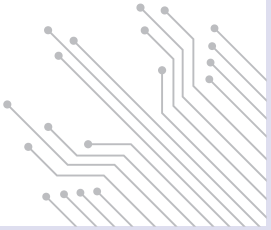
Source: Adapted from Global Cybersecurity Index 2024[155]

f Legal measures: Measures based on the existence of legal frameworks dealing with cybersecurity and cybercrime.
Technical measures: Measures based on the existence of technical institutions, standards, and frameworks dealing with cybersecurity and cybercrime.
Organisational measures: Measures based on the existence of coordination institutions, policies and strategies for cybercrime management and cybersecurity development at the national level.
Capacity development measures: Measures based on the existence of research and development, awareness raising, education and training programmes, certified professionals, and public-sector agencies fostering capacity development.
Cooperation measures: Measures based on the existence of partnerships, cooperation frameworks, and information-sharing networks at the national, regional, and global levels.

Additionally, Quad countries' national cybersecurity strategies are at varying stages of development. The US National Cybersecurity Strategy, launched by the then Biden administration in 2023, is broadly thought to be the most robust. Japan and Australia have also had national cybersecurity strategies in place since 2021 and for 2023-2030, respectively. India is yet to release a cybersecurity strategy, although it already has several key agencies and bodies tasked with upholding cybersecurity.

Sensitive Geopolitical Relationships

Cyberspace is emerging as an arena for geopolitical confrontation, and countries have to take steps to actively counter threats.[156] Quad nations tend to perceive China as a common threat and often define their own goals and motives accordingly. At the same time, China is a leading trade partner for all Quad countries,[157] with influence and control over supply chains.[158] India also shares a border with China, and the two nations have yet to fully resolve their five-year-long protracted border standoff. These factors could make it difficult for the Quad partners to align their regulations to present a united front against China even as such alignments continue to advance the group's other security and developmental objectives.



VI

Towards Stronger Quad Cooperation

Release Joint Cyber Threat Advisories

In recent years, the US has worked with its formal treaty allies to issue joint advisories on the APTs and threat actors targeting them. Most recently, in March 2024, together with the relevant cybersecurity agencies from Australia, Canada, the UK, and New Zealand, it issued an advisory warning against the actions of the Volt Typhoon threat actor. The Quad countries can likewise frame a joint cyber threat advisory, specifying the technical dimensions and complexities of cyber incidents without political attribution or ascribing the malicious activity to a particular threat actor. This will also facilitate more expeditious information-sharing on the evolving cyber threat landscape in the region.

Standardise Cyber Incident Reporting and Investigation Norms

The cybersecurity agencies of the four countries can develop a standard taxonomy to classify incidents based on their risk assessment, objective, technique, and targeted sector. Another way to achieve alignment is to agree to common timeframes for reporting cyber incidents. However, this will also require implementing systems or apparatus and technical capacity among the CERTs and other relevant agencies. Additionally, the countries can consider creating a joint system to advise each other on the specific capabilities required for standardised incident reporting and forensic investigations. For example, if the US Cybersecurity and Infrastructure Security Agency investigates a specific threat vector, its counterparts in the other three Quad countries can apply the same investigative techniques to analyse and assess cyber incidents affecting their networks. Once similar systems and capacities are in place, a certain degree of interoperability will also be achieved. The Quad countries can also prioritise specific critical infrastructure sectors to develop such reporting capacity.

Define Standards for Safeguarding Critical Infrastructure

The 'Quad Cybersecurity Partnership: Joint Principles' commit Quad members to align baseline standards for the software and software development ecosystem. Likewise, to tackle the challenge of diverse regulations across the Quad countries regarding protecting critical infrastructure, the grouping can define shared standards by working with operators and regulators such as the US Cybersecurity and Infrastructure Security Agency and India's NCIIPC. Existing Quad mechanisms can be leveraged to further the development of such standards:

- The Quad Senior Cyber Group can serve as a model for harmonising regulations across the Quad countries by adopting and implementing shared cybersecurity standards.
- The Joint Principles for Secure Software can be used to advocate for common software security standards, reducing vulnerabilities and ensuring consistent security measures.

- Sector-specific contact groups can facilitate the development of harmonised cybersecurity regulations by promoting a consensus-based approach to global cybersecurity standards.

Hold Periodic Exercises and Cyberattack Simulations

To test the resilience of critical infrastructure, the Quad countries can conduct joint exercises that simulate sustained attacks on specific infrastructure sectors. This approach will enable them to evaluate and enhance their collaborative response capabilities, identify internal strengths and weaknesses, and learn from these experiences. Such exercises are crucial for identifying areas that require capacity-building.

Create a Roadmap for Aligning Quad Cybersecurity Regulations

Under the aegis of the Quad Cybersecurity Partnership, Quad members could jointly conduct mapping and consultative exercises to identify specific regulatory areas where convergences may be possible. Based on their findings, the Quad could create a phased roadmap or action plan for achieving regulatory alignment in specific areas. The roadmap will need to account for domestic regulatory amendments that may need to be made before Quad-level synergies are operationalised. An expert group or advisory panel appointed by the Quad Senior Cyber Group could be tasked with developing this roadmap.

Strengthen PPPs Around Cybersecurity

The 'Quad Cybersecurity Partnership: Joint Principles' specify collaborating with industry on cybersecurity and critical infrastructure protection policies and implementing minimum software-security standards for government-procured software. Other areas of joint work that could be considered are:

- Involving private players as trainers/mentors in Quad cybersecurity capacity-building programmes.

- Working closely with QUIN to advance cybersecurity-focused partnerships between investors, businesses, and public institutions and to explore cross-border PPPs.
- Working towards establishing a Quad Business Council that could act as the "industry voice" for the Quad, link governments to businesses, and promote long-term commercial partnerships around technologies focused on cybersecurity and cyber safety, among other areas of significance for the businesses. Industry engagement is necessary for the Quad to recognise the private sector and businesses as equal stakeholders.

Undertake Joint Capacity-Building Initiatives

The Quad countries can advance joint capacity-building initiatives to strengthen the skills and talents required for detecting and deterring cyber threats. The exchange of knowledge and skills among participants can help enhance resilience against evolving cyber threats and develop a skilled workforce capable of addressing complex cybersecurity challenges.

Support Information-Sharing

The Quad countries should develop mechanisms for sharing critical threat and vulnerability intelligence. Linkages can be established among organisations responsible for cybersecurity in the four countries to share intelligence through dialogues and periodic engagements.

