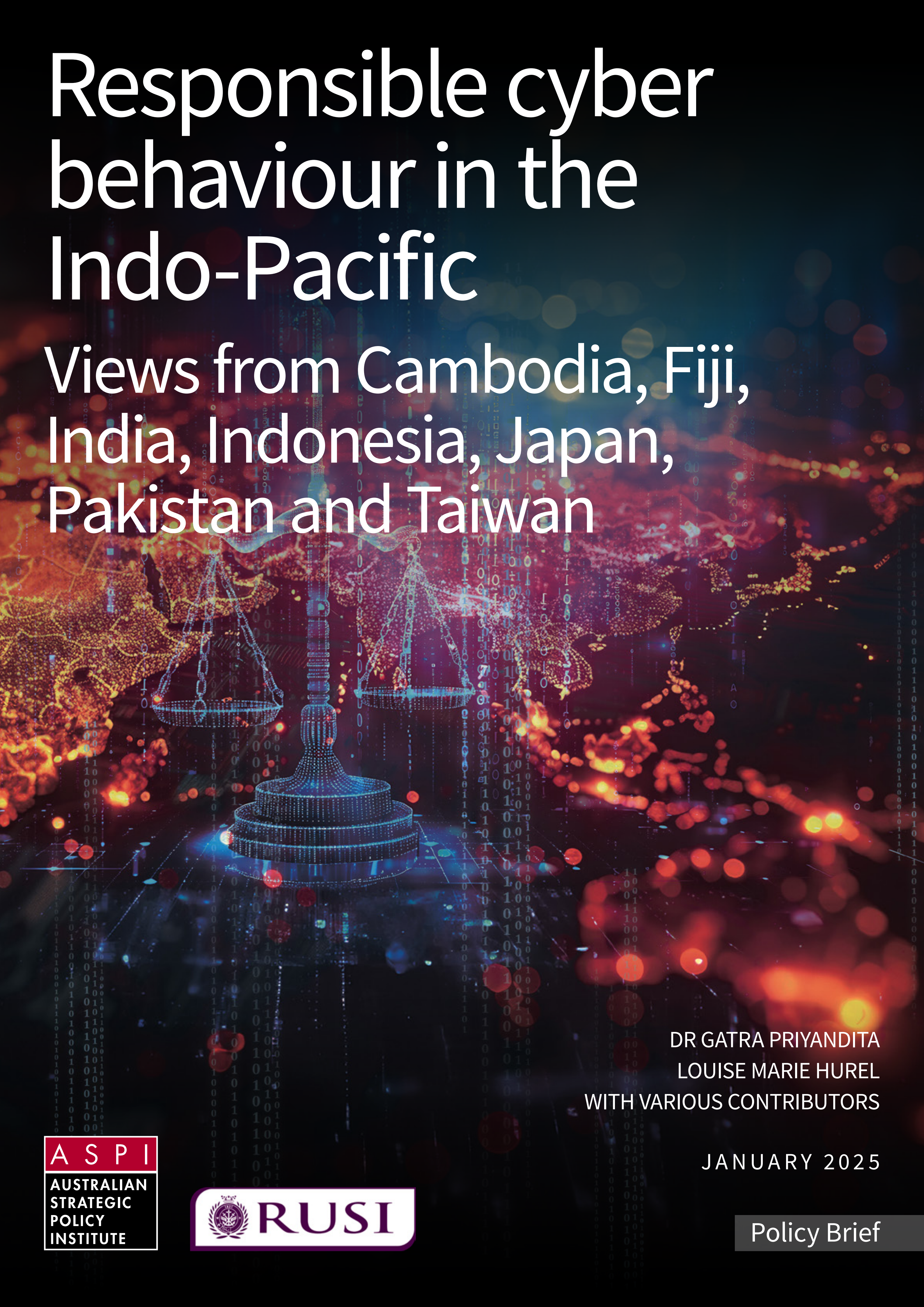


Responsible cyber behaviour in the Indo-Pacific

Views from Cambodia, Fiji, India, Indonesia, Japan, Pakistan and Taiwan

DR GATRA PRIYANDITA
LOUISE MARIE HUREL
WITH VARIOUS CONTRIBUTORS

JANUARY 2025

ASPI
AUSTRALIAN
STRATEGIC
POLICY
INSTITUTE

RUSI

Policy Brief

About the authors

Dr Gatra Priyandita is a Senior Analyst at ASPI's Cyber, Technology and Security Program.

Louise Marie Hurel is a Research Fellow at RUSI.

Contributors

Ilaitia B Tuisawau, Cybersecurity Advisor, Fijian Government.

Anushka Saxena, Research Analyst, The Takshashila Institution.

Dr Wilhelm Vosse, Professor of Political Science and International Relations, International Christian University.

Dr Rabia Akhtar, Director for Centre for Security, Strategy, and Policy Research, University of Lahore.

Dr Yisuo Tzeng, A/Director, Institute for National Defense and Security Research (Taiwan).

Acknowledgements

ASPI and RUSI would like to thank the authors of this compendium for their contributions, and also thank Arindrajit Basu, Bart Hogeveen, Eugene EG Tan, Nori Katagiri, Rogier Creemers, Bart Voogt, James Boorman, Raoul Heinrichs, Chris Taylor, Siriwat Chhem and many others for their feedback, comments, and contributions throughout the development of this publication—all of which were of great value in ensuring the proper balance between detail and nuance when approaching responsible cyber behaviour through a national lens.

About the report

This publication is produced by ASPI. It's part of the Responsible Cyber Behaviour project, an initiative led by the Royal United Services Institute in partnership with ASPI, to map understandings of responsible cyber behaviour through national and regional case studies and to connect experts from different sectors and regions through the Global Partnership for Responsible Cyber Behaviour.

GLOBAL PARTNERSHIP FOR RESPONSIBLE CYBER BEHAVIOUR

About ASPI

The Australian Strategic Policy Institute was formed in 2001 as an independent, non-partisan think tank. Its core aim is to provide the Australian Government with fresh ideas on Australia's defence, security and strategic policy choices. ASPI is responsible for informing the public on a range of strategic issues, generating new thinking for government and harnessing strategic thinking internationally. ASPI's sources of funding are identified in our annual report, online at www.aspi.org.au and in the acknowledgements section of individual publications. ASPI remains independent in the content of the research and in all editorial judgements. It is incorporated as a company, and is governed by a Council with broad membership. ASPI's core values are collegiality, originality and innovation, quality and excellence, and independence.

ASPI's publications—including this paper—are not intended in any way to express or reflect the views of the Australian Government. The opinions and recommendations in this paper are published by ASPI to promote public debate and understanding of strategic and defence issues. They reflect the personal views of the authors and should not be seen as representing the formal position of ASPI on any particular issue.

ASPI Cyber, Technology and Security

ASPI's Cyber, Technology and Security (CTS) analysts inform policy debates in the Indo-Pacific through original, rigorous and data-driven research. CTS is a leading voice in global debates on cyber, emerging and critical technologies, foreign interference and issues related to information operations and disinformation. CTS has a growing mixture of expertise and skills with teams of researchers who concentrate on policy, technical analysis, information operations and disinformation, critical and emerging technologies, cyber capacity building and internet safety, satellite analysis, surveillance and China-related issues. To develop capability in Australia and across the Indo-Pacific region, CTS has a capacity-building team that conducts workshops, training programs and large-scale exercises for the public, private and civil-society sectors.

CTS enriches regional debate by collaborating with civil-society groups from around the world and by bringing leading global experts to Australia through our international fellowship program. We thank all of those who support and contribute to CTS with their time, intellect and passion for the topics we work on.

If you would like to support the work of the CTS, contact: ctspartnerships@aspi.org.au.

Funding

This publication is funded with support from the UK Foreign, Commonwealth and Development Office.

Cover artwork: Byron Illyes, ASPI.

Responsible cyber behaviour in the Indo-Pacific

Views from Cambodia, Fiji, India, Indonesia, Japan, Pakistan and Taiwan

DR GATRA PRIYANDITA
LOUISE MARIE HUREL
WITH VARIOUS CONTRIBUTORS

JANUARY 2025

ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

RUSI

Policy Brief

Important disclaimer
This publication is designed to provide accurate and authoritative information in relation to the subject matter covered. It is provided with the understanding that the publisher is not engaged in rendering any form of professional or other advice or services.

First published January 2025

Published in Australia by the Australian Strategic Policy Institute

ASPI
Level 2
40 Macquarie Street
Barton ACT 2600
Australia

Tel Canberra + 61 2 6270 5100
Tel Washington DC +1 202 414 7353
Email enquiries@aspi.org.au
www.aspi.org.au
www.aspistrategist.org.au

Facebook.com/ASPI.org

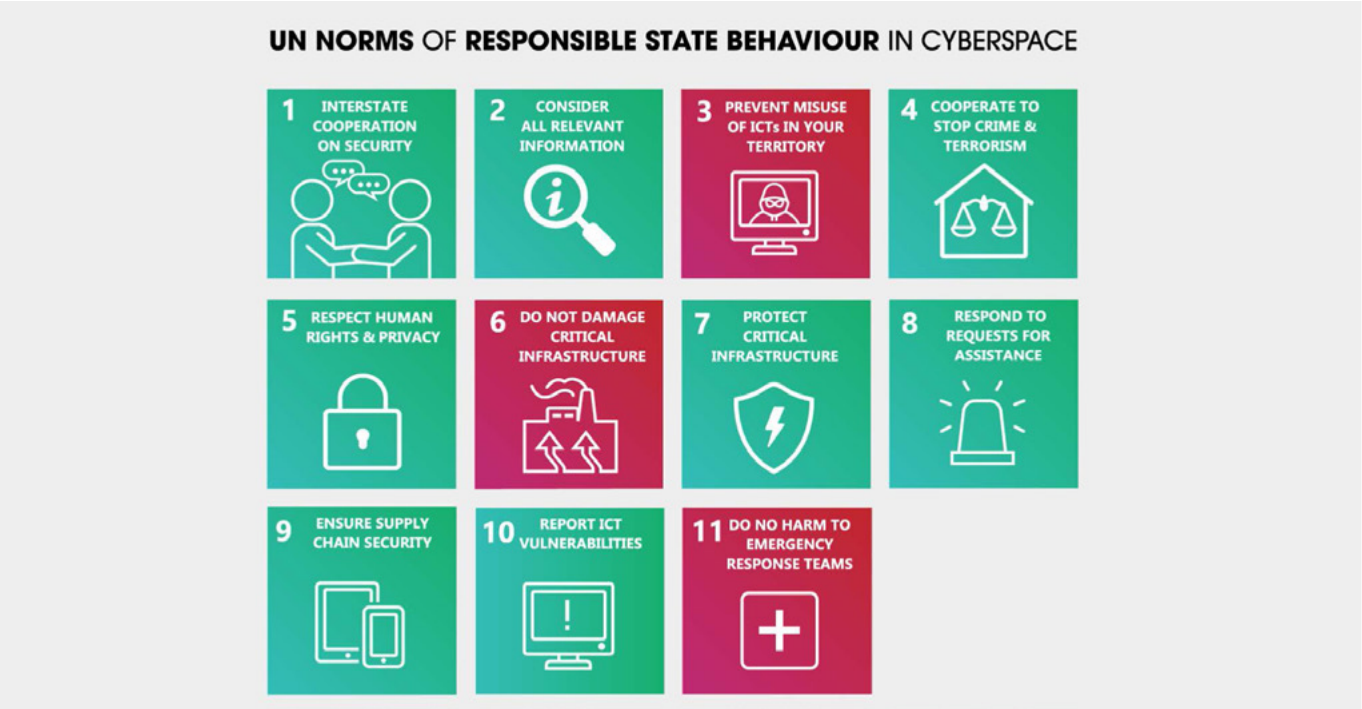
@ASPI_org

Contents

What's the problem?

In July 2025, the mandate of the United Nations Open-Ended Working Group on the security and use of information and communications technologies (hereafter OEWG) ends. This marks the latest chapter of international discussions on responsible behaviour in cyberspace. Throughout a 20-year period, a corpus of reports has been delivered that outline standards of behaviour.[1] Taken together, this is referred to as the 'UN framework of responsible state behaviour' and includes an acceptance that international law applies to state conduct in cyberspace and a commitment to observe a set of norms (see Figure 1).[2]

Figure 1: UN Norms of Responsible State Behaviour in Cyberspace


UN NORMS OF RESPONSIBLE STATE BEHAVIOUR IN CYBERSPACE
1 INTERSTATE COOPERATION ON SECURITY
2 CONSIDER ALL RELEVANT INFORMATION
3 PREVENT MISUSE OF ICTs IN YOUR TERRITORY
4 COOPERATE TO STOP CRIME & TERRORISM
5 RESPECT HUMAN RIGHTS & PRIVACY
6 DO NOT DAMAGE CRITICAL INFRASTRUCTURE
7 PROTECT CRITICAL INFRASTRUCTURE
8 RESPOND TO REQUESTS FOR ASSISTANCE
9 ENSURE SUPPLY CHAIN SECURITY
10 REPORT ICT VULNERABILITIES
11 DO NO HARM TO EMERGENCY RESPONSE TEAMS

These international norms are generally considered the benchmark for the notion of 'responsibility' in cyberspace, and one of the components of this 'framework'. However, the UN framework is fraught for several reasons:

- It suffers from a narrow application. The UN framework relates principally to cyber issues that affect international peace and security. This sets a high-security threshold for what should be considered part of the responsible cyber agenda.
- The UN framework focuses—almost exclusively—on the obligations of states under international law.
- It largely applies to externalities as it directs how states ought to behave towards each other, and not to how states should act domestically.
- The UN framework amplifies a perspective on responsible behaviour that's been spearheaded by the earliest and most mature cyber nations, in particular the P5 members of the UN Security Council.