Appendix

Table 10: The Domestic Regulatory Landscape of the Quad Countries

	Australia	India	Japan	US
General	Australia introduced the Cyber Security Act 2024, the Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Act 2024, and the Intelligence Services and Other Legislation Amendment (Cyber Security) Act 2024 in November 2024.[159] The Security of Critical Infrastructure Act 2018, as amended by the new Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Act 2024, provides the framework for managing risks relating to critical infrastructure. The Privacy Act 1988 and Australian Privacy Principles provide for managing personal information in an open and transparent way.	The Information Technology Act 2000 (IT Act 2000) is the foundational law governing cyberspace in India. The IT Act provides for offences such as tampering with computer source documents,[160] computer-related offences,[161] dishonestly receiving stolen computer resources or communication devices,[162] identity theft,[163] cheating by personation by using computer resources,[164] violation of privacy,[165] cyber terrorism,[166] publishing or transmitting obscene[167] or sexually explicit[168] material in electronic form, and publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form.[169] The Act also provides for penalty and compensation for damage to computer, computer system[170] and compensation for failure to protect data.[171]	The two main statutes that penalise cybercrimes are the Act on the Prohibition of Unauthorised Computer Access and the Penal Code.[172] The Basic Act on Cybersecurity provides the basic framework for the responsibilities and policies of the national and local governments to enhance cybersecurity.[173] Further, the Act on the Protection of Personal Information is the principal data protection legislation in Japan.	The US lacks a single federal law regulating cybersecurity and privacy, and different states have their own laws.[174] The US has focused on laws addressing privacy, identity theft, data security, hacking, and other issues.[175] The Computer Fraud and Abuse Act was enacted in 1986 to address cyber-based crimes. The Division of Privacy and Identity Protection of the Federal Trade Commission[176] oversees issues related to consumer privacy, credit reporting, identity theft, and information security and enforces several laws, including: • Federal Trade Commission Act, which provides for the protection of consumers' personal information • The Fair Credit Reporting Act • The Gramm-Leach-Bliley Act • The Children's Online Privacy Protection Act • The Health Breach Notification Rule The Cybersecurity Information Sharing Act of 2015 aimed at improving cybersecurity in the US through enhanced sharing of information about cybersecurity threats.

	Australia	India	Japan	US
		In addition, the IT Act 2000 allows for the creation of rules[177] and regulations[178] for carrying out the provisions of the IT Act 2000. Such rules include: • Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013[179] • Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011[180] • Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021[181] • Information Technology (Information Security Practices and Procedures for Protected System) Rules, 2018[182] • Information Technology (Security Procedure) Rules, 2004[183] • Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009[184] In addition, the Digital Personal Data Protection Act, 2023 imposes duties on data principals and provides for penalties in case of any breach.[185]		The Cybersecurity and Infrastructure Security Agency Act of 2018 established the Cybersecurity and Infrastructure Security Agency to provide for cybersecurity and infrastructure protection. Further, the Cyber Incident Reporting for Critical Infrastructure Act of 2022 provides for the reporting of covered cyber incidents. The 2024 National Security Memorandum on Critical Infrastructure Security and Resilience aims to further advance the effort to strengthen and maintain secure, functioning, and resilient critical infrastructure. The 2021 Executive Order on Improving the Nation's Cybersecurity[186] provides for the standards and requirements that all Federal Information Systems should meet. The Privacy Act of 1974 protects individuals from the collection, use, disclosure, and maintenance of their personal information by federal agencies. The US Securities and Exchange Commission has released incident disclosure regulations requiring the disclosure of material breaches and the submission of annual reports. Additionally, there are laws at the state level, such as the California Consumer Privacy Act.

	Australia	India	Japan	US
Critical Infrastructure Protection	The Security of Critical Infrastructure Act 2018 provides that the following sectors of the Australian economy would be considered critical infrastructure sectors:[187] • Communications • Data storage or processing • Financial services and markets • Water and sewerage • Energy • Healthcare and medical • Higher education and research • Food and grocery • Transport • Space technology • Defence industry A critical infrastructure sector asset is defined as an asset that relates to a critical infrastructure sector.[188] The Act provides that the Minister may declare a particular asset to be a system of national significance if the asset is a critical infrastructure asset and if the Minister is satisfied that the asset is of national significance.[189] The Act provides for keeping a register of information in relation to critical infrastructure assets[190] and requires the responsible entity for a critical infrastructure asset to comply with a critical infrastructure risk management programme.[191]	Under the IT Act 2000, "Critical Information Infrastructure" has been defined as "computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety".[192] The IT Act 2000 empowers the appropriate Government to declare any computer resource that directly or indirectly affects the facility of Critical Information Infrastructure to be a protected system[193] and allows the appropriate government to authorise persons to have access to such protected systems. The Act further provides that unauthorised access to a protected system shall be punished with imprisonment of either description for a term that may extend to 10 years and a fine. The Information Technology (Information Security Practices and Procedures for Protected System) Rules, 2018 expand on the provisions of the IT Act 2000 and provide for Information Security Practices and Procedures for Protected System and Roles and Responsibilities of "Protected System(s)" towards National Critical Information Infrastructure Protection Centre.	The Basic Act on Cybersecurity defines "critical social infrastructure providers" as "those engaged in business that provides infrastructure which is the foundation of the lives of the people and economic activities, and whose functional failure or deterioration would cause an enormous impact on them".[194] Article 6 of the Act provides that a critical social infrastructure provider is to deepen its interest in and understanding of the importance of cybersecurity and to endeavour independently and actively to ensure cybersecurity, as well as endeavouring to cooperate in the implementation of the cybersecurity policy that the national or local government implements, in order to stably and properly provide its services. Further, Article 14 provides that the government is to provide measures such as formulating standards, exercises, and training, enabling information-sharing, promoting other voluntary activities, and other necessary measures regarding cybersecurity in critical social infrastructure providers and other related entities. Japan's Cybersecurity Policy for Critical Infrastructure Protection defines critical infrastructure as "sectors that comprise the backbone of national life and economic activities formed by businesses providing services that are extremely difficult to be substituted; if the function of the services is suspended or deteriorates, it could have a significant impact on national life and economic activities."	Critical infrastructure is defined as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[195] The US considers the following 16 sectors as critical infrastructure sectors: • Chemical • Commercial facilities • Communications • Critical manufacturing • Dams • Defence industrial base • Emergency services • Energy • Financial services • Food and agriculture • Government services and facilities • Healthcare and public health • Information technology • Nuclear reactors, materials, and waste • Transportation systems • Water and wastewater The 2024 National Security Memorandum on Critical Infrastructure Security and Resilience set forth a revised framework for federal agency roles and responsibilities within the national critical infrastructure risk management enterprise.[196] The memorandum seeks to strengthen the security and resilience of its critical infrastructure while taking into consideration the principles of shared responsibility, risk-based approach, minimum requirements, accountability, information exchange, expertise and technical resources, international engagement, and policy alignment.

	Australia	India	Japan	US
	The Act further provides that, if a cybersecurity incident has a relevant impact on a critical infrastructure asset, the responsible entity for the asset may be required to give a relevant Commonwealth body a report about the incident.[197] The Act further provides enhanced cybersecurity obligations that relate to systems of national significance[198] and requires certain entities relating to a critical infrastructure asset to provide information in relation to the asset and to notify if certain events occur in relation to the asset. The Act allows the Minister to require certain entities relating to a critical infrastructure asset to do, or refrain from doing, an act or thing if the Minister is satisfied that there is a risk of an act or omission that would be prejudicial to security.[199] The Act further allows the Secretary to require certain entities relating to a critical infrastructure asset to provide certain information or documents.[200] It also provides a regime for the Commonwealth to respond to serious cybersecurity incidents.[201] The Act also allows the Secretary to undertake an assessment of a critical infrastructure asset to determine whether there is a risk to national security relating to the asset. Certain information obtained or generated under, or relating to the operation of, this Act is protected information. Lastly, the Act provides that the Minister may privately declare an asset to be a critical infrastructure asset and that the Minister may privately declare a critical infrastructure asset to be a system of national significance.[202]		Accordingly, there are 15 critical infrastructure sectors: • Information and communication services • Financial services • Aviation services • Airports • Railway services • Electric power supply services • Gas supply services • Government and administrative services • Medical services • Water services • Logistics services • Chemical industries • Credit card services • Petroleum industries • Ports and harbours The policy provides the purpose of critical infrastructure protection, the responsibilities of stakeholders, the basic concept, of critical infrastructure and the enhancement of incident response capability.[203] Further, the Guideline for Establishing Safety Principles for Ensuring Cybersecurity of Critical Infrastructure provide standards or references for the decisions and actions taken by critical infrastructure operators in relation to ensuring cybersecurity.[204]	The memorandum provides the roles and responsibilities of the various agencies, including the Secretary of Homeland Security, Sector Risk Management Agencies, the Federal Senior Leadership Council, the Department of State, the Department of Defense, the Department of Justice, the Department of Commerce, the Department of Energy, the Director of the National Security Agency, the General Services Administration, the Nuclear Regulatory Commission, and the Federal Communications Commission. The memorandum discusses risk management and provides for the creation of a National Infrastructure Risk Management Plan. It also provides for Sector Risk Management Agencies for Designated Critical Infrastructure Sectors.

	Australia	India	Japan	US
Cyber-Incident Reporting Norms	A cybersecurity incident is defined[205] as one or more acts, events, or circumstances involving any of the following: unauthorised access to computer data or a computer programme; • unauthorised modification of computer data or a computer programme; • unauthorised impairment of electronic communication to or from a computer; • unauthorised impairment of the availability, reliability, security, or operation of a computer, computer data, or a computer programme. If a critical cyber incident has occurred, it must be reported within 12 hours of becoming aware of the incident.[206] If 'other' cyber incident has occurred, it must be reported within 72 hours of becoming aware of the incident.[207]	Under the Cyber Security Directions,[208] any service provider, intermediary, data centre, body corporate, and government organisation shall mandatorily report cyber incidents to CERT-In within six hours of noticing such incidents or being brought to notice about such incidents. Cyber incidents that need to be reported include targeted scanning/ probing of critical networks/systems, compromise of critical systems/information, unauthorised access of IT systems/ data, defacement of website or intrusion into a website, and unauthorised changes such as inserting malicious code or links to external websites, performing malicious code attacks such as spreading virus/ worm/Trojan/bots/ spyware/ransomware/ cryptominers, etc. In addition, all organisations that have "protected systems", as designated by the government under Section 70 of the Information Technology Act, 2000, have to report security incidents that impact protected systems to the National Critical Information Infrastructure Protection Centre. However, there is no specific deadline for the same.[209]	There are no general requirements for reporting security breaches under Japanese law.[210] The APPI requires business owners to report a personal data security breach to data-protection authorities immediately, usually within three to five days.[211]	In 2022, the US took a significant step towards cohesive breach notifications with the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA), which sets uniform cybersecurity incident reporting requirements for operators of critical infrastructure.[212] The Act requires the reporting of covered cyber incidents no later than 72 hours from the time the entity reasonably believes the incident occurred. Similarly, ransom payments made in response to a ransomware attack must be reported within 24 hours after the ransom payment has been made.

About the Authors

Sameer Patil is Director, Centre for Security, Strategy and Technology, Observer Research Foundation.

Anirban Sarma is Director, Centre for Digital Societies, Observer Research Foundation.

Basu Chandola is Associate Fellow, Centre for Digital Societies, Observer Research Foundation.

Endnotes

1 Ministry of External Affairs, Government of India, https://www.mea.gov.in/press-releases.htm?dtl/29110/IndiaAustraliaJapanUS_Consultations_on_IndoPacific_November_12_2017.

2 U.S. General Services Administration, *Improving the Nation's Cybersecurity,* Federal Register, 2021, https://www.gsa.gov/technology/it-contract-vehicles-and-purchasing-programs/information-technology-category/it-security/executive-order-14028.

3 Sameer Patil, "India's Cyber Security Landscape: Vulnerabilities and Responses," in *Securing India in the Cyber Era* (Routledge India, 2021), https://www.taylorfrancis.com/chapters/mono/10.4324/9781003152910-2/india-cyber-security-landscape-sameer-patil.

4 "The White House," https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/24/quad-joint-leaders-statement/

5 Aspen Digital Report, *Harmonizing Cybersecurity Regulation: A Security Symphony*, 2023.

6 "Harmonizing Cybersecurity Regulation: A Security Symphony"

7 Tatiana Nascimento Heim, "Global Governance and Regulation of Cybersecurity: Towards Coherence or Fragmentation?" (PhD diss., University of Twente, 2023), https://ris.utwente.nl/ws/portalfiles/portal/306180289/vers_o_pure.pdf

8 Henry Young, "Harmonizing Cybersecurity Regulations Is a Win-Win," BSA TechPost, July 10, 2024, https://techpost.bsa.org/2024/07/10/harmonizing-cybersecurity-regulations-is-a-win-win/.

9 Australian Signals Directorate (ASD), *Annual Cyber Threat Report 2023–2024*, Australian Government, 2024, https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/annual-cyber-threat-report-2023-2024 .

10 Ministry of Electronics and Information Technology, Government of India, *Official Website of CERT-In* (New Delhi: Ministry of Electronics and Information Technology), https://www.cert-in.org.in/.

11 Ministry of Electronics and Information Technology, Government of India, "CERT-In Annual Reports of 2020 to 2023," https://www.cert-in.org.in/.

12 Refna Tharayil, "Cyberattacks on CNI Surge by 30% in 2024, Study Reveals," *Tech Monitor*, August 27, 2024, https://www.techmonitor.ai/technology/cybersecurity/cyberattacks-on-critical-infrastructure-surge-by-30-in-2024-knowbe4-report-reveals.

13 MITRE, "Volt Typhoon," https://attack.mitre.org/groups/G1017/.

14 Electronic Transactions Development Agency, *APT group: RedEcho*, https://apt.etda.or.th/cgi-bin/showcard.cgi?g=RedEcho.

15 MITRE, "BlackTech," https://attack.mitre.org/groups/G0098/.

16 U.S. Department of Homeland Security, *China - Publications on Nation-State Cyber Actors*, Cybersecurity & Infrastructure Security Agency (CISA), https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors/china/publications.

17 "ASD Reports Increase in Cyber Attacks," *ABC News*, November 15, 2023, https://www.abc.net.au/news/2023-11-15/asd-reports-increase-in-cyber-attacks/103103320.

18 Australian Signals Directorate (ASD), *ASD Cyber Threat Report: July 2022 – June 2023*, Australian Government, 2023, https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/asd-cyber-threat-report-july-2022-june-2023.