This has resulted in a lopsided but dominant perspective on responsible cyber behaviour—one that overlooks states' domestic responsibilities in terms of the use of cyberspace for domestic and internal security purposes; practices of good governance for cyber capabilities and operational controls; and one that has overlooked perspectives from developing and emerging economies.

What's the solution?

As cyberspace has become a ubiquitous dimension of social, economic, political and military activities, there's a need to expand the notion of responsibility in cyberspace. While this has become common language in national and international cybersecurity strategies and practices in Australia, Europe, the UK and the US, it's less evidently articulated in most other parts of the world, including in most of the Indo-Pacific.[3]

This report introduces a more comprehensive framework to explore the concept of responsible cyber behaviour and additionally offers perspectives from seven Indo-Pacific countries on what constitutes 'responsible' cyber behaviour. The selected countries are less represented and examined in global and regional cyber policy conversations, in both Track 1 and Track 2 settings. These countries vary in size, economic development, systems of government and strategic outlook—and so provide much-needed validation and challenge to established thinking and norms.

The insights presented in this report should provide policymakers, negotiators, civil society and researchers in the fields of cyber policy, cyber diplomacy and the non-proliferation of dual-use technologies with a better understanding of various national perspectives. In doing so, it will help to inform the scope of work for the next chapter of international cyber negotiations.

A framework for responsible cyber behaviour

The UN framework for responsible state behaviour has set a crucial baseline for including the notion of 'responsibility' into international cyber policy discussions and agreements. But, as mentioned, it's presently lopsided in its focus. It may also no longer adequately reflect countries' greatest concerns in relation to cyber matters. In the past decade alone, the cybersecurity threat landscape has changed radically. Phenomena such as ransomware, spyware and artificial-intelligence (AI)-enabled cyber intrusions jeopardise national security and regional stability, and it's now recognised that most state-sponsored cyber campaigns involve acts of intelligence-gathering and espionage. Furthermore, more states are engaging with, and outsourcing to, criminal actors to secure economic and strategic advantage via cyber means.

To account for these developments in the understanding of the notion of responsibility, we propose to look at three dimensions: national, operational, and international levels of responsibility. We provide coverage of 'national dimensions' first in each instance to highlight expectations by each government of what it means to be a responsible actor in cyberspace. This is followed by consideration of the 'operational dimension' — that is, how each government regulates the export and use of cyber and ICT capabilities — and finally the 'international dimension' —that is, respective expectations of good international behaviour in cyberspace.

1. The national dimension assesses how countries 'regulate' their cyber power by looking at the policies, legislation, regulations, guidelines and standards that governments apply at home, the institutions responsible use of cyberspace and with cyber-related capabilities, as well as countries' diplomatic engagement and their national positions.
2. The operational dimension assesses how countries justify developing capacities and capabilities to act in cyberspace. Those considerations range from establishing institutions to combat cybercrime, to offensive or defensive cyber operations, and acquiring technologies to support domestic capacities to respond to incidents and emerging cyber threats.
3. The international dimension assesses how countries perceive international legal and normative debates and efforts at international cooperation. It touches on statements and commitments in relation to 'responsibility' in cyberspace, and further draws from memorandums of understanding, bi-, tri- and multilateral agreements and other foreign relations arrangements.

These dimensions can be applied universally, but, in this report, we apply them to analyse the state of play in seven Indo-Pacific countries: Cambodia, Fiji, India, Indonesia, Japan, Pakistan and Taiwan. All chapters follow a similar structure and are presented according to the three dimensions of responsible cyber behaviour—national, operational, and international. Each dimension is given different weightings in each profile, reflecting country-specific cultural, economic and political settings.

All chapters rely on a mix of primary sources (official government documents, white papers, speeches, legislation) and secondary sources (media coverage, reports, research papers). The chapter authors are experts in their respective countries and mostly native speakers. That's important, as it allows them to analyse various sources, including local media sources and interpret government documents. Inevitably, research limitations exist. Even with a greater diversity of sources, public information on many aspects of responsible cyber behaviour is scarce. Areas such as 'operational responsibility' are particularly challenging due to the varying degrees of transparency with which countries disclose capabilities and report on public spending, export controls and the acquisition of dual-use technologies. That lack of public data highlights gaps in research and public debate on responsible cyber behaviour. Each chapter identifies those gaps, offering valuable indicators for future research in the Indo-Pacific.

The geopolitics of cyberspace in the Indo-Pacific

To understand responsible cyber behaviour, we must consider the broader global and regional dynamics and how they shape how individual countries pursue their interests in cyberspace. In the Indo-Pacific, this includes:

- the geostrategic context of the region, where great-power rivalry is intensifying
- how geopolitical tensions and geo-economic relations shape perceptions of risk and mitigation
- diverse levels of cyber maturity and enabling cybersecurity capabilities across the region.

The Indo-Pacific encompasses more than 40 countries, it is home to nearly half of the world's population and generates approximately US$50 trillion in economic activity annually. The region is a stage for US–China strategic competition, as both powers advance their interests through diplomatic, economic, military and cyber means. In fact, the Indo-Pacific is also home to some of the most sophisticated and persistent cyber threat actors, including state-sponsored criminal actors and threats that are used for a range of ends—from cyber espionage to intellectual property theft, critical-infrastructure disruption and financial crime. Cyber activities also enable regional conflicts and acts of foreign interference that are playing out across the region.

As threats evolve and countries build their capacities (sometimes in distinct ways), it's crucial to understand how those countries internalise their obligations and commitments under international law and existing norms; which direction their cyber strategies take; and which justifications they have for developing cybersecurity capabilities within their security sector institutions.[4] Analysing those elements is essential to forming a more comprehensive understanding of how responsible cyber behaviour is practised, despite the use of different terminology or diverging interpretations of 'responsibility'.

Responsible cyber behaviour in the Indo-Pacific

The national perceptions and approaches to responsible cyber behaviour of the seven selected countries reflect the region's historical, cultural, economic and political diversity, and contrast with those of the region's major partners, such as the US and Europe.

Overall, however, the following common observations relating to responsible cyber behaviour across the Indo-Pacific can be made:

1. Responsible cyber behaviour is *not* a generally recognised concept; even the commitments made on responsible state behaviour in the context of the UN remain ambiguous and ill-understood and require more effort in terms of implementation.[5] Also, the acceptance that international law applies to state conduct in cyberspace isn't yet an embraced feature of domestic policy and regulations.
2. To date, responsible cyber behaviour is seen to deal with external threat actors—state and non-state, including criminal groups—and their misbehaviour for reasons including the misuse of cyber and strategic technologies (Japan, Taiwan); engagement in criminal activities (Cambodia); ICT security (Fiji, Indonesia); violation of data sovereignty and personal data protection (India); and terrorist use of the internet (Pakistan). The fact that few countries explicitly reference UN norms in their national strategies casts doubt over whether states (and their respective government departments) consider or are aware of international commitments when establishing domestic cyber policies and practices. Internally, few countries have developed guidelines or mechanisms to prevent the use of ICT for malign purposes.
3. For most of the Indo-Pacific stakeholders, responsible cyber behaviour starts with accepting—and reaffirming—the principle of state sovereignty in cyberspace. As a consequence, states are entitled to establish cyber functions within their security apparatuses for purposes of national security and defence, although there's no expectation that they should do so. Secrecy around any of these capabilities and activities is considered acceptable, even when it's recognised that this complicates oversight. In cases where regulations exist, enforcement remains inconsistent and ill-resourced. Continued reports of misuse of cybertools by state agencies against domestic and foreign constituencies highlight this challenge.
4. Economic imperatives are often central to all policies, including on cybersecurity. Whereas the UN framework has concentrated on the impact of cyberspace on international peace and security, most Indo-Pacific countries are predominantly concerned with socio-economic development, digitalisation and connectivity.
5. Given that most Indo-Pacific countries lack sovereign cyber and digital capabilities, responsible cyber behaviour is about the opportunity to freely choose their strategic partners and seek investments, technical support and equipment, and capacity building that could strengthen the stability of the state, advance socio-economic development, or both.
6. Furthermore, responsible cyber behaviour is a concept that allows countries to legitimately pursue and advocate for their own cyber priorities, such as combating cybercrime, seeking data sovereignty and securing affordable and reliable connectivity, and to expect recognition of those priorities by other states as well as multinational technology companies and their host-nation jurisdictions. For India and Taiwan, their democratic predispositions fuel civil-society efforts to limit cyber-enabled surveillance. Fiji, which is vulnerable to natural disasters, views climate-resilience cooperation as part of responsible behaviour, including in relation to digital cooperation.
7. Responsible cyber behaviour in the Indo-Pacific may involve the recognition that it's equally important to protect physical infrastructure as it is to protect and secure the information environment. At the moment, many Indo-Pacific countries' response to cyber-enabled threats is to over-regulate, introducing a slew of legislation and regulations

that focus on criminalising certain behaviours. There's also been an increase in their reliance on surveillance technologies, content controls and other restrictive policies on freedoms of information, speech and expression.

8. For most Indo-Pacific stakeholders, responsible cyber behaviour is about the nurturing of expertise within government and non-government (Track 2) sectors, and their (ease of) access to most relevant and impactful international platforms, such as the UN OEWG.
9. Responsible cyber behaviour may involve the need for guidelines for the purchase, selling and use of dual-use technologies. Four of the seven countries reviewed—Fiji, Cambodia, Indonesia and Pakistan— lack such guidelines, do not have strong safeguards or haven't clearly or publicly elaborated them. Meanwhile, India, Japan and Taiwan have specific controls in place and adhere to international frameworks such as the Wassenaar Arrangement. Japan's guiding principle for weapons and military technology exports is to trade with friendly nations only; Taiwan maintains similar controls. The existence of that legislation and those regulations, however, may not be enough to effectively curtail the unwanted proliferation of dual-use technologies. Parliamentary or public oversight of governments' and industries' compliance is currently lacking.

Conclusion

At a time when international discussions on security and collaboration in cyberspace are under pressure from deepening strategic competition, there's a serious need to develop a deeper understanding of how other states understand what it means to be a responsible cyber actor. This report contributes to that conversation by presenting viewpoints from often under-analysed state-based perspectives across the Indo-Pacific.

Our analysis shows that domestic and operational cyber policies, practices and capabilities lack the agreed standards, principles or norms that allow a notion of 'responsibility' to be internalised. It's unlikely that most Indo-Pacific governments will exercise greater transparency and accountability in their own right, instead pointing to principles of state sovereignty (and non-interference) and the need to first address capacity shortfalls. Nonetheless, the international community, Tracks 1 and 2, should advance the broadening of the notion of responsible cyber behaviour on the premise that it's grounded in the existing UN framework. To better understand how states conceive of what it means to be a responsible actor in cyberspace, we must consider how governments and non-government actors reconcile domestic interests and international commitments. From there, additional standards, principles and guidelines could be developed to address states' internal and operational responsibilities.

Country chapters

Cambodia

Gatra Priyandita and Louise Marie Hurel[6]

Overview

Cyber-enabled threats have emerged as a security concern in Cambodia, given increasing cyber attacks against Cambodian organisations and the proliferation of cyber-scam compounds in the country. While Cambodia has laid legal and institutional foundations to defend its cyberspace, such as the Cybercrime Law and Cybersecurity Law, much of the responsibility for protecting systems is left to individual operators, and overall enforcement at the national level remains weak.

Cambodia's focus on regime stability and sovereignty shapes its approach to responsible cyber behaviour. Domestically, the government aims to strengthen cybersecurity infrastructure, promote public and private awareness, and legislate against cybercrimes.

Internationally, Cambodia advocates for multilateral cooperation on cybersecurity, supporting capacity-building initiatives so long as they're done without political conditions. It prefers a collaborative approach in forums such as ASEAN and the UN, where it encourages the development of binding rules to limit the misuse of ICTs by state actors. Cambodia's stance emphasises the importance of national sovereignty and mutual respect in cyberspace. However, challenges remain in fully aligning domestic actions with international positions. Cambodia struggles to balance its focus on regime security with human rights considerations, and its cybersecurity efforts are still evolving. Despite advocating for responsible behaviour globally, Cambodia faces internal inconsistencies in implementing those principles.