19 U.S. Department of Homeland Security, *Cybersecurity Advisory - PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure*, Cybersecurity and Infrastructure Security Agency (CISA), February 7, 2024, https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a.

20 U.S. Department of Homeland Security, *Fact Sheet: PRC State-Sponsored Cyber Activity—Actions for Critical Infrastructure Leaders*, Cybersecurity and Infrastructure Security Agency (CISA), March 2024, https://www.cisa.gov/sites/default/files/2024-03/Fact-Sheet-PRC-State-Sponsored-Cyber-Activity-Actions-for-Critical-Infrastructure-Leaders-508c_0.pdf.

21 Microsoft Corporation, *Microsoft Digital Defense Report 2023*, 2023, https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023.

22 U.S. Department of Homeland Security, *People's Republic of China (PRC) Ministry of State Security APT40 Tradecraft in Action*, Cybersecurity and Infrastructure Security Agency (CISA), July 8, 2024, https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-190a.

23 Ministry of Foreign Affairs of Japan, Government of Japan, https://www.mofa.go.jp/press/danwa/press6e_000312.html.

24 Mari Yamaguchi, "Japan Says Chinese Military Likely Behind Cyberattacks," *AP News*, April 20, 2021, https://apnews.com/article/world-news-technology-business-tokyo-japan-f35854b6acb5ebd27a1a54d2417d2929.

25 Federal Bureau of Investigation (FBI), "APT 40 Cyber Espionage Activities," U.S. Department of Justice, https://www.fbi.gov/wanted/cyber/apt-40-cyber-espionage-activities.

26 Walter Sim, "Hit by Wave of Online Attacks, Japan Shifts to 'Active Cyber Defence'," *The Straits Times*, January 20, 2025, https://www.straitstimes.com/asia/east-asia/hit-by-wave-of-cyber-attacks-japan-shifts-to-active-cyber-defence.

27 Insikt Group, "China-linked Group RedEcho Targets the Indian Power Sector Amid Heightened Border Tensions," Recorded Future, February 28, 2021, https://www.recordedfuture.com/redecho-targeting-indian-power-sector .

28 "Chinese Hackers Target India's Serum Institute, Bharat Biotech: Report," *NDTV*, March 1, 2021, https://www.ndtv.com/india-news/chinese-hackers-target-india-s-serum-institute-bharat-biotech-report-2381309 .

29 "13 TB Data Encrypted in Ransomware Attack on AIIMS by Unknown Threat Actors: Centre," *The Hindu*, December 15, 2022, https://www.thehindu.com/news/national/13-tb-data-encrypted-in-ransomware-attack-on-aiims-by-unknown-threat-actors-centre/article66271226.ece.

30 "Mumbai Power Outage Today: Local Trains Suspended, CCTVs and Traffic Signals Down After Grid Failure; 10 Points," *India Today*, October 12, 2020, https://www.indiatoday.in/india/story/mumbai-power-cut-today-local-trains-suspended-traffic-signals-down-grid-failure-tata-1730733-2020-10-12.

31 Sameer Patil, "Expanding Chinese Cyber-Espionage Threat Against India," Observer Research Foundation, April 18, 2022, https://www.orfonline.org/expert-speak/expanding-chinese-cyber-espionage-threat-against-india.

32 U.S. Office of the Director of National Intelligence, *Ransomware Attacks Surge in 2023; Attacks on Healthcare Sector Nearly Double*, February 28, 2024, https://www.dni.gov/files/CTIIC/documents/products/Ransomware_Attacks_Surge_in_2023.pdf.

33 U.S. Office of the Director of National Intelligence, *Ransomware Attacks Surge in 2023; Attacks on Healthcare Sector Nearly Double*

34 U.S. Mission to the United Nations, *Remarks at a UN Security Council Briefing on Ransomware Attacks Against Hospitals and Other Healthcare Facilities and Services*, November 8, 2024, https://usun.usmission.gov/remarks-at-a-un-security-council-briefing-on-ransomware-attacks-against-hospitals-and-other-healthcare-facilities-and-services/.

35 Microsoft Corporation, *Microsoft Digital Defense Report 2024*, 2024, https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024.

36 Tharayil, "Cyberattacks on CNI Surge by 30% in 2024, Study Reveals".

37 U.S Office of the Director of National Intelligence, *Ransomware Attacks in the US and the Rest of the World, January 2020–December 2022*, January 2022, https://www.dni.gov/files/CTIIC/documents/products/Ransomware_Attacks_in_the_US_and_the_Rest_of_the_World__January_2020_December_2022.pdf.

38 U.S Office of the Director of National Intelligence, *Ransomware Attacks Surge in 2023; Attacks on Healthcare Sector Nearly Double*.

39 U.S. Department of Health and Human Services (HHS), *2020 Healthcare and Public Health (HPH) Cybersecurity Retrospective*, December 2020, https://www.hhs.gov/sites/default/files/2020-hph-cybersecurty-retrospective-tlpwhite.pdf.

40 Microsoft Corporation, *Microsoft Digital Defense Report 2024*.

41 Check Point, *The State of Cyber Security 2025*, https://engage.checkpoint.com/security-report-2025?utm.

42 Jonathan Greig, "Suspected Chinese Gov't Hackers Used Ransomware as Cover in Attacks on Brazil Presidency, Indian Health Org," *The Record*, June 27, 2024, https://therecord.media/chamelgang-china-apt-ransomware-distraction.

43 Cybersecurity and Infrastructure Security Agency (CISA), *The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years*, U.S. Department of Homeland Security, May 8, 2023, https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years.

44 "Ransomware attack from Russia hits Japan's biggest port, delaying cargo," *The Straits Times*, July 5, 2023, https://www.straitstimes.com/asia/east-asia/ransomware-attack-from-russia-hits-japan-s-biggest-port-delaying-cargo.

45 "Nagoya Port Cyberattack May Become Security Wake-Up Call," *The Asahi Shimbun*, July 13, 2023, https://www.asahi.com/ajw/articles/14954966 .

46 Robert Legare and Nicole Sganga, "North Korean Charged in Ransomware Attacks on NASA, U.S. Hospitals," *CBS News*, July 25, 2024, https://www.cbsnews.com/news/north-korean-hacker-cyber-attacks-nasa-u-s-hospitals-military/.

47 "APT45: North Korea's Digital Military Machine," Google Cloud Blog, https://cloud.google.com/blog/topics/threat-intelligence/apt45-north-korea-digital-military-machine

48 "Russian Targeting of Election Infrastructure During the 2016 Election: Summary of Initial Findings and Recommendations," U.S. Senate Select Committee on Intelligence, https://www.intelligence.senate.gov/publications/russian-targeting-election-infrastructure-during-2016-election-summary-initial-findings.

49 Congressional Research Service, "The Designation of Election Systems as Critical Infrastructure," September 18, 2019, https://crsreports.congress.gov/product/pdf/IF/IF10677.

50 Microsoft Corporation, before *"Microsoft Digital Defense Report 2024"*

51 Fergus Hanson et al., "Hacking Democracies," *Australia Strategic Policy Institute,* May 15, 2019, https://www.aspi.org.au/report/hacking-democracies.