National dimensions

Institutions and accountability

The Cambodian Government's understanding of 'responsibility' in cyberspace stems from its threat environment and constrained capacity to secure cyberspace. Cambodia remains vulnerable to transnational crime, and its security forces struggle to combat cyber-enabled crimes. Transnational criminal organisations, for example, run online scam compounds using forced labour. In 2023, the UN High Commissioner on Human Rights reported that approximately 100,000 people were forced to work in such scam compounds.[7] Cambodia also faces state-sponsored cyberattacks, notably from Vietnam and China, which target Cambodian Government agencies and private entities.[8] Faced with such challenges, Cambodia has, for the first time, included cyber defence as a priority in its 2022 National Defence Policy. This reflects the growth in threats emanating from cyberspace and a recognition that Cambodia needs to prepare to face those challenges.[9]

Respect for national sovereignty, which includes refraining from cyber operations that violate the sovereignty of other nations and engaging in capacity-building efforts without political conditions, is a key message that Cambodia expresses internationally. The drivers of those views are deeply rooted in Cambodia's historical experiences, political landscape and cultural values. Cambodia's dark period under the Khmer Rouge and subsequent recovery have fostered a strong emphasis on sovereignty and national security. Politically, the government's focus on maintaining peace and stability shapes its cybersecurity policies. Culturally, there's a collective understanding of the importance of community protection and mutual respect, translating into expectations of responsible behaviour in cyberspace.

Additionally, Cambodia's views have been influenced and internalised through participation in international discussions and frameworks on cyber norms, particularly those advocated by the UN and ASEAN.

Domestically, the government signals its responsibility through efforts that improve cybersecurity standards in government and promote cybersecurity awareness among the private sector and individuals. The Cambodia ICT Masterplan 2020 emphasises developing robust legal and institutional frameworks to ensure cybersecurity.[10] Meanwhile, the Cybercrime Law aims to combat cyber offences. The Cambodian Government has also engaged with industry to encourage responsible behaviour. The National Bank of Cambodia, for example, has specifically engaged with the banking sector through the Technology Risk Management Guidelines, which underscore the importance of ongoing risk management in identifying, assessing and responding to cyber risks. However, efforts to enforce those laws and guidelines are patchy, given constraints in financial and human resources.

Operational dimensions

Responsible use and acquisition of technologies

Cambodia lacks specific laws or guidelines on the responsible use and acquisition of technologies. The Telecommunications Law of 2015 is the primary legislation addressing telecommunications and related activities in Cambodia. The law emphasises the safety and development of telecommunications infrastructure but falls short of detailing specific cybersecurity requirements for protecting data and network security. The lack of specific cybersecurity standards in these laws creates several constraints. Firstly, the lack of detailed regulations leaves government and private entities without clear guidelines for implementing robust cybersecurity measures. That is regulatory vacuum increases the risk of cyber threats and data breaches, as entities might not have standardised practices to follow. Secondly, the weak enforcement provisions mean that even the existing broad guidelines might not be effectively implemented, leading to inconsistent cybersecurity practices across different sectors. Finally, the general nature of these laws may inadvertently enable excessive surveillance and monitoring by authorities.

Law enforcement has procured and employed ICT tools for surveillance without clear regulatory restrictions. Cambodia has cooperated extensively with Chinese firms, which provide spyware, surveillance, and DNA screening equipment. Open-source reports also indicate that Cambodian authorities have utilised spyware and surveillance technologies to monitor political dissidents, activists, and journalists.[11] Associated procurement processes are opaque, with minimal public disclosure or oversight, further fuelling fears of abuse. Human rights organisations and international bodies have criticised Cambodia for using cyber-enabled technologies to suppress dissent and infringe on privacy rights. This lack of regulatory transparency underscores the urgent need for stronger frameworks and increased transparency in technology acquisition and use.

Responsible cyber operations

Cambodia's Ministry of National Defense (MND) and the General Commissariat of National Police under the Ministry of Interior are the primary agencies involved in cybersecurity operations. Since 2022, the MND and Royal Cambodian Armed Forces have built cyber-defence capabilities to safeguard the military's networks and critical national infrastructure. Initial efforts have focused on developing legal frameworks, organisational structures and interagency cooperation mechanisms to address cyber threats. There are no clear restrictions or constraints on what the government, the military, or law enforcement can and can't do in cyberspace domestically.

The MND's Cyber Warfare Unit operates under the directives of the MND, focusing on military cybersecurity policies and strategic defence against cyber threats. Similarly, the General Commissariat of National Police follows the procedural guidelines outlined by the Ministry of Interior, which include cybercrime prevention, investigation and collaboration with international law-enforcement agencies. Those units also gather cyber intelligence and share information with national and international bodies. However, these cyber units' auditing, reporting, and accountability mechanisms aren't well -publicised, and their operations have limited transparency. While there might be internal oversight and reporting structures within the respective ministries, there's a lack of publicly available information on formal auditing processes or external accountability measures. That lack of transparency underscores concerns about the potential misuse of power and the need for stronger governance frameworks to ensure that cybersecurity operations are conducted responsibly and ethically.

International dimensions

International law and cyber norms

The Cambodian Government supports the application of international law in cyberspace and adheres to the UN norms of responsible state behaviour.[12] Even though it hasn't published its interpretation, regional bodies such as ASEAN have been the closest to rehearsing and indicating what responsible state behaviour in cyberspace means for the region. That was the case for the statement provided by Cambodia, on behalf of ASEAN countries, at the UN OEWG, which noted that 'ASEAN reaffirms the need to enhance cooperation to promote an open, secure, stable, accessible, and interoperable, and peaceful ICT environment and prevent the risk of misperception and miscalculation by developing trust and confidence.'[13] Cambodia hasn't elaborated on how it might seek international law to apply in cyberspace.

However, Cambodia wants to see the international community 'develop rules, norms, principles within a framework of binding obligations'.[14] Officials believe binding rules would help to constrain state actors' potential misuse of ICTs against other states while encouraging cooperation under commonly agreed-upon terms. For that reason, in 2019, Cambodia joined 12 other countries—including China, Russia and Venezuela—to advocate for the establishment of an international convention to combat cybercrime. The Cambodian Government believes that such a convention could strengthen international legal mechanisms to ensure that states behave responsibly in cyberspace.[15]

Foreign policy and international cooperation

A commitment to international cooperation, capacity building and respect for state sovereignty informs the government's pursuit of good international behaviour. Fundamentally, Cambodia also insists that any support must be provided 'without prejudice to the sovereignty of states, the confidentiality of national policies and plans, respect for partnership and human rights and freedom, as well as apolitical and non-discriminatory [*sic*]'.[16] This statement was probably in response to a perception that development support by donor countries privileges democratic countries over others. Few government documents explicitly reference the global framework for responsible state behaviour in cyberspace.

The Cambodian Government demonstrates responsibility in cyberspace by participating in regional cooperation efforts. Cambodia has actively participated in initiatives such as the Singapore Cooperation Programme's 'Governing Cybersecurity: Policies, Practices, and Processes', where officials from Southeast Asian states received training on cybersecurity policies based on Singapore's experience.[17] Additionally, Cambodia has been involved in technical cooperation projects to improve cyber resilience, such as the Project for Improvement of Cyber Resilience with Japan's International Cooperation Agency and the Cambodia National Computer Incident Response Team Assessment funded by the International Telecommunication Union.[18]

Cambodia's approach also underscores the significance of regional solidarity and collective security in addressing cyber threats. The Ministry of Post and Telecommunications and Ministry of Interior affirmed Cambodia's commitment to collaborate with ASEAN member states towards an open, inclusive, safe and secure cyberspace during the ASEAN Ministerial Conference on Cybersecurity, Singapore International Cyber Week, and ASEAN Senior Officials Roundtable on Cybercrime, where discussions centred on building trust and security in the emerging digital order. Those cybersecurity forums allow Cambodia to learn from different nations' best practices and share a local perspective that's often under-represented internationally.

Fiji

Ilaitia B Tuisawau and Louise Marie Hurel

Overview

Fiji, an archipelago with nearly 1 million people, has 95% of its population online.[19] Cyber threats have emerged as a growing concern, especially in the light of major cyberattacks. For instance, in 2021, a cyberattack on the Fiji Government's ICT services took systems offline for two weeks.[20] The country's vulnerability to the effects of climate change imposes further risks that telecommunications infrastructure can be threatened by natural disasters and rising sea levels. Fiji's perception of responsible cyber behaviour is, thus, shaped by its limited cyber capacity, geographical vulnerability as a small island nation, and role as a regional hub for digital connectivity. As the Pacific Islands Forum (PIF) host nation, Fiji played a key role in the 2018 Boe Declaration on Regional Security, which identified cybersecurity as a regional priority.

Fiji views responsible cyber behaviour through the lens of cooperation. Internationally, it's committed to adhering to global standards, sharing information on cyber threats and participating in cyber capacity-building (CCB) initiatives. Fiji often seeks external support to strengthen its resilience against cyberattacks, recognising that its modest cyber workforce and infrastructure require ongoing development. Cooperation with more cyber-mature countries is a cornerstone of Fiji's strategy, together with its active participation in multilateral forums such as the UN and the PIF.

Domestically, Fiji strives to build internal cybersecurity capacity by establishing institutions, laws and regulations, such as the Online Safety Act and the Online Safety Commission. Those initiatives highlight Fiji's commitment to promoting responsible behaviour at the governmental and individual levels as part of a culture of online safety and accountability.

For Fiji, responsible state behaviour means conforming to internationally agreed norms and ensuring that its cyber capabilities are used for defensive purposes, such as combating transnational crime. Fiji lacks offensive cyber capabilities and specific regulations for dual-use technologies.

National dimensions

Institutions and accountability

Fiji's structural factors, as outlined, drive a consistent approach to training, sustainability and national policy-development partnerships.

Concerned about the impact of natural disasters on ICT infrastructure, Fiji joined other Pacific nations in the 2018 Boe Declaration to broaden the concept of security to include cybersecurity and a commitment to 'maximising protections and opportunities for Pacific infrastructure and peoples in the digital age'.[21] Fiji's cybersecurity policies consistently underline the need for international cooperation to secure cyberspace and develop national capacities.[22] The government participates in CCB activities, recognising its lack of resources—financial and human—to manage an active cybersecurity centre.

The Fiji Government and Fijian civil society further emphasise the need for climate-resilient support in CCB. The Boe Declaration declared climate change the top security challenge for Pacific island states.[23] In its 2022 submission to the UN OEWG on ICT, Fiji highlighted the importance of 'climate-resilient' cybersecurity infrastructure and called on international efforts to support that.[24]

Internally, the government aims to be a responsible cyber actor by improving its cybersecurity capacity. Key legal foundations include the Criminal Act 2009, Online Safety Act 2018 and Cybercrime Act 2021. The Cybercrime Act addresses offences against computer systems and content-related offences.[25] Despite the Online Safety Act focusing on deterring offensive or harmful content—and thus being arguably 'different' in scope from what had been agreed in the framework for responsible behaviour in cyberspace—one of its objectives is to 'promote responsible online behaviour and online safety' and do so in tandem with promoting a safe online culture and environment.[26]

In 2023, the Ministry of Home Affairs and Immigration and the ministry responsible for communications initiated consultations to develop the National Critical Infrastructure Cybersecurity Incident Response and Recovery Framework and establish a Critical Infrastructure Computer Emergency Response Team (CI-CERT) and national CERT. That same year, Fiji participated in regional workshops, such as the Asia Pacific Network Information Centre, to develop draft versions of the National Cybersecurity Incident Response and Recovery Framework.[27] In 2024, Fiji and Australia signed a memorandum of understanding on cybersecurity to develop the national CERT.

Fiji has structured a strategic vision for domestic cybersecurity governance, drafting the National Security Strategy (NSS) in 2016, covering all aspects of national security, including critical-infrastructure security and cybersecurity. Despite multiple revisions, the Cabinet hasn't yet endorsed the NSS. In December 2023, the government committed to reviewing the NSS in 2024. However, no document has yet been published at the time of writing.[28] Fiji is also undergoing a second Cyber Maturity Model review to inform the national cybersecurity strategy's development.[29] Despite recognising the need for a strategy, it remains a medium-level priority on the political agenda. Essentially, private companies are responsible for managing their information security with little government assistance.

Those initiatives highlight Fiji's view that responsible cyber behaviour intersects with international security, trade and economic development. However, cybersecurity and cybercrime remain challenging due to resource limitations and competing agendas. Support from neighbouring countries and non-government organisations can help to prioritise and consolidate responsible cyber behaviour through institutional developments and policy updates. Notably, Fiji's accession to the Budapest Convention on Cybercrime signals a step towards legal harmonisation and enhanced cooperation.

Operational dimensions

Responsible use and acquisition of technologies

Fiji lacks direct guidelines or regulations on the responsible use and acquisition of technologies, including controls for dual-use exports. The central Fiji Procurement Office under the Ministry of Finance coordinates all government technology procurements, but public information on usage guidelines or restrictions is unavailable.