52 "Australia's Parliamentary IT System Hacked Earlier This Year: Report," *Reuters*, October 28, 2019, https://www.reuters.com/article/technology/australias-parliamentary-it-system-hacked-earlier-this-year-report-idUSKBN1XO311/.

53 Colin Packham, "Exclusive: Australia Concluded China Was Behind Hack on Parliament, Political Parties – Sources," *Reuters*, September 16, 2019, https://www.reuters.com/article/world/exclusive-australia-concluded-china-was-behind-hack-on-parliament-political-pa-idUSKBN1W106H/.

54 Cyber Security Act of 2024, Act No. 98 of 2024.

55 Nick Boyle et al., "Australia's First Standalone Cyber Security Law – the Cyber Security Act 2024," *Bird and Bird*, December 18, 2024, https://www.twobirds.com/en/insights/2024/australia/australias-first-standalone-cyber-security-law-the-cyber-security-act-2024.

56 "Cyber Security Legislative Package 2024," Parliament of Australia, 2024, https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/CyberSecurityPackage

57 "Introduction of landmark Cyber Security Legislation Package," *Department of Home Affairs*, October 9, 2024, https://www.homeaffairs.gov.au/news-media/archive/article?itemId=1247# .

58 Mike Franklin, "ACSC and the Australian Cyber Security Strategy: Why They Matter to You," *Protecht*, February 13, 2024, https://www.protechtgroup.com/en-au/blog/acsc-and-the-australian-cyber-security-strategy-why-they-matter-to-you .

59 Information Technology Act of 2000, Act No. 21 of 2000, Chapter IX and XI.

60 The Digital Personal Data Protection Act, 2023, Act No. 22 of 2023.

61 Nishith Desai Associates, "Cybersecurity Law and Policy: Present Scenario and the Way Forward," Nishith Desai Associates, 2023, https://www.nishithdesai.com/fileadmin/user_upload/pdfs/Research_Papers/Cybersecurity-Law-and-Policy.pdf .

62 Ministry of Electronics and Information Technology, *National Cyber Security Policy -2013,* https://www.meity.gov.in/writereaddata/files/downloads/National_cyber_security_policy-2013%281%29.pdf#:~:text=To%20protect%20 .

63 The Basic Act on Cybersecurity, Act No. 104 of 2014.

64 The Basic Act on Cybersecurity, Act No. 104 of 2014, Article 1.

65 Hiromi Hayashi et al., "Cybersecurity Laws and Regulations Japan 2025," International Comparative Legal Guides, 2025, https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/japan.

66 "Federal Cybersecurity and Data Privacy Laws Directory," IT Governance, 2025, https://www.itgovernanceusa.com/federal-cybersecurity-and-privacy-laws .

67 Vivek Mishra and Sameer Patil, "Decoding the Biden Administration's Cyber Security Policy," Observer Research Foundation, January 2024, https://www.orfonline.org/research/decoding-the-biden-administration-s-cyber-security-policy.

68 Feng Wang et al., "The Development of Resilience Research in Critical Infrastructure Systems: A Bibliometric Perspective," Risk Analysis, September 2024, https://onlinelibrary.wiley.com/doi/10.1111/risa.17648 .

69 "Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Bill 2024," Parliament of Australia, 2024, https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r7255 .

70 The Security of Critical Infrastructure Act 2018, Act No. 29 of 2018, Section 8D and 8E.

71 Information Technology Act of 2000, Act No. 21 of 2000, Section 70, Explanation.

72 Information Technology Act of 2000, Act No. 21 of 2000, Section 70.

73 S.S. Rana & Co., "Information Technology (Information Security Practices And Procedures For Protected System) Rules, 2018 Notified," *Mondaq*, August 23, 2018, https://www.mondaq.com/india/security/730070/information-technology-information-security-practices-and-procedures-for-protected-system-rules-2018-notified .

74 Kriti, "Telecommunications (Critical Telecommunication Infrastructure) Rules, 2024," *SCC Online*, November 25, 2024, https://www.scconline.com/blog/post/2024/11/25/telecommunications-critical-telecommunication-infrastructure-rules-legal-news/ .

75 Cybersecurity Strategic Headquarters Government of Japan, *The Cybersecurity Policy for Critical Infrastructure Protection*, March 8, 2024, https://www.nisc.go.jp/eng/pdf/cip_policy_2024_eng.pdf

76 Cybersecurity Strategic Headquarters Government of Japan, *Guideline for Establishing Safety Principles for Ensuring Cybersecurity of Critical Infrastructure*, July 4, 2023, https://www.nisc.go.jp/eng/pdf/principles_cip_eng.pdf .

77 USA PATRIOT Act of 2001, P.L. 107-56, Section 1016(e).

78 Cybersecurity and Infrastructure Security Agency, "Critical Infrastructure Sectors," https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors

79 Brian E. Humphreys, "The 2024 National Security Memorandum on Critical Infrastructure Security and Resilience," Congressional Research Service, July 25, 2024, https://crsreports.congress.gov/product/pdf/IF/IF12716 .

80 Information Technology Act of 2000, Act No. 21 of 2000, Section 70, Explanation.

81 Cybersecurity Strategic Headquarters Government of Japan, *The Cybersecurity Policy for Critical Infrastructure Protection*, March 8, 2024, https://www.nisc.go.jp/eng/pdf/cip_policy_2024_eng.pdf .

82 USA PATRIOT Act of 2001, P.L. 107-56, Section 1016(e).

83 Srishti Saxena and Kaushal Mahan, "Establishing Global Norms to Protect Critical Information Infrastructure," *T20 Policy Brief*, May 2023, https://t20ind.org/wp-content/uploads/2023/05/T20_Policy-Brief_TF7_730.pdf

84 The Security of Critical Infrastructure Act 2018, Act No. 29 of 2018, Section 8D.

85 CDAC, "Cybersecurity," https://web.archive.org/web/20240623053636/https://www.cdac.in/index.aspx?id=cs_ss_ScadaIntro

86 "The Cybersecurity Policy for Critical Infrastructure Protection"

87 Cybersecurity and Infrastructure Agency, "Critical Infrastructure Sectors"

88 Srishti Saxena and Kaushal Mahan, "Establishing Global Norms to Protect Critical Information Infrastructure," *T20 Policy Brief*, May 2023, https://t20ind.org/wp-content/uploads/2023/05/T20_Policy-Brief_TF7_730.pdf

89 Saxena and Mahan, "Establishing Global Norms to Protect Critical Information Infrastructure"

90 Saxena and Mahan, "Establishing Global Norms to Protect Critical Information Infrastructure".

91 The Security of Critical Infrastructure Act 2018, Act No. 29 of 2018.

92 Cyber Security Act of 2024, Act No. 98 of 2024, Section 27.

93 MeitY, *Directions under sub-section (6) of section 70B of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet*, April 28, 2022, https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf .

94 "Cyber Security Law In India: Summary of Reporting Obligations," *SpiceRoute Legal*, https://spiceroutelegal.com/data-protection/cyber-security-law-in-india-summary-of-reporting-obligations/

95 Daisuke Yamaguchi et al., "Japan," *Global Investigations Review*, June 9, 2023, https://globalinvestigationsreview.com/guide/the-guide-cyber-investigations/third-edition/article/japan .

96 "Japan – Breach Notifications," *BakerMckenzie*, https://resourcehub.bakermckenzie.com/en/resources/global-data-privacy-and-cybersecurity-handbook/asia-pacific/japan/topics/breach-notification-requirements#.

97 "Prudential Standard CPS 234 Information Security," https://www.apra.gov.au/sites/default/files/cps_234_july_2019_for_public_release.pdf .

98 "Central Electricity Authority (Cyber Security in Power Sector) Guidelines," 2021, https://cea.nic.in/wp-content/uploads/notification/2021/10/Guidelines_on_Cyber_Security_in_Power_Sector_2021-2.pdf

99 Telecommunications (Critical Telecommunication Infrastructure) Rules, 2024, https://egazette.gov.in/(S(o4ckyeus0zsljsjidbaxu5zw))/ViewPDF.aspx

100 SEBI, *Cybersecurity and Cyber Resilience Framework (CSCRF) for SEBI Regulated Entities (REs)*, https://www.sebi.gov.in/legal/circulars/aug-2024/cybersecurity-and-cyber-resilience-framework-cscrf-for-sebi-regulated-entities-res-_85964.html

101 Reserve Bank of India, *Cyber Security Framework in Banks*, https://www.rbi.org.in/commonman/Upload/English/Notification/PDFs/NT41802062016.pdf

102 Securities and Exchange Commission, *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure,* https://www.federalregister.gov/documents/2023/08/04/2023-16194/cybersecurity-risk-management-strategy-governance-and-incident-disclosure

103 Department of Financial Services, *New York State Department of Financial Services 23 NYCRR 500: Cybersecurity Requirements for Financial Services Companies,* https://www.dfs.ny.gov/system/files/documents/2023/03/23NYCRR500_0.pdf

104 Quad, *Leaders' Joint Statement: "The Spirit of the Quad, "* 2021, https://www.mea.gov.in/bilateral-documents.htm?dtl/33620/Quad_Leaders_Joint_Statement_The_Spirit_of_the_Quad .

105 "Quad Senior Cyber Group," Department of Home Affairs, https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/quad-senior-cyber-group .

106 Quad, *Quad Leaders' Joint Statement*, 2022, https://www.mea.gov.in/bilateral-documents.htm?dtl/35357/Quad+Joint+Leaders+Statement .

107 Quad, *Quad Leaders' Joint Statement*, 2023, https://www.mea.gov.in/bilateral-documents.htm?dtl/36571/Quad_Leaders_Joint_Statement .

108 "2023 Quad Leaders' Summit," Department of Home Affairs, https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/quad-senior-cyber-group/2023-quad-leaders-summit .

109 Quad, *The Wilmington Declaration Joint Statement from the Leaders of Australia, India, Japan, and the United States*, 2024, https://www.mea.gov.in/bilateral-documents.htm?dtl/38320/ .

110 Department of Foreign Affairs and Trade, *Joint Statement on the Strategic Dialogue on Cybersecurity of Civil Society Under Threat of Transnational Repression*, 2023, https://www.dfat.gov.au/news/news/joint-statement-strategic-dialogue-cybersecurity-civil-society-under-threat-transnational-repression .

111 "U.S., U.K., and Australia Issue Joint Cybersecurity Advisory," *Cybersecurity and Infrastructure Security Agency*, July 28, 2021, https://www.cisa.gov/news-events/news/us-uk-and-australia-issue-joint-cybersecurity-advisory .

112 "U.S., U.K., Australia, Canada and New Zealand Release Cybersecurity Best Practices for Smart Cities," *Cybersecurity and Infrastructure Security Agency*, April 19, 2023, https://www.cisa.gov/news-events/news/us-uk-australia-canada-and-new-zealand-release-cybersecurity-best-practices-smart-cities .

113 "Parties/Observers to the Budapest Convention and Observer Organisations to the T-CY," Council of Europe, https://www.coe.int/en/web/cybercrime/parties-observers .

114 "India Partnership," Department of Foreign Affairs and Trade, https://www.dfat.gov.au/international-relations/themes/cyber-affairs-and-critical-technology/india-partnership .

115 "Australia-Japan Joint Declaration on Security Cooperation," Department of Foreign Affairs and Trade, October 22, 2022, https://www.dfat.gov.au/countries/japan/australia-japan-joint-declaration-security-cooperation .

116 "The 5th Japan – Australia Cyber Policy Dialogue," Ministry of Foreign Affairs of Japan, December 4, 2023, https://www.mofa.go.jp/press/release/pressite_000001_00016.html .

117 "Japan and Australia Launch Pacific Digital Development Initiative," DigWatch, September 6, 2024, https://dig.watch/updates/japan-and-australia-launch-pacific-digital-development-initiative .

118 Liam Nevill et al., "The Australia–US Cyber Security Dialogue," *Australian Strategic Policy Institute*, March 17, 2017, https://www.aspi.org.au/report/australia-us-cyber-security-dialogue .

119 "US and Australia Sign First-Ever Cyber Agreement to Develop Virtual Training Range," U.S. Cyber Command, December 4, 2020, https://www.cybercom.mil/Media/News/Article/2434919/us-and-australia-sign-first-ever-cyber-agreement-to-develop-virtual-training-ra/ .

120 "Joint Statement on Australia-U.S. Ministerial Consultations (AUSMIN) 2024," Minister for Foreign Affairs Senator the Hon Penny Wong, August 7, 2024, https://www.foreignminister.gov.au/minister/penny-wong/media-release/joint-statement-australia-us-ministerial-consultations-ausmin-2024

121 "India-Japan sign Memorandum of Cooperation in the field of Cybersecurity," *IndBiz*, October 7, 2020, https://indbiz.gov.in/india-japan-sign-memorandum-of-cooperation-in-the-field-of-cybersecurity/ .

122 "Fifth India-Japan Cyber Dialogue," Ministry of External Affairs, September 14, 2023, https://www.mea.gov.in/press-releases.htm?dtl/37119/Fifth+IndiaJapan+Cyber+Dialogue .

123 "Framework for the U.S.-India Cyber Relationship," US Embassy, 2016, https://in.usembassy.gov/framework-u-s-india-cyber-relationship/ .

124 "India-U.S. Emerging Technologies Working Group," Carnegie India, https://carnegieendowment.org/india/india-us-emerging-technologies-working-group?lang=en.

125 "India and US sign MoU on Cybercrime Investigations," *Ministry of External Affairs*, January 18, 2025, https://www.mea.gov.in/press-releases.htm?dtl/38924/India+and+US+sign+MoU+on+Cybercrime+Investigations.

126 "The 9th Japan-US Cyber Dialogue," Ministry of Foreign Affairs of Japan, June 27, 2024, https://www.mofa.go.jp/press/release/pressite_000001_00394.html.