In 2021, Fiji passed the Cybercrime Act, inspired by its ratification of the Budapest Convention on Cybercrime. The Act criminalises cyber-enabled crimes such as unauthorised access to computer systems and interceptions of data.[30] However, Fiji doesn't mandate the reporting of cyber incidents. The banking and financial services sectors maintain the highest cybersecurity standards, as they're prime targets for cyberattacks. In March 2023, the Reserve Bank of Fiji imposed minimum cybersecurity standards for those sectors through the Prudential Supervision Policy Statement.[31]

All ICT network infrastructure in Fiji is owned by private companies (Telecom Fiji Limited and mobile operators Vodafone Fiji and Digicel Fiji), which aren't required to adhere to government policies on acquiring technologies or equipment. For instance, unlike in many Western states, there are no regulations restricting the use of Chinese devices for both core network equipment and customers' digital devices. Practical economic and developmental considerations drive the procurement of ICT equipment.

Fiji benefits from six submarine cables providing connectivity and emerging players that are expanding infrastructure projects.[32] In 2023, Starlink received a licence to deliver broadband internet services, and, in 2024, Starlink services were expanded to more than 300 Fijian islands.[33] The Deputy Prime Minister noted in the announcement that 'licensing of Starlink for commercial use is a game changer for Fiji as it strengthens our resilience in providing connectivity during natural disasters—this also serves the purpose of the Fiji Government's efforts in connecting the unconnected population.'[34]

Responsible cyber operations

Fiji has no known offensive cyber capabilities and lacks guidelines for cyber operations. Cybertools are primarily used for countering transnational crime (such as drug trafficking, money laundering and terrorism). The Fiji Police Force has the primary power to intercept information online and for the enforcement of cybercrime legislation. The 2021 Cybercrime Act has provisions that allow the police to issue warrants for subscriber data and communications content. However, the procedure for lawful online interception by the Fiji Police isn't publicly available.

There's no specific parliamentary unit tasked with the oversight of cybersecurity. However, the parliamentary standing committees on foreign affairs and defence, justice, law and human rights could function as platforms for parliamentarians to highlight issues in cyberspace.

International dimensions

International law and cyber norms

As the then-chair of the PIF, Fiji released a statement to the UN OEWG on ICT on 30 March 2022. It committed to the applicability of international law, the UN Charter, and the UN's eleven norms of responsible state behaviour in cyberspace.[35] However, Fiji hasn't detailed how international law specifically applies in cyberspace. Fiji's support for international law and norms is likely to reflect its vulnerability to foreign cyberattacks. The global framework for responsible state behaviour encourages international cooperation to prevent the misuse of ICTs, supporting Fiji's development needs.

Fiji's 2022 statement also emphasised critical information infrastructure security. It highlighted two key areas: the need to identify critical infrastructure in cyberspace and the unique contribution from Pacific island countries, which emphasised capacity building for climate-resilient ICT infrastructure.

Fiji's government has been consistently active in its engagement with the UN OEWG process. That includes contributions to joint papers on CCB measures, a proposal for a UN Cyber Points of Contact Directory, and the Cybersecurity Capacity Maturity Model as part of the assessment and development of national strategies. For example, the joint submission for the UN Cyber Points of Contact Directory sought to support communication checks and information-sharing during cyber incidents.[36]

Foreign policy and international cooperation

Fiji has long advocated for international CCB, primarily through regional efforts and bilateral agreements with Indo-Pacific countries. Fiji's foreign policy and international partnerships strongly connect its development and cybersecurity agendas.

Regional cooperation has been key to advancing shared cybersecurity goals among Pacific island countries. The Boe Declaration's action plan included supporting forum members' accession to the Budapest Convention, developing national cybersecurity policies, providing education and training on responsible cyber behaviour, and strengthening CERTs.

The Boe Declaration's action plan explicitly mentions responsible cyber behaviour and has guided broader collaboration with Indo-Pacific countries. They include the Partners in the Blue Pacific, a group composed of Australia, Japan, New Zealand, the UK and the US. Set up in 2022 to economically support Pacific island nations, it has incorporated cybersecurity as an area for prospective collaboration.[37] In 2023, it participated in the Pacific Cyber Capacity Building and Coordination Conference as a potential annual forum.[38]

Australia and New Zealand play important roles in Fiji's cybersecurity governance. In February 2024, Fiji established the Vuvale Partnership with Australia, which includes cybersecurity cooperation. That was followed by a cybersecurity memorandum of understanding in May 2024, focusing on critical infrastructure and CERT development and promoting international cyber norms.[39] Similarly, the 2022 Duavata Partnership with New Zealand underscores cybersecurity and intelligence as priority areas of cooperation. Beyond bilateral and multilateral arrangements, the country is also part of technical cooperation networks such as the Pacific Cyber Security Operational Network (PaCSON), which is a regional network of cybersecurity experts in the Pacific dedicated to coordinating and supporting incident-response activities.[40]

Fiji is also working to improve its capacity to combat cybercrime. In 2024, it acceded to the Budapest Convention on Cybercrime, aligning its domestic laws with international standards.[41] That enables Fiji to enhance international cooperation in cybercrime investigations with other signatories and benefit from initiatives such as the GLACY+ project, which is a resource for technical assistance in fighting cross-border cybercrime.[42]

India

Anushka Saxena

Overview

India's perception of responsible cyber behaviour reflects the country's view of digital technology as a key driver of economic growth and social development. However, India's complex cyber threat landscape includes threats from cybercriminals, terrorist organisations and state actors involved in cyber espionage. That includes the use of cyber means to spread disinformation that risks social unrest, particularly on sensitive political and religious matters.

India has no official document defining 'responsible cyber behaviour', but its policies and laws provide insights into its approach. Two dimensions shape India's perspective. First, India stresses international cooperation and adherence to norms that prevent the misuse of ICTs for malign purposes. Given the transnational nature of cyber threats, Indian officials believe that collaboration between states is essential. Second, India defines responsible behaviour domestically by regulating irresponsible cyber activities, such as cyberterrorism and data breaches.

India's top-down approach to cybersecurity focuses on regulatory interventions in which the government plays a central role in guiding private-sector and civil-society efforts to protect cyberspace. That approach includes a broad mandate for public authorities, from enforcing punitive measures against noncompliance to conducting surveillance and offensive countermeasures against cyber threats.

Although India is still developing its doctrine on responsible technology use, key pillars are emerging in AI and drones, where privacy and ethical standards are key considerations. In the military domain, cyber-linked technologies are used for intelligence, surveillance and reconnaissance and offensive countermeasures.

Internationally, India advocates for states to refrain from cyber operations that violate norms, such as state-sponsored cyberterrorism. As a leader of the Global South, India strongly supports CCB. It seeks to create mechanisms such as the UN Cyber Points of Contact Directory to strengthen cooperation and mitigate cyber vulnerabilities.

National dimensions

Institutions and accountability

India is the world's second most 'connected' country, with more than 800 million active internet users.[43] The 2022 annual report by CERT-In highlighted 1,180 cyber threat alerts and vulnerabilities—a 12% increase from 2021.[44] Data breaches pose a major threat to Indian IT infrastructure, especially government servers. India has also been facing significant threats by foreign state and non-state actors targeting its critical national-security infrastructure. One example is the threat posed by Chinese cyber actors, which can be placed in the context of the larger, strategically competitive, relationship between India and China.

India's perspectives on responsibility can be interpreted from its legislation and government documents. It lacks a unified national cybersecurity policy but relies on several laws to address cyber threats. The Information Technology Act 2000 defines responsible cyber behaviour by mandating 'reasonable security practices' to protect sensitive data from unauthorised access and misuse. While the Act doesn't explicitly refer to 'responsible cyber behaviour', it frames breaches of personal data as irresponsible, requiring strict legal consequences.

In 2013, India introduced the National Cybersecurity Policy, which promotes cyber hygiene, user responsibility and secure information flows.[45] The policy offers insights into India's view of cyber responsibility. One objective is to foster a 'culture of cybersecurity and privacy enabling responsible user behaviour'. That includes promoting cyber hygiene practices, cooperating with government actors to prevent and prosecute cybercrime, and establishing internal guidelines for secure information flow and crisis management in businesses. The policy encourages businesses to adopt internal security guidelines but has been criticised for imposing rigid requirements, such as the controversial six-hour cyber incident reporting rule mandated by CERT-In in 2022.[46] Although intended to enhance security, the rule faced criticism for being unrealistic and having excessive data-retention mandates. The 2013 policy isn't binding, and many elements are too broad for targeted action. However, progress has been made on some strategies, such as operating the 24/7 National Critical Information Infrastructure Protection Centre for reporting cybersecurity incidents and establishing a regulatory framework for critical information infrastructure.[47]

The government also views responsible behaviour as ensuring content security, particularly in managing online hate speech and offensive material. The government uses articles 69A, 69B and 79A of the IT Act 2008 (amended) to block content on platforms such as Facebook (Meta) and Twitter (X) when necessary for national security and public order. In 2021, it introduced new intermediary guidelines to enforce technology companies' cooperation with law enforcement.[48] In February 2021, the Ministry of Electronics and Information Technology introduced the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, requiring tech companies to cooperate with law enforcement to track users spreading information against the national interest. Those measures aim to 'institutionalise social media' as part of the government's top-down cyber and IT security approach.[49]

India's approach combines domestic cybersecurity governance and content regulation, highlighting its emphasis on national security. However, it faces criticism for impinging on free speech.

Operational dimensions

Responsible use of technologies

As a hub for ICT services, India governs the acquisition of cyber-linked technologies through certain regulations targeting the private sector and civilians. The 2023 Telecommunications Act, for instance, requires telecom networks and service providers to comply with cybersecurity standards set by the central government or the Telecom Regulatory Authority of India (TRAI).[50] The Act mandates secure storage of traffic data and proper management of encryption. It also empowers the government to temporarily take control of telecom services or intercept communications if national security or foreign relations are threatened. The Telecom Regulatory Authority regularly updates the cybersecurity standards.

There are no ethics, privacy and cybersecurity guidelines on AI-based technologies. Instead, AI regulations in India are currently focused on building capacity, developing an indigenous computer cluster and enabling research and innovation in the field. However, the 2023 *India AI report*, which lists the priorities of the Ministry of Electronics and Information Technology concerning AI, highlights the risk of generative AI in enabling cybercrime and lists 10 guidelines to build 'responsible AI'.[51]

Responsible cyber operations

India has built institutional capacity for offensive cyber operations. In 2018, the Defence Cyber Agency (DCA) and the cyber groups for the Indian Armed Forces were established to empower the military's cyber capabilities and conduct cyberwarfare.[52] The DCA conducts those operations, which may involve network hacking, surveillance, data recovery and encrypted communication infiltration.[53] The DCA collaborates with CERT-In and the National Cybersecurity Coordination Centre, which track and report cybersecurity threats.[54] However, the DCA's activities, budget and operations remain undisclosed.[55]

The National Technical Research Organisation, reporting directly to the Prime Minister's office, probably oversees offensive operations against cyber aggression, such as data breaches or attacks on critical infrastructure.[56] Such acts of 'aggression' may comprise breaches of sensitive data and uploads of critical national-security information to the dark web, attacks on critical information infrastructure and cyberterrorism.

Domestic surveillance operations are important to the Indian Government's policy to address irresponsible cyber behaviour. Under section 69 of the IT Act 2008 (amended), the central and state governments can intercept, monitor or decrypt any information in a computer resource to protect 'sovereignty, national security, friendly relations with international governments, [and] integrating public order'.[57] India views responsible cyber behaviour and ICT use as activities that don't undermine those priorities, authorising all levels of government to tackle threats through surveillance. The Indian Cyber Crime Coordination Centre under the Ministry of Home Affairs also enables citizens to register as 'unlawful content flaggers' to report online content for removal.[58]

Although oversight mechanisms mandate regular reviews of surveillance operations, parliamentary requests often run up against the inherent secrecy of intelligence operations.[59] The 2021 Pegasus spyware scandal, in which journalists, politicians and activists were surveilled, highlights enduring concerns about unchecked surveillance practices.[60]

International dimensions

International law and cyber norms

While India supports the global framework for responsible state behaviour in cyberspace, it hasn't outlined a specific interpretation of how international law applies. One principle that India strongly champions is that state sovereignty and territorial integrity should extend to cyberspace. Officials have emphasised that a state aware of harmful cyber activities originating from, or routed through, its territory must take reasonable steps to stop them, reflecting India's approach to quasi-state actors (QSAs) conducting cross-border cyber operations and the issue of state responsibility.[61]

India prioritises countering cyber terrorism. Its contribution to the 2022 OEWG *Annual progress report* called for strengthened law-enforcement cooperation to prevent cyberspace from being used for terrorist purposes.[62] At the OEWG's fifth substantive session in 2023, India highlighted the threat posed by QSAs and state-sponsored cybercriminals.

Having been the target of state-sponsored cyber operations, India has called on international partners to develop joint accountability mechanisms for QSAs' irresponsible cyber behaviour. Examples include signing a memorandum of understanding between CERT-In and its Japanese counterpart in 2015 for information-sharing on cyber threats and vulnerabilities, and the US–India Cyber Relationship Framework, which enables cybersecurity-related cooperation between law-enforcement agencies in both countries.[63]

From India's perspective, multilateral regulation of QSAs' activities and the formulation of clear norms of state responsibility for the cyber activities of QSAs operating within states' territory are important legal principles. India has subsequently argued at the OEWG that 'QSAs exploit a legal gap in our understanding that allows them some of the advantages of sovereignty without corresponding obligations.'[64]

In this regard, India has pushed for seamless threat-intelligence sharing by establishing a global Point of Contact Directory, wherein countries must assign a diplomatic and technical liaison during deliberations on specific cyber/ICT security areas. Beyond just threat-intelligence sharing, this enables cyber-related conflict de-escalation through confidence-building measures, such as establishing national points of contact.[65] This proposal is part of India's broader goal to enhance capacity-building among its key national ICT security stakeholders, such as CERT-In and the Telecom Cyber Security Incident Response Team. India's push for a Global Cyber Security Cooperation Portal reflects its commitment to joint capacity building despite enduring constraints.[66]

India lacks a public cyber attribution policy. In response to incidents such as the ShadowPad malware attacks from China, India focuses on building resilience, investing in chief information security officers, formulating cyber crisis management plans, and monitoring threats through the National Cyber Coordination Centre. That reflects India's reactive approach to cybersecurity, prioritising post-incident responses over the proactive enforcement of responsible behaviour.[67]

Foreign policy and international cooperation

The Indian Government's vision of itself as a leader of the Global South shapes its international cyber engagement. Amid deepening strategic competition between states, India seeks to project its desired leadership role by advocating CCB, especially for less cyber-mature countries in the Global South. It has signed more than 30 cyber agreements with Global South countries, focusing on dialogue and technical training.[68] Additionally, India exports indigenous technologies, such as the Unified Payment Interface and India Stack, to offer cost-effective solutions to ICT-related challenges in developing countries. Those efforts extend to regional organisations such as ASEAN and the IBSA (India, Brazil, South Africa) Dialogue Forum.

To a lesser extent, India leverages the Quad partnership with Australia, Japan and the US to advance its cyber and technology interests. While the Quad promotes collaboration in cybersecurity, critical-infrastructure protection and emerging technologies, India opposes using coordinated countermeasures or joint attribution.

Despite its global ambitions, India's top-down, government-led approach to cyber governance limits engagement with the private sector and civil society. India's delegations at the OEWG have excluded private-sector and civil-society participation, and its cybersecurity regulations involve minimal consultation with businesses.[69] Although India nominally supports 'multistakeholderism', it hasn't signed the Paris Call for Trust and Security in Cyberspace, despite calls by several key Indian non-government stakeholders.

Indonesia

Gatra Priyandita

Overview

Indonesia perceives responsible behaviour in cyberspace as requiring countries to take three main actions: refrain from misusing cybertools to violate another country's sovereignty; commit to international cooperation; and engage in CCB. That perspective stems from Indonesia's view of cyberspace as a key vulnerability, and by its limited capacity to enforce laws and investigate cyber incidents.

Internationally, Indonesia advocates multilateral cooperation to impose legal and normative constraints on powerful states' misuse of ICTs. It uses diplomacy to advocate for the peaceful use of ICTs, seek support for capacity-building and ensure that sovereignty and multilateralism are upheld in international cyber norms. Its approach to international issues in cyberspace is shaped by its commitment to multilateralism, its status as a developing economy with growing cyber capacity, and its insistence on sovereignty as the foundation of international relations.

While it maintains legal and institutional instruments to respond to cyber threats, Indonesia's capability is hampered by a lack of resources. It maintains cyber capabilities for defensive purposes, though there are insufficient checks to prevent the misuse of ICTs by authorities.

National dimensions

Institutions and accountability

The Indonesian Government recognises the transformative powers of digital technology but also acknowledges the risks emanating from cyberspace. The National Cyber and Crypto Agency (*Badan Siber dan Sandi Negara*, BSSN) reported more than 1 billion 'traffic anomalies' in 2022, underscoring the country's vulnerability to cyber threats, including ransomware and cyber terrorism.[70]

Indonesia's approach to cybersecurity crystalised throughout the 2010s. The BSSN, established in 2017 and empowered by a 2021 presidential mandate, is the primary agency responsible for developing, implementing and evaluating cybersecurity policies.[71] Many other government agencies, including the National Police and the Ministry of Communication and Informatics, are also responsible for various aspects of law enforcement and cyber and information security policy formulation. Those agencies maintain international communication channels, which they may use to share information about cyber incidents and coordinate capacity-building initiatives. BSSN collaborates with civil society and experts to monitor the cyber threat environment. [72]

Indonesia's legal framework requires organisations to secure their systems. The Personal Data Protection Bill mandates minimum cybersecurity standards, and noncompliance is punishable by fines and imprisonment.[73] The bill was passed in October 2022 and is effective as of October 2024. Nonetheless, exactly how the law will be implemented remains uncertain.

Internationally, Indonesian officials recognise that international cooperation is another dimension of responsible cyber behaviour. The country's international cyber engagements emphasise collaboration on CCB, information/intelligence sharing, and strengthening law-enforcement networks.[74] The government expects cyber-mature countries to assist less-developed countries in building the capacity to respond to challenges in cyberspace.

Indonesia's submissions to the ASEAN Regional Forum express concerns that cyberspace is being 'misused' by state actors in a manner that 'poses risks to international peace and security as well as stability of national political, economic and social [*sic*] domain'.[75] In response, Indonesia calls on states to 'promote the use of ICTs for peaceful purposes'—in particular, with 'respect for sovereignty, human rights, fundamental freedoms, as well as sustainable and digital development'.[76] Indonesia has, through the UN OEWG process, called for the international community to pursue a 'collective declaration of all states to refrain from militarisation of cyberspace that may undermine international peace and security'.[77]

Operational dimensions

Responsible use and acquisition of technologies

To prevent the misuse of cyberspace, Indonesia has sought to demonstrate greater government control over ICTs through several legislative and regulatory instruments, particularly the 2008 Information and Electronic Transaction (ITE) Law. The law, along with its subsequent revisions (2016 and 2023) and other operational regulations, establishes the legal framework outlining the responsibilities of electronic service operators in Indonesia. Under the ITE Law, hacking and the private possession of hardware, software or other tools used to commit cybercrime are criminal offences. While no specific legal framework regulates the infection of IT systems with malware, under the ITE Law that action can be classified as system interference.

Through the BSSN, the Indonesian Government continuously publishes guidelines and organises practical awareness-building exercises to build community readiness for cybersecurity incidents. The agency has also published standards and regulations concerning the security of ICT products. However, the BSSN's capacity to review and audit the technologies used by the government is constrained by under-resourcing, poor institutional communication about ICT use and limited human capital.

Domestically, Indonesia has no standing government policy on coordinated vulnerability disclosure. However, the Personal Data Protection Bill, strongly modelled on the European Union's General Data Protection Regulation, requires organisations affected by data breaches to submit written notifications to the BSSN. While the BSSN and the National Police engage industry and experts to map the cyber threat environment and offer support, the absence of a disclosure requirement limits the government's capacity to fully grapple with Indonesia's cyber threat landscape.

Responsible cyber operations

The Indonesian Armed Forces (*Tentara Nasional Indonesia*, TNI) is responsible for cyber defence. In 2017, the TNI established a cyber unit (*Satuan Siber*, Satsiber) responsible for developing doctrine, policy and procedures to respond to cyber threats, particularly those targeting defence-related critical infrastructure.[78] Each branch of the armed services has subordinate cyber units under Satsiber, supported by the Cyber Defence Centre, which operates under the command of the Defence Intelligence Agency within the Ministry of Defence.[79] Discussions are ongoing about creating a 'cyber force', although its shape and purpose haven't yet been elaborated.[80]

Despite this force structure, Indonesia's cyber defence lacks a formal doctrine. Internal military documents focus on organisational and resource matters, such as coordination, staffing and infrastructure, rather than specifying when and how cybertools should be deployed.[81] Indonesia has no stated policy on offensive cyber operations.[82] Consistent with its largely defensive strategic culture, Indonesia's cyber capabilities are defensive and don't serve a purpose beyond protecting national security, fighting cybercrime and cyberterrorism and addressing other domestic challenges.[83] Diplomacy and multilateralism remain key to Indonesia's approach to addressing external cyber threats. Although long-term plans to establish offensive cyber capabilities exist, those capabilities haven't yet materialised.[84]

In response to internal security challenges (particularly terrorism), the Indonesian security apparatus maintains well-developed capabilities for domestic surveillance. There are publicly known cases of surveillance equipment being used against citizens for purposes other than national security.[85] There's no single rule for interception, and there are no known guidelines on what is and isn't permissible. Rather, a series of ministerial and agency regulations provide certain individuals with the authority to conduct cyber-enabled interceptions. For instance, police surveillance requires the approval of the head of the Criminal Investigation Agency of the National Police (Bareskrim).[86] Those investigations must also, in principle, be based on serious considerations of privacy and human rights. However, existing policy documents don't clarify the guardrails that would prevent misuse.

International dimensions

International law and cyber norms

Indonesia endorses the global framework of responsible state behaviour in cyberspace and has participated in the UN Group of Governmental Experts (UN GGE). Indonesia has endorsed that international law, particularly the UN Charter, is essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful ICT environment. However, the government prefers separate legal arrangements regarding international laws governing cyberspace. Indonesia has specifically argued against the 'automatic application of existing laws without examining the context and unique nature of activities in cyberspace' and suggested that 'practical adjustment and possible new interpretations are needed.'[87]

In an October 2021 submission to the Ad Hoc Committee on Cybercrime, Indonesia emphasised the wide-ranging implications of cybercrime.[88] It called for a cybercrime treaty to be mindful of those implications and to reflect the principles of sovereign equality and non-interference in states' domestic affairs. It preferred that this treaty considers content-related crimes, including disinformation and copyright infringement. Consistent with its preference for multilateralism, Indonesia prefers that the treaty promotes cooperation on cybercrime through information sharing and best-practice exchanges.

Indonesia is particularly concerned about developing offensive cyber capabilities, fearing they could lead to the militarisation of cyberspace. Its 2015 Defence White Paper noted that 'scientific and technological development' will make future wars more likely to be defined by 'information superiority', 'cyber-attacks', and the misuse of technologies such as 'genetic engineering, biotechnology, and nanotechnology'.[89] Indonesia is particularly concerned about threats targeted at critical infrastructure, such as health and information facilities.[90]

Foreign policy and international cooperation

Because of Indonesia's leading role in the Non-Aligned Movement and its embeddedness in ASEAN political culture, public attributions of ICT incidents to other states are unlikely.[91] The government hasn't politically attributed a cyber-enabled attack to a state actor. The ITE Law includes provisions on extraterritorial jurisdiction but doesn't address attribution issues or state-to-state activities. Rather, the focus is on encouraging more capacity-building to help less cyber-mature countries address cyber challenges.

In pursuing those goals, Indonesia has supported regional cooperation at the ASEAN level, especially in increasing human resource capacity to minimise the capability gap among ASEAN member states.[92] Indonesia has bilateral memorandums of understanding on cyber cooperation with China, the UK, Australia, South Korea, the EU, the US and Russia.[93] Those agreements, which involve the BSSN, cover multiple areas of cooperation, including CCB, establishing points of contact for incident handling, cooperation on cybercrime/cyberterrorism, and spreading radical online content. International cooperation and CCB are perceived as pathways to support Indonesia's relatively weak capacity in responding to challenges in cyberspace.[94]

Indonesia actively advocates for CCB and encourages collaboration with various domestic and international stakeholders.[95] Furthermore, Indonesia has also advocated information-sharing between states through institutionalised dialogues at the multilateral, regional and bilateral levels.[96]

A core issue for Indonesia is combating terrorist organisations' use of digital technology. Faced with challenges such as the spread of Islamic fundamentalism and hate crimes online, government documents highlight the threat of cyberspace being hijacked to 'spread hatred and racial ideology'.[97] Demonstrating its commitment to combating cyber terrorism, Indonesia signed up for the 2019 Christchurch Call initiative, which encouraged governments and online service providers to make voluntary commitments aimed at stopping terrorist and other violent content.

Beyond the threat of terrorism, Indonesia is concerned about the use of cyberspace as an avenue for 'disrupt[ing] public order'—a broad term that human rights activists have pointed out could be easily misused.[98] In particular, the ITE Law is frequently weaponised by both authorities and members of the public; reports of defamation, religious blasphemy and disrupting social order frequently dominate cases of cybercrime.[99]

Japan

Wilhelm Vosse

Overview

Japan's 2021 Cybersecurity Strategy highlights the importance of the rule of law in cyberspace, prioritising norms of responsible state behaviour. The strategy outlines measures to deter irresponsible cyber activities through coordination with allies and comprehensive responses across political, economic, technological, legal and diplomatic spheres. Japan also emphasises confidence-building measures between states to prevent instability in cyberspace.

A significant part of Japan's cyber strategy includes capacity-building initiatives in the Indo-Pacific, promoting responsible behaviour through public–private collaboration and international cooperation. Japan stresses the importance of multistakeholder engagement in establishing global norms in cyberspace.

Japan maintains strict constitutional norms, such as the secrecy of communications, and engages in extensive public–private consultations regarding cyberspace and regulating dual-use technologies. Those legal norms, rooted in its postwar history, are an important tool of its soft power.