127 "United States-Japan Joint Leaders' Statement," White House, February 7, 2025, https://www.whitehouse.gov/briefings-statements/2025/02/united-states-japan-joint-leaders-statement/

128 Nicolò Bussolati, "Harmonisation of Cybercrime Law: Past Solutions, Present Tensions, and Future Challenges" (PhD diss., University of Amsterdam, 2020), https://pure.uva.nl/ws/files/51253937/Thesis.pdf.

129 International Chamber of Commerce (ICC) Working Paper, "Protecting the Cybersecurity of Critical Infrastructures and Their Supply Chains," July 2024, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/ICC-2024_Protecting-the-cybersecurity-of-critical-infrastructures-and-their-supply-chains.pdf .

130 Mirzokhid Musayev, "Legal Frameworks for Cybersecurity in Fuel-Energy Companies," *Elektron Ilmiy Journal* 2, no. 3, July 20, 2024, https://www.elita.uz/index.php/jurnal/article/view/197 .

131 International Chamber of Commerce (ICC) Working Paper, "Protecting the Cybersecurity of Critical Infrastructures and Their Supply Chains".

132 "Harmonizing Cybersecurity Regulation: A Security Symphony"

133 T. Ecabert et al., "Implications of Cyber Incident Reporting Obligations on Multinational Organizations Headquartered in Switzerland," *International Cybersecurity Law Rev.* 5, 2024: 585–614, https://link.springer.com/article/10.1365/s43439-024-00129-x .

134 KPMG LLP, "Cybersecurity Strategy: ONCD, GAO," Regulatory Alert, June 2024, https://kpmg.com/kpmg-us/content/dam/kpmg/pdf/2024/cybersecurity-harmonization-reciprocity-reg-alert.pdf .

135 "Harmonizing Cybersecurity Regulations Is a Win-Win."

136 "Harmonizing Cybersecurity Regulation: A Security Symphony"

137 CyberPeace Institute, "Protecting Critical Infrastructure Through the Implementation of Cyber Norms," April 26, 2023, https://cyberpeaceinstitute.org/protecting-critical-infrastructure-through-cyber-norms/ .

138 "Harmonizing Cybersecurity Regulation: A Security Symphony"

139 Heim, "Global Governance and Regulation of Cybersecurity."

140 "Cloud Front," https://d1wqtxts1xzle7.cloudfront.net/99216799/International_organizations_II_tom-libre.pdf?1677556769=&response-content-disposition=inline%3B+filename%3DInternational_organizations_II_tom.pdf&Expires=1740036715&Signature=CeI7F8giqGdfN48Sn6Y7eEwR3AvTLv4G9YlnoADCp6CXF9XxCKSZh~4bHltpj-FmOHLxMOCf2Ux~kU8raNliv3Kyw-kKbxniDBvmLmSilDIRryXz-69VTqlv87gvzCzSpvm0fnExyQd7jf2Ru~fa0eyhqv~TSEwo7A3UQdOjTRNTI~5WEbQue6p6FjK9sv6B6Ed4BGRbkDSk6AsBkuxTIDinWxlwl0Se1mt8yUxes4oVekG57hNm9wIkKvTab7Bt-nIutCeliIaGQg3Hy2EbtXaMqkSl5ZxDFcu6zDbZ1eMCgHOtqZLI~vh6FQs-bQGy2wb0w~NfFfVd3FWw-nJrpZQ__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA#page=298

141 Milica Pavić and Igor Jokanović, "Legislation on Critical Infrastructure in the Republic of Serbia, the Region and the European Union," *Journal of Faculty of Civil Engineering* 39, 2021: 17–32, https://zbornik.gf.uns.ac.rs/doc/ZR39.02.pdf .

142 Fabio Ramazzini Bechara and Samara Bueno Schuch, "Cybersecurity and Global Regulatory Challenges," *Journal of Financial Crime* 28, no. 2, 2021: 359–374, https://www.wellesu.com/10.1108/jfc-07-2020-0149

143 Joint Statement from Quad Leaders, The White House, https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2021/09/24/joint-statement-from-quad-leaders/

144 Lavina Lee, "Assessing the Quad: Prospects and Limitations of Quadrilateral Cooperation for Advancing Australia's Interests" (PhD diss., Lowy Institute, 2020), https://www.lowyinstitute.org/publications/assessing-quad-prospects-limitations-quadrilateral-cooperation-advancing-australia-s

145 Zongyou Wei, "The Evolution of the 'QUAD': Driving Forces, Impacts, and Prospects," *China International Strategy Review* 4, 2022: 288–304, https://link.springer.com/article/10.1007/s42533-022-00119-w

146 Wei, "The Evolution of the 'QUAD'."

147 Charlotte Edmond, "Australia Revamps Cybersecurity Plans Following Succession of Breaches," World Economic Forum, December 21, 2023, https://www.weforum.org/stories/2023/12/cybersecurity-strategy-breach-hacker-critical-infrastructure-australia/ .

148 Ministry of Electronics and Information Technology, Government of India, https://www.meity.gov.in/writereaddata/files/DIA_Presentation%2009.03.2023%20Final.pdf .

149 Sanhita Chauriha, "Explained: The Digital India Act 2023," Vidhi Centre for Legal Policy, August 8, 2023, https://vidhilegalpolicy.in/blog/explained-the-digital-india-act-2023/ .

150 Iclg, "Home-iclg," https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/japan#:~:text=The%20law%20was%20amended%20in,take%20effect%20by%20October%202025 .

151 Walter Sim, "Hit by Wave of Online Attacks, Japan Shifts to 'Active Cyber Defence'," *The Straits Times*, January 20, 2025, https://www.straitstimes.com/asia/east-asia/hit-by-wave-of-cyber-attacks-japan-shifts-to-active-cyber-defence .

152 Mai Trinh Nguyen and Minh Quang Tran, "Balancing Security and Privacy in the Digital Age: An In-Depth Analysis of Legal and Regulatory Frameworks Impacting Cybersecurity Practices," *International Journal of Intelligent Automation and Computing* 6, no. 5, 2023: 1–12, https://research.tensorgate.org/index.php/IJIAC/article/view/61 .

153 Anil Trigunayat and Ambika Khemka, "Navigating Complexities in Indo-Pacific: India's Approach to Quad and Chinese Challenge," *Firstpost*, October 6, 2024, https://www.firstpost.com/opinion/navigating-complexities-in-indo-pacific-indias-approach-to-quad-and-chinese-challenge-13822556.html .

154 International Telecommunication Union (ITU), *Global Cybersecurity Index 2024*, Geneva, ITU, 2024, https://www.itu.int/epublications/publication/global-cybersecurity-index-2024

155 "Global Cybersecurity Index 2024"

156 Serhii Lysenko et al., "Global Cybersecurity: Harmonising International Standards and Cooperation," *Review Article*, June 11, 2024, https://malque.pub/ojs/index.php/mr/article/download/3820/1692

157 Of the Quad countries, India and Australia have the most significant trade relations with China.

158 Congressional Research Service, *The "Quad": Cooperation Among the United States, Japan, India, and Australia,* January 30, 2023, https://crsreports.congress.gov/product/pdf/IF/IF11678

159 Magdalena Blanch-de Wilt Cameron Whittfield and Annie Zhang, "Australia's 2024 Cyber Security Reforms," *Herbert Smith Freehills*, January 23, 2025, https://www.herbertsmithfreehills.com/insights/2024-12/australias-2024-cyber-security-reforms .