The government plays a central role in protecting critical infrastructure, investigating cyber incidents and regulating the export of dual-use technologies. Japan's commitment to international law and norms is reflected in its active participation in shaping global cyber norms through forums such as the UN GGE and OEWG. Japan's focus on strengthening cybersecurity capabilities, enhancing international cooperation and fostering an open cyberspace reflects its ambition to be a model for responsible cyber behaviour.

National dimensions

Institutions and accountability

Japan seeks a free, fair and secure cyberspace to support economic development and a stable international order. Responsible behaviour in cyberspace involves protecting critical infrastructure, promoting public–private partnerships and fostering international cooperation.[100] The government supports UN norms to promote stability and security. Japan also emphasises cooperation in cybercrime prevention and CCB.[101]

Japan expects public and private entities to implement robust cybersecurity measures to protect ICT infrastructure from malicious actors. Private companies work with government agencies like the National Center of Incident Readiness and Strategy for Cybersecurity, the Ministry of Economy, Trade and Industry (METI), and the Ministry of Internal Affairs and Communications in multistakeholder forums. That collaboration improves practical measures to counter cyber risks. The government aims to set an example by adhering to responsible behaviour norms and encouraging other nations to adopt similar practices.[102]

METI plays a key role in regulating technology that could be used for cyberattacks and collaborates with private companies on IT infrastructure security, training and data protection. It's also one of the core government institutions that cooperates with private companies in strengthening the security of their IT infrastructure, training qualified personnel, building capacity and raising awareness about the required handling of data and protecting privacy.

Japan's Public Security Intelligence Agency (PSIA) publishes annual reports on cyberattacks and attribution. When cyberattacks involve foreign governments or actors, the PSIA coordinates with the Ministry of Foreign Affairs and the Ministry of Defence.[103] Japan uses joint public attribution with partner countries to strengthen responsible behaviour in cyberspace. Those statements, published by the Foreign Ministry, are intended to serve as a disincentive for state actors to use cyberspace maliciously. Japan has recently become more active in joint public attributions, although it remains cautious, particularly with China and Russia. For example, Japan supported the US attribution of the 2017 WannaCry attack to North Korea but remains hesitant to attribute attacks involving China. Japan attributed only six in a 2023 comparative analysis of 164 official public political attribution cases.[104]

Operational dimensions

Responsible use and acquisition of technologies

Once a major electronic equipment exporter, Japan has seen that role diminish, but a select group of Japanese IT and chip manufacturers remain competitive in global markets. Japan's military and dual-use technology exports began in 2015, guided by non-proliferation treaties, including the International Atomic Energy Agency Safeguards and the Wassenaar Arrangement for conventional weapons.[105] It also participates in export-control frameworks to regulate technologies with potential cybersurveillance applications. In December 2021, Japan began considering stricter domestic measures to regulate the sale of cybersurveillance technologies to countries that violate human rights, in response to the Biden administration's announcement of a multilateral framework to regulate exports of surveillance technology.[106]

To limit the export of technologies that can be used for cyber-enabled attacks, Japanese export regulations cover a range of telecommunication equipment, including fibre-optic cables and wireless communication wiretapping devices.[107] Japan's principle guiding weapons and military-technology exports limits them to friendly countries. Every six months, it updates its End User List, which 'provides exporters with referential information on foreign entities for which concern cannot be eliminated regarding involvement in activities such as the development of WMDs or other items'.[108]

The government has also taken action to manage the expanded role of dual-use technologies. In December 2022, it issued its revised National Security Strategy, National Defence Strategy and Defence Buildup Program. In the section on 'Capabilities in the cyber domain', the Defence Buildup Program sets out to enhance the cybersecurity capabilities of Japan's Ministry of Defense and Japan's Self-Defense Forces.[109] It will work more closely with critical infrastructure providers and the defence industry.

In recent years, Japan has fallen behind in IT and cybersecurity. It's placed 32nd out of 64 countries ranked in the 2023 International Institute for Management Development's World Digital Competitiveness rankings—an index measuring how states adopt digital technologies.[110] This is a drop from its 29th place in 2022 and its peak of 22nd in 2018. In the light of this and in an effort to bolster cybersecurity, the government is working to establish secure command-and-control capabilities in high-priority equipment systems based on a 'zero trust' concept.[111] Japan's Risk Management Framework, introduced in 2023 by the Ministry of Defense and the Self-Defense Forces, emphasises continuous risk assessment for IT systems and cutting-edge technology.[112] Since 2015, METI has issued Cybersecurity Management Guidelines for private companies. The guidelines require companies to recognise and report cybersecurity risks and implement organisational cybersecurity measures.[113]

In July 2022, the US–Japan Economic Policy Consultative Committee published its Plan of Action to strengthen the rules-based economic order, among other things, by better securing critical and emerging technologies and strengthening supply-chain resilience. Central to the responsible use of cyberspace were efforts to impose export controls and cybersurveillance systems to counter their misuse by malicious actors.[114]

Japan's 2022 Cybersecurity Strategy included plans to extend its active cyber-defence capabilities, improve cyber situational awareness and human capital, and coordinate across ministries to respond to cyber threats.[115] However, it isn't very detailed regarding what technologies Japanese Government institutions intend to acquire to respond to hacking, surveillance or other invasive technologies.

In March 2024, Japan supported a White House statement to deepen cooperation to counter the proliferation and misuse of spyware.[116] Soon after, METI published an interim report on its policy for revising the export-control system, which included stronger advance reporting requirements for overseas dual-use technology transfers.

Responsible cyber operations

Operationally, responsible cyber behaviour involves proper authorisation for conducting cyber operations. In Japan, the core institutions that collect cyber intelligence are the Cabinet Intelligence and Research Office and the PSIA, which cooperate with the Ministry of Foreign Affairs, the Ministry of Defense and the National Police Agency.[117] Each body advises the Cabinet Intelligence Committee and the National Security Council. The PSIA contributes to cyber-intelligence countermeasures, collecting and analysing HUMINT information. Japan has also taken other steps to enhance its operational capacity, such as joining NATO's Cooperative Cyber Defence Centre of Excellence.[118]

Despite that, Japan has yet to emerge as a leader in government or military cyber operations, both defensive and offensive. Although Japan's 2018 and 2021 cybersecurity strategies mention 'active cyber defence' (ACD), they lack detail. The 2022 National Security Strategy provides more specificity, calling for the 'penetrat[ion] and neutralis[ation] of the servers of potential attackers'.[119] However, beyond that, no concrete decisions on ACD activities have been finalised.

To strengthen the responsible use of cyberspace, Japan aims to be a model for other countries by ensuring that certain principles, such as data privacy or the secrecy of private communications, are still observed. The most important legal instruments in this regard are article 21 of the Japanese Constitution and article 4 of the Telecommunication Business Act, which guarantee the privacy of communications.

Reconciling the twin imperatives of maintaining the highest standards of privacy and establishing an effective cyber defence hasn't been easy. As of November 2024, the Japanese Diet was still debating whether the ACD mentioned in the 2022 National Security Strategy is constitutional.[120] Some politicians and commentators have argued that Japan's official adoption of ACD would be considered irresponsible.[121] While other countries in the same situation would be more likely to argue that national-security considerations trump domestic laws, Japan's calculus is somewhat different.

International dimensions

International law and cyber norms

Japan accepts the UN's eleven norms of responsible state behaviour as guiding principles of state actions in cyberspace. It's also committed to confidence-building measures to increase transparency, predictability and mutual understanding in cyberspace.[122]

In May 2021, Japan issued its Basic Position of the Government of Japan on International Law Applicable to Cyber Operations, clarifying how international law applies to cyberspace, identifying violations and outlining tools for states affected by cyber operations.[123] Japan also promotes the Data Free Flow with Trust principles under the Comprehensive and Progressive Agreement for Trans-Pacific Partnership and the Japan–US Digital Trade Agreement, advocating for the free flow of information, the rule of law, internet openness, autonomy from malicious control, and multistakeholder governance.[124]

Above all, Japan asserts that states must not violate another state's sovereignty or intervene in domestic matters. Cyber operations causing physical damage or compromising functionality, especially against critical infrastructure, may constitute violations of sovereignty.[125] Japan supports the Responsibility of States for Internationally Wrongful Acts principle, emphasising the need to attribute cyberattacks, hold states accountable, prevent recurrence and allow countermeasures against enabling states.[126] Japan advocates for peaceful dispute resolution and opposes using force unless cyber operations constitute an armed attack under article 51 of the UN Charter.[127]

Foreign policy and international cooperation

Japan is active in cyber diplomacy through bilateral, regional and global exchanges and cyber-focused dialogues. Its bilateral dialogues with partners such as the US, the UK and the EU focus on collaborations on regional and global cyber governance. Japan also regularly conducts exchanges and confidence-building measures with India and ASEAN member states.

Japan has had a few notable successes. Globally, it spearheaded the adoption of the Ise-Shima G7 Principles and Actions on Cyber for responsible behaviour in cyberspace.[128] Those principles call for closer cooperation between governments, businesses and non-state actors to uphold rules and laws in cyberspace. Regionally, Japan has led the ASEAN–Japan Cybersecurity Capacity Building Centre, a Japanese partnership with Thailand's Electronic Transactions Development Agency, which opened in Bangkok in 2018. The centre has trained hundreds of civil servants from ASEAN member states to make government IT systems more resilient against cyberattacks.[129]

Japan also supports CCB initiatives through the Japan International Cooperation Agency and partnerships with European counterparts, combining cybersecurity training with broader economic and social development efforts. Addressing cybercrime and intellectual property theft is central to Japan's agenda, and it argues that trust in the security of IT systems, data privacy and government oversight are crucial for fostering economic growth and innovation.[130] To strengthen domestic political support for those cyber norms, Japan often argues that public trust in the security of information held on IT platforms, data privacy and government oversight of the integrity of IT systems is a core condition for reliance on ICT systems and greater future investment in them.[131]

Pakistan

Rabia Akhtar

Overview

Pakistan's approach to responsible cyber behaviour combines efforts to create a resilient digital environment at home with a strong stance on global cyber governance. However, Pakistan faces credibility issues. While it promotes responsible behaviour globally, its domestic actions, including using advanced surveillance tools, have raised privacy concerns and accusations of government overreach. That inconsistency creates a gap between Pakistan's international advocacy and its internal practices.

Pakistan seeks to establish itself as a responsible cyber actor by focusing on domestic security and advocating for the peaceful use of cyberspace. Domestically, the government has taken steps to build a secure and inclusive cyber environment, most notably through the National Cyber Security Policy of 2021.[132] The policy aims to protect critical infrastructure, secure digital assets and safeguard daily activities such as banking and health care. However, despite the policy's potential benefits, its implementation is hampered by limited resources and institutional capacity.

Internationally, Pakistan views the internet as a shared global resource, similar to the oceans or outer space. It actively supports the global framework for responsible state behaviour in cyberspace. It has advocated for a legally binding instrument to regulate cyber actions, including a ban on offensive cyberweapons, reflecting concerns about cyberspace becoming a domain of conflict.

National dimensions

Institutions and accountability mechanisms

For Pakistan, being a responsible state actor in cyberspace means securing its digital landscape and promoting peaceful internet use globally. It supports the UN-led global framework on responsible state behaviour in cyberspace and advocates for global cooperation to combat cyber threats and share intelligence and best practices. Pakistan recognises collaboration as crucial for building resilience against cyberattacks, especially given its limited cyber capabilities. Pakistan further emphasises equitable internet access, viewing it as a global common. Politically, protecting national sovereignty and critical infrastructure from cyber threats drives the agenda towards robust cybersecurity measures.

Domestically, the government encourages companies and individuals to meet basic cybersecurity standards. The National Cyber Security Policy 2021 mandates appointing chief information security officers and complying with national security standards. The government also encourages incident reporting to the National Cyber Emergency Response Team and prioritises digital literacy to promote safe online practices.

While progress is underway, Pakistan faces challenges in applying national cybersecurity standards and lacks accredited experts, leaving systems vulnerable to attacks. However, after cyber incidents targeting its ICT infrastructure, Pakistan's Economic Coordination Committee approved a US$36 million investment to enhance technical capabilities in 2024. That followed the launch of the 2021 cybersecurity policy, which identified 11 cybersecurity risks and challenges, including phishing campaigns and for-hire hacker services.[133] The policy was the culmination of a series of government discussions and initiatives that were initially triggered by the 2013 Snowden revelations, which exposed the UK's surveillance of Pakistan.[134]

Pakistan's cybersecurity policy explicitly states that cyberattacks on Pakistan's critical infrastructure or critical information infrastructure are acts of aggression against national sovereignty.[135] The policy reinforces the notion that other states are expected to behave responsibly. The policy also mandates that organisations in critical sectors adhere to national cybersecurity standards and appoint qualified cybersecurity professionals. The CERT Rules of 2023 further promote incident reporting, while the Cyber Patriot Program incentivises public involvement in identifying vulnerabilities.

The policy further emphasises international cooperation to protect Pakistani citizens from cyberattacks. Pakistan recognises that cyber threats can emerge from poorly protected systems outside its borders. The policy emphasises cooperation with international law-enforcement and cybersecurity organisations, sharing threat information, coordinating responses and taking proactive measures to protect its digital systems and citizens' data from external threats.

Operational dimensions

Responsible use and acquisition of technologies

Due to acute internal security concerns, the Pakistan Government and some private entities have obtained various advanced surveillance tools. For example, since 2012, the Federal Investigation Agency has used advanced phone-hacking tools from Cellebrite, an Israeli digital intelligence company, acquired through a third party in Singapore.[136] Meanwhile, in 2015, several Pakistani contractors with alleged ties to state institutions attempted to procure a software suite from the Italian firm Hacking Team, which would allow for discreet monitoring of computers and mobile devices.[137] There are no specific rules or transparency requirements for procuring and selling those technologies, raising concerns about the legitimacy of their use.

Despite those technological procurements, Pakistan still lacks comprehensive cybersecurity standards. The government has struggled to properly implement legislation and regulations on data security, supply-chain security, vulnerability management and data-breach reporting. That oversight leaves the country vulnerable to cyber threats and fails to allay ethical concerns regarding the use of surveillance technologies.

Indeed, a closer look at Pakistan's practices reveals a troubling pattern of irresponsibly using technology to monitor its own citizens. The lack of transparency and control over those powerful tools has led to overreach and potential violations of privacy. For instance, Human Rights Watch reports that non-government organisations in Pakistan have faced intimidation, harassment and surveillance by government authorities, highlighting a misuse of surveillance technologies.[138] Digital authoritarianism is also on the rise in Pakistan: one study has revealed that the government uses advanced surveillance technology and strict digital laws to monitor and control online activities.[139] That control includes internet shutdowns, censorship and the targeting of dissidents. State agencies often collaborate with technology companies to enforce those measures under the guise of protecting national security and public order. However, activists and civil-society groups do push back against those restrictions. Despite harassment and legal challenges, they continue to advocate publicly for protecting internet freedom in Pakistan.

Responsible cyber operations

The National Response Center for Cyber Crimes, a law enforcement agency under the Federal Investigation Agency, specialises in addressing cybercrime.[140] Beyond that, understanding the operations of Pakistan's national security, defence and intelligence agencies' cyber units is challenging due to a lack of publicly accessible data. Pakistan doesn't publicly disclose its offensive cyber capabilities, but the country does advocate for a prohibition on developing offensive cyberweapons.[141] However, the Cyber Operations Tracker by the Council on Foreign Relations has recorded at least 13 reported cyber operations allegedly sponsored by Pakistan since 2020.[142] Accusations have been made regarding the alleged involvement of Pakistan's Inter-Services Intelligence, the country's principal intelligence agency, in supervising or supporting various hacking groups.[143]

International dimensions

International law and cyber norms

Pakistan believes that established principles of non-use of force, sovereign equality, peaceful dispute resolution and non-interventionism apply to cyberspace.[144] Officials have highlighted the grave risk of a 'cyber arms race' and the potential unintended consequences of developing and using such technologies. In the light of this, Pakistan has called for an 'outright ban on the development of offensive cyber weapons', which could cause widespread disruption to critical infrastructure and have wider political ramifications.[145] The country has also called for an inclusive and transparent dialogue to address the issue of cyber arms control and to establish norms and rules of behaviour in cyberspace.

Acknowledging definitional challenges in the international law, Pakistan has stressed the need to more concretely define key terms such as 'cyber attack' and 'cyber terrorism'.[146] It supports legally binding instruments to regulate state behaviour and promote the responsible use of digital technologies.[147] It also supports international cooperation as necessary to develop an effective framework to promote responsible state behaviour in cyberspace.

Pakistan faces credibility issues in its stance on cyber norms. Domestically, it's been criticised for using surveillance technologies to monitor its citizens under the guise of national security. Internationally, it promotes responsible behaviour in cyberspace, creating a contradiction between its actions at home and abroad. To resolve that, Pakistan must align its domestic practices with its international commitments, enhancing trust and reputation at home and abroad.

Foreign policy and international cooperation

Pakistan's foreign policy approach regarding cybersecurity seeks to ensure its continued influence in shaping global and regional initiatives. To that end, Pakistan engages internationally in various cyber-related forums, including UN OEWG, the International Telecommunication Union and the Internet Corporation for Assigned Names and Numbers. That approach also emphasises the need for trusted information exchange about cyber threats with public, intergovernmental and non-governmental bodies, including liaison and coordination with national and international cybercrime agencies.

Outside of its advocacy against the proliferation of 'offensive cyber weapons', the Pakistan Government has also advocated bridging the digital divide between developed and developing countries. Pakistan believes that the internet is a precious 'common heritage of mankind', as are other global commons such as space and oceans—a reference explicitly outlined in its position on the applicability of international law in cyberspace.[148] At its core, Pakistan envisions a world in which the benefits and opportunities of the internet are accessible to all, ensuring equitable distribution for the progress of humanity. That vision has informed its preference to see international cooperation for capacity building.

Taiwan

Yisuo Tzeng and Louise Marie Hurel

Overview

Taiwan doesn't explicitly use the term 'responsible cyber behaviour'. However, its perception of state responsibility is tightly interlinked with having the capacity to build economic and security resilience in the face of tensions with China. For Taiwan, the concept of responsible cyber behaviour encompasses three core (if implicit) elements:

- responsibility as the willingness to refrain from interfering in the domestic affairs of other states
- responsibility as the domestic capacity to respond to and protect against such interference
- responsibility as the commitment to maintaining a free and open internet.

Those views of responsibility take shape in the unique context of cross-strait relations. The oscillating temperature of those relations has often meant that Taiwan must balance its approach in reactive and preventive ways across all three dimensions of responsible cyber behaviour: international, domestic and operational.

Taiwan has continually ramped up its domestic cybersecurity institutions, especially since 2016, when Tsai Ing-wen assumed the presidency. Legislative efforts have also sought to establish clearer roles and responsibilities domestically for baseline cyber and data security measures. Political leadership and oversight on the use of cyber capabilities and ICTs by the military mean that their use is largely restricted to defensive purposes. Despite its non-recognition at the UN and absence in different multilateral forums, Taiwan does adhere to the norms of responsible state behaviour in cyberspace.

National dimensions

Institutions and accountability

Taiwan's view of responsible cyber behaviour is substantively informed by national security considerations, primarily due to ongoing cyber-enabled threats from the People's Republic of China.[149] Taiwan's government has upheld the cardinal principle that 'cyber security is national security' since the publication of the 2017 National Cyber Security Program of Taiwan.[150] That document outlined primarily what the government needs to do to improve cybersecurity to forestall foreign adversarial malign infiltration/influence. For instance, Taiwan deems it vital to protect critical information infrastructure from sabotage by hackers sponsored by the Chinese Government.

In response to the mounting cyberattacks and influence operations from China, Taiwan's 2018 Cyber Security Management Act established standards for the public and private sectors, requiring chief information security officers, cybersecurity training and incident-response mechanisms. Noncompliance leads to penalties, reflecting Taiwan's strong stance on cybersecurity accountability.[151] The Act establishes baseline standards for public- and private-sector accountability in cybersecurity. It designates the Executive Yuan as the competent authority stipulating 'cyber security responsibility levels' for government and 'specific non-government agencies' (critical infrastructure providers, government-owned enterprises and government-endowed foundations).[152] The Act also supports establishing a particular domestic understanding of responsibility through 'negative measures'. The Act designates penalties for specific non-governmental agencies that fail to comply with the regulation (that is, develop, amend or implement a cybersecurity maintenance plan, submit a report on implementation and improvement of a plan, establish an incident-response mechanism and/or report a cybersecurity incident).[153]

Beyond national-security concerns, Taiwan's attitude to responsible cyber behaviour is also informed by public apprehensions over privacy—which, given concerns about espionage and insider threats, can be a fine balance. Taiwan maintains laws and regulations that monitor property rights infringements, child abuse, hate speech and disinformation. The legislation on personal data protection goes way back to the Personal Data Protection Act of 2015, which stipulates only the responsibility to protect personal data collected by necessary, appropriate means. That said, organisations responsible for personal data leaks bear the responsibility to cover the tangible and intangible losses and, in certain cases, can even face criminal prosecutions.[154]

Disinformation campaigns, often linked to Chinese influence operations, are treated as national-security threats in Taiwan.[155] Espionage, cognitive warfare and subversion have become regular tactics used by China to destabilise Taiwan, influence public opinion and disrupt Taiwan's relations with key allies such as the US. Taiwan's legal amendments target disinformation for undermining social order and national security and demonstrate its approach to responsible cyber behaviour by criminalising harmful activities.[156]

The proposed expansion of Taiwan's domestic intelligence apparatus sparked opposition concerns over political surveillance and fears of excessive government surveillance.[157] In response, the government adopted a 'patch management' approach, amending existing laws rather than drafting a new overarching cybersecurity act. Amendments to laws such as the Criminal Code and the National Security Act target those spreading disinformation or harming social order and national security. By criminalising harmful conduct and unauthorised data access, Taiwan primarily addresses individual and organisational actions rather than broader geopolitical issues.

Operational dimensions

Responsible use and acquisition of technologies

Due to its broader diplomatic isolation, Taiwan remains excluded from most multilateral organisations. However, it still adheres to many international norms and resolutions approved by the UN and multistakeholder agreements. In the cyber domain, Taiwan's Ministry of Economic Affairs and the newly established Ministry of Digital Affairs promote the growth of its cybersecurity industry while upholding non-invasive, democratic, rules-based frameworks such as the Wassenaar Arrangement. For example, acquisitions or exports of cyber-related technologies must be checked against the Wassenaar control list of cyber-intrusive tools.[158] Following Russia's invasion of Ukraine, Taiwan followed the US's path by imposing export controls on chips, cybersecurity software and servers destined for Russia.[159]

Taiwan also closely follows the US Bureau of Industry and Security regulatory list to align with the US's decoupling and de-risking from China. Taiwanese Government agencies, including the ministries of Justice and National Defense, call for the cybersecurity industry to avoid buying or selling banned Chinese surveillance technologies.[160]

While Taiwan lacks specific regulations for supply-chain cybersecurity, its public and private sectors closely follow the US Department of Defense's Cybersecurity Maturity Model Certification (CMMC) to safeguard the flow of controlled unclassified information. Taiwan's Ministry of Digital Affairs, not the Ministry of National Defence, oversees efforts to implement CMMC certification, given historical sensitivities regarding military involvement in business affairs.[161]

While Taiwan's armed forces depend on the supply of US weapons, Taiwan has also cultivated a defence industrial base mostly composed of small to medium-sized enterprises, including some cybersecurity capabilities.[162] To encourage defence industrial base enterprises to further invest in improved cybersecurity, many seek to achieve CMMC certification and join the US defence industrial base supply chain.

Responsible cyber operations

Several government agencies, each with specific cyber operations capabilities, handle cyber threats. The Cyber Command (Information, Communications and Electronic Force Command), established in 2017, leads those efforts.[163] Before its formation, Taiwan's intelligence apparatus had already developed cyber operations units. The National Security Bureau leads the intelligence community with two cyber operations units and one for countering disinformation. The Military Intelligence Agency of the Ministry of Defense focuses on cyber espionage, while the Psychological Operations Platoon of the Political Warfare Department oversees influence campaigns and counters malign influence.[164]

At its inauguration, then President Tsai Ing-wen emphasised the Cyber Command's defensive nature, noting that its primary mission is to protect military ICT infrastructure and national critical information systems.[165] However, Taiwan's defence posture is evolving.[166] The latest defence reports show a shift towards 'defending forward'—a concept modelled after US and UK active cyber defence strategies. The 2023 *Annual defense report* acknowledged that cyber and electronic warfare tactics have become essential for modern battlefields.[167]

Taiwan faces significant challenges in recruiting and retaining cybersecurity talent, which hinders the growth of its military cyber capabilities. Efforts to collaborate with 'white-hat' hackers remain contentious due to trust and reliability concerns.

On the counterintelligence and criminal investigation front, the Investigative Bureau of the Ministry of Justice and the National Policy Agency of the Ministry of Interior have long been experienced in digital crime investigations. Law enforcement requires a warrant for any cyber-intrusive actions, and intelligence operations must follow clear orders and rules of engagement, ensuring legality and oversight in Taiwan's cybersecurity efforts.

International dimensions

International law and cyber norms

Despite challenges, the Taiwanese Government remains committed to the application of international law in cyberspace, although it hasn't elaborated on how it applies. In particular, questions remain about how international law, specifically international humanitarian law, would apply in an armed conflict between Taiwan and China, given the contested views regarding Taiwan's status.[168]

Foreign policy and international cooperation

With Taiwan largely isolated from the institutions of global governance, the country has instead sought participation in alternative multistakeholder and technical forums. Those include the Asia Pacific Regional Internet Governance Forum (held in Taipei in 2024), the Internet Corporation for Assigned Names and Numbers and the Forum on Incident Response Teams. The Taiwan Internet Governance Forum has become iconic for connecting Taiwan to the global discourse on cyber governance.