160 Information Technology Act of 2000, Act No. 21 of 2000, Section 65.

161 Information Technology Act of 2000, Act No. 21 of 2000, Section 66.

162 Information Technology Act of 2000, Act No. 21 of 2000, Section 66B.

163 Information Technology Act of 2000, Act No. 21 of 2000, Section 66C.

164 Information Technology Act of 2000, Act No. 21 of 2000, Section 66D.

165 Information Technology Act of 2000, Act No. 21 of 2000, Section 66E.

166 Information Technology Act of 2000, Act No. 21 of 2000, Section 66F.

167 Information Technology Act of 2000, Act No. 21 of 2000, Section 67.

168 Information Technology Act of 2000, Act No. 21 of 2000, Section 67A.

169 Information Technology Act of 2000, Act No. 21 of 2000, Section 67B.

170 Information Technology Act of 2000, Act No. 21 of 2000, Section 43.

171 Information Technology Act of 2000, Act No. 21 of 2000, Section 43A.

172 Hiromi Hayashi, Masaki Yukawa, and Daisuke Tsuta, "Cybersecurity Laws and Regulations Japan 2025," *International Comparative Legal Guides*, 2025, https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/japan .

173 The Basic Act on Cybersecurity, Act No. 104 of 2014.

174 "Federal Cybersecurity and Data Privacy Laws Directory," IT Governance, 2025, https://www.itgovernanceusa.com/federal-cybersecurity-and-privacy-laws.

175 J Kosseff, "Upgrading Cybersecurity Law," *Hous. L. Rev.* 61, 2023: 51.

176 "Division of Privacy and Identity Protection," FTC, https://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection/our-divisions/division-privacy-and-identity .

177 Information Technology Act of 2000, Act No. 21 of 2000, Section 87.

178 Information Technology Act of 2000, Act No. 21 of 2000, Section 89

179 Ministry of Electronics & Information Technology, *Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules,* 2013, https://www.meity.gov.in/writereaddata/files/G_S_R%2020%20%28E%292_0.pdf

180 Ministry of Electronics & Information Technology, *Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules,* 2021, https://www.meity.gov.in/sites/upload_files/dit/files/GSR313E_10511(1).pdf

181 "Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules"

182 Ministry of Electronics & Information Technology, *Information Technology (Information Security Practices and Procedures for Protected System) Rules,* 2018, https://www.meity.gov.in/writereaddata/files/NCIIPC-Rules-notification.pdf

183 Ministry of Electronics & Information Technology, *Information Technology (Security Procedure) Rules,* 2004, https://i4c.mha.gov.in/theme/resources/actRule/Information%20Technology%20(security%20Procedure)%20Amendment%20Rules,%202004.pdf

184 Ministry of Electronics & Information Technology, *Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules,* 2009, https://www.meity.gov.in/writereaddata/files/Information%20Technology%20%28%20Procedure%20and%20safeguards%20for%20blocking%20for%20access%20of%20information%20by%20public%29%20Rules%2C%2020-09.pdf

185 The Digital Personal Data Protection Act, 2023, Act No. 22 of 2023.

186 "Improving the Nation's Cybersecurity," Executive Order 14028, May 12, 2021, https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity .

187 The Security of Critical Infrastructure Act 2018, Act No. 29 of 2018, Section 8D.

188 The Security of Critical Infrastructure Act 2018, Act No. 29 of 2018, Section 8E.

189 The Security of Critical Infrastructure Act 2018, Act No. 29 of 2018, Section 52B.

190 The Security of Critical Infrastructure Act 2018, Act No. 29 of 2018, Section Part 2.

191 The Security of Critical Infrastructure Act 2018, Act No. 29 of 2018, Part 2A.

192 Information Technology Act of 2000, Act No. 21 of 2000, Section 70, Explanation.

193 Information Technology Act of 2000, Act No. 21 of 2000, Section 70.

194 The Basic Act on Cybersecurity, Act No. 104 of 2014., Article 3(1).

195 USA PATRIOT Act of 2001, P.L. 107-56, Section 1016(e).

196 Brian E. Humphreys, "The 2024 National Security Memorandum on Critical Infrastructure Security and Resilience," *Congressional Research Service*, July 25, 2024, https://crsreports.congress.gov/product/pdf/IF/IF12716 .

197 The Security of Critical Infrastructure Act 2018, Act No. 29 of 2018, Section 30BA.

198 The Security of Critical Infrastructure Act 2018, Act No. 29 of 2018, Part 2C.

199 The Security of Critical Infrastructure Act 2018, Act No. 29 of 2018, Part 3.

200 The Security of Critical Infrastructure Act 2018, Act No. 29 of 2018, Section 37.

201 The Security of Critical Infrastructure Act 2018, Act No. 29 of 2018, Part 3A.

202 The Security of Critical Infrastructure Act 2018, Act No. 29 of 2018, 6A.

203 Cybersecurity Strategic Headquarters Government of Japan, *The Cybersecurity Policy for Critical Infrastructure Protection*, March 8, 2024, https://www.nisc.go.jp/eng/pdf/cip_policy_2024_eng.pdf .

204 Cybersecurity Strategic Headquarters Government of Japan, *Guideline for Establishing Safety Principles for Ensuring Cybersecurity of Critical Infrastructure*, July 4, 2023, https://www.nisc.go.jp/eng/pdf/principles_cip_eng.pdf .

205 The Security of Critical Infrastructure Act 2018, Act No. 29 of 2018, Section 12M.

206 The Security of Critical Infrastructure Act 2018, Act No. 29 of 2018, Section 30BC.

207 The Security of Critical Infrastructure Act 2018, Act No. 29 of 2018, 30BD.

208 Ministry of Electronics & Information Technology, *Directions under sub-section (6) of section 70B of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet*, https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf .

209 "Cyber Security Law In India: Summary of Reporting Obligations," *SpiceRoute Legal*, https://spiceroutelegal.com/data-protection/cyber-security-law-in-india-summary-of-reporting-obligations/ .

210 Daisuke Yamaguchi et al., "Japan," *Global Investigations Review*, June 9, 2023, https://globalinvestigationsreview.com/guide/the-guide-cyber-investigations/third-edition/article/japan .

211 "Japan – Breach Notifications," *BakerMckenzie*, https://resourcehub.bakermckenzie.com/en/resources/global-data-privacy-and-cybersecurity-handbook/asia-pacific/japan/topics/breach-notification-requirements# .

212 Kosseff, "Upgrading Cybersecurity Law"

ORF OBSERVER RESEARCH FOUNDATION

20 Rouse Avenue
New Delhi-110002
Ph: +91-11-35332000 Fax: +91-11-35332005
www.orfonline.org | info@orfonline.org