Moreover, such experiences also speak to the core principles of Taiwan's approach to cyber diplomacy: the commitment to a free, open internet—which equally underpins international initiatives such as the UN Global Digital Compact and the Freedom Online Coalition. Demonstrating Taiwan's commitment to that principle—and rejecting those that don't commit—Taiwanese MP Audrey Tang (now Digital Affairs Minister) delivered a tele-speech at the UN Internet Governance Forum in 2017 to break through China's attempts to block Taiwan's participation in international forums.[169]

International cooperation can be framed in different ways. In 2023, lawmakers in the US introduced the Taiwan Cybersecurity Resiliency Act, 'which would require the US Department of Defense to expand cybersecurity cooperation with Taiwan to help it counter cyber threats from China'.[170] Other types of cooperation have included joint cyber exercises. That was the case, for example, for a Taiwan–US cybersecurity offensive and defensive exercise led by the Department of Cyber Security of the Executive Yuan.[171]

Notes

[1] For a more detailed understanding of the UN Group of Government Experts (GGE) and OEWG time lines, see Dennis Broeders, Francois Delerue, Arun Sukumar, *Responsible behaviour in cyberspace: global narratives and practice*, Publications Office of the European Union, Luxembourg, 2023.

[2] 'Background to UN discussions on responsible state behaviour', UN Institute for Disarmament Research, online.

[3] For examples, see Department of Home Affairs, *2023–2030 Australian Cyber Security Strategy*, Australian Government, 2023, online; 'EU statement—UN Open-Ended Working Group on ICT: rules, norms and principles of responsible behaviour of states', Delegation of the EU to the UN in New York, 30 March 2022, online; National Cyber Force, 'Responsible cyber power in practice', UK Government, 4 April 2023, online; State Department, 'United States International Cyberspace & Digital Policy Strategy', US Government, 6 May 2024, online.

[4] See, for instance, Louise Marie Hurel et al., 'Cyber capabilities in the Indo-Pacific: shared ambitions, different means?', *RUSI Commentary*, 3 May 2024, online.

[5] See, for instance, Gatra Priyandita, 'Now that ASEAN has its cyber norms checklist, the hard work begins', *The Strategist*, 25 October 2024, online.

[6] We thank Siriwat Chhem for his contributions to the making of this piece.

[7] Sui-lee Wee, 'They're forced to run online scams. Their captors are untouchable', *New York Times*, 28 August 2023, online.

[8] 'New APT32 malware campaign targets Cambodian Government', *The Record*, November 2020, online; 'Cambodian government subjected to Chinese APT attacks', *SC Magazine*, 9 November 2023, online.

[9] Ministry of Defence, *National Defence Policy 2022*, Cambodian Government, 2022, online.

[10] Telecommunication Regulator of Cambodia, *Cambodia ICT Masterplan 2020*, Cambodian Government, 2020, online.

[11] See, for instance, see Aun Chhengpor, 'Surveillance Tools, DNA screening equipment part of Cambodia's new security deal with China', *Voice of America*, 6 October 2021, online.

[12] Permanent Mission to the UN, 'Statement on behalf of the Association of Southeast Asian Nations', Kingdom of Cambodia, 30 March 2022, online.

[13] 'Statement by His Excellency Mr Sovann Ke, First Substantive Session of the Open-Ended Working Group on security of and in the use of information and communications technologies 2021–2025', Permanent Mission of Cambodia to the UN, 13–17 December 2021, online.

[14] 'Statement by His Excellency Mr Sovann Ke, First Substantive Session of the Open-Ended Working Group on security of and in the use of information and communications technologies 2021–2025'.

[15] Discussion with Cambodian officials.

[16] Kingdom of Cambodia, 'Submission by the Kingdom of Cambodia to the United Nations Office for Disarmament Affairs', *Reaching Critical Will*, 30 November 2023, online.

[17] ASEAN Secretariat, 'Governing cybersecurity: policies, practices and processes', 2023, online.

[18] Japan International Cooperation Agency, 'Signing of record of discussion on technical cooperation project with Cambodia: Project for Improvement of Cyber Resilience', Japanese Government, 5 December 2022, online.

[19] Meri Radinibaravi, 'Digital connectivity: Government aims to improve access for all', *Fiji Times*, 15 February 2024, online.

[20] Semi Turaga, 'More than 30 govt websites accessible after cyber incident—AG', *Fiji Village*, 17 April 2021, online.

[21] Pacific Islands Forum, 'Boe Declaration on Regional Security', 2018, online. For Fiji's view on ICT infrastructure vulnerability, see Tupou'tuah Baravilala, 'Republic of Fiji statement on the applicability of international law', OEWG on Security of and in the Use of ICT 2021–2025, 30 March 2022, online.

[22] See, for instance, Pacific Islands Forum, 'Open-Ended Working Group on security of and in the use of information and communications technologies 2021–2025—Third Substantive Session', Pacific Islands Forum with UN missions, July 2022, online. See also speech by Manoa Kamikamica, 'Launch event of the GFCE Pacific Hub', Ministry of Trade, Co-operatives, Small and Medium Enterprises, Fijian Government, 3 October 2023, online.

[23] Pacific Islands Forum, 'Boe Declaration on Regional Security'.

[24] Tupou'tuah Baravilala, 'Republic of Fiji statement on the applicability of international law'.

[25] 'Cybercrime Act 2021', Parliament of Fiji, 2021, online.

[26] 'Online Safety Act 2018', *The Laws of Fiji*, 2018, online.

[27] Shania Shayal Prasad, 'Cyber threats a concern for individuals and critical infrastructure', *FBC News*, 21 August 2023, online.

[28] Kelvin Anthony, 'Fiji to craft new national security strategy for "a more secure and vibrant future"', *RNZ*, 14 December 2023, online.

[29] 'Release: Fiji, the United Kingdom and OCSC unite to conduct Fiji's second national cybersecurity maturity assessment', Oceania Cyber Security Centre, 26 February 2024, online.

[30] 'Cybercrime Act 2021'.

[31] This policy is applicable to commercial banks, credit institutions, insurance companies, insurance brokers, securities exchange, management companies of managed investment schemes, stockbrokers, the Fiji National Provident Fund, the Fiji Development Bank, and restricted foreign exchange dealers. See 'Prudential Supervision Policy Statement no. 2', Reserve Bank of Fiji, 3 March 2023, online.

[32] 'Submarine cable map', *TeleGeography*, online.

[33] Arnold Chanel, 'Starlink's impact in Fiji', *The Fiji Times*, 26 May 2024, online.

[34] Vijay Narayan, 'Starlink now live across Fiji', *Fiji Village*, 20 May 2024, online.

[35] Tupou'tuah Baravilala, 'Republic of Fiji statement on the applicability of international law', OEWG on Security of and in the use of ICT 2021–2025.

[36] 'Implementing cyber confidence measures globally—towards the UN Point of Contact Directory', working paper submitted on 25 November 2022 by Australia, Brazil, Canada, Chile, Fiji, Germany, Israel, the Republic of Korea, Mexico, the Netherlands, Singapore and Uruguay, UN Office of Disarmament Affairs, 2022, online.

[37] Foreign, Commonwealth and Development Office, 'Partners in the Blue Pacific (PBP): joint statement, September 2022', UK Government, 23 September 2022, online.

[38] 'Pacific nations unite to address cybersecurity challenges', GFCE, August 2023, online.

[39] Ministry of Foreign Affairs, 'Fiji and Australia sign MoUs for ports and infrastructure services and cybersecurity cooperation', Fijian Government, 30 April 2024, online.

[40] 'Welcome to PaCSON', Pacific Cyber Security Operational Network, online.

[41] 'Fiji and Vanuatu invited to join the Budapest Convention on Cybercrime', Council of Europe, 8 December 2021, online.

42 'GLACY+: Fiji becomes the 18th priority country of GLACY+ project: initial assessment of criminal justice capacities on cybercrime and e-evidence concluded', Council of Europe, 28–29 June 2022, online.

43 Shivani Shinde, 'India has over 800 mn internet users; most use tech for OTT services: study', *Business Standard*, 27 February 2024, online.

44 Ministry of Electronics and Information Technology (MEIT), *CERT-In annual report 2022*, Indian Government, 2022, online.

45 MEIT, 'National Cybersecurity Policy', Indian Government, 2013, online.

46 Indian Computer Emergency Response Team (CERT-In), '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', Indian Government, 28 April 2022, online.

47 Saikat Datta, *The NCIIPC and its evolving framework*, Observer Research Foundation, 3 November 2016, online.

48 MEIT, 'The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021'. Indian Government, 25 February 2021, online.

49 This is a term used in the 'Framework & Guidelines for Use of Social Media for Government Organisations' issued in April 2012 and seems appropriate to use in the context of government regulations on private-sector compliance. See MEIT, 'Framework & Guidelines for Use of Social Media for Government Organisations', Indian Government, April 2012, online.

50 'The Telecommunications Act, 2023', *E-Gazette—Government of India*, 24 December 2023, online.

51 MEIT, 'India AI 2023', Indian Government, 2023, online.

52 'Cyber warfare', *Government of India—Press Information Bureau,* 3 December 2021, online.

53 PC Katoch, 'Defence Cyber Command', *SP's Naval Forces*, 6 July 2021, online.

54 Arindrajit Basu, *India's international cyber operations: tracing national doctrine and capabilities*, UN Institute for Disarmament Research, December 2022, online.

55 'Cyber warfare'.

56 Cherian Samuel, Munish Sharma, *India's strategic options in a changing cyberspace*, Pentagon Press LLP, New Delhi, 2019.

57 'The Information Technology Act, 2008', online.

58 Anushka Jain, 'MHA's new programme allows volunteers to report "anti-national" online content for removal', Internet Freedom Foundation, 23 February 2021, online.

59 MEIT, 'The Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009', Indian Government, 2009, online.

60 Kamesh Shekar, Shifali Mehta, *The state of surveillance in India: national security at the cost of privacy?*, Observer Research Foundation, 17 February 2022, online.

61 It's important to note here that, despite India's emphasis on state responsibility for the extraterritorial activities of advanced persistent threat actors, India doesn't have a culture of attribution of cyber incidents to states. See Soumik Ghosh, 'Lack of cyber attribution a major challenge for India: Lt Gen Pant', *CSO Online,* 2 September 2020, online.

62 Indian Government, 'Statement on APR Rev. 1 by India', UN Office for Disarmament Affairs, 26 July 2022, online.

63 Neelam Sethi, Abhishek Thakur, 'Cyber warfare and national security challenges', reference note number 35/RN/Ref./July/2017, *Lok Sabha*, July 2017, online.

64 Sethi & Thakur, 'Cyber warfare and national security challenges'.

65 1540 Committee, 'National Points of Contact', UN, online.

66 Permanent Mission of India, New York, 'Working paper on Global Cyber Security Cooperation Portal', *Reaching Critical Will*, 25 July 2023, online.

67 MEIT, 'Lok Sabha unstarred question no. 4745', Indian Government, 24 March 2021, online.

68 Ministry of External Affairs, *Annual report 2021–2022*, Indian Government, 2022.

69 Arindrajit Basu, 'India's "passive" multistakeholder cyber diplomacy', in Ian Johnstone et al. (eds), *Building an international cybersecurity regime*, ElgarOnline, 19 September 2023, online.

70 'BSSN records decrease in cyberattacks in 2022', *Antara News,* 19 January 2023, online.

71 Critically, BSSN was established under a presidential directive rather than through the usual legislative process via parliament. As a result, it lacks the legal authority to enforce cybersecurity standards across government departments.

72 'Who are we?', *Indonesia Honeynet Project*, online.

73 'Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi', Indonesian People's Representative Council, October 2022, online.

74 ASEAN Secretariat, *ASEAN Regional Forum—Annual security outlook 2022*, Jakarta, 2022, 121.

75 ASEAN Secretariat, *ARF Annual security outlook 2021*, Jakarta, 2021, 126.

76 ASEAN Secretariat, *ARF Annual security outlook 2021*.

77 'Indonesia's response on the pre-draft report of the UN OEWG on the Developments in the Field of ICT in the Context of International Security', UN, April 2020, online.

78 'TNI bentuk Satsiber', *Ministry of Communication and Digital Affairs*, 26 August 2020, online.

79 Ministry of Defence, 'Pushansiber', Indonesian Government, online.

80 'President Jokowi orders cyber force formation: minister', *Antara News*, 23 September 2024, online.

81 See, for example, Ministry of Defense, *Pedoman Pertahanan Siber*, Indonesian Government, 2014, online.

82 'Indonesia', in *Cyber capabilities and national power: a net assessment*, International Institute for Strategic Studies, 28 June 2021, online.

83 *Pedoman Pertahanan Siber.*

84 'Lemhanas Governor proposes establishment of Cyber Force', *Antara News*, 7 August 2023, online.

85 'A web of surveillance: unravelling a murky network of spyware exports to Indonesia', research briefing, Amnesty International, 1 May 2024, online; Fikri Harish, 'Israeli-made spyware Pegasus used in Indonesia since 2018, says IndonesiaLeaks', *The Jakarta Post*, 14 June 2023, online.

86 'Regulation of the Head of the National Police no. 5 2020 on the Procedure for Police Surveillance', National Police of Indonesia, 2020, online.

87 Indonesia, 'Indonesia's response on the pre-draft report of the UN OEWG on the Developments in the Field of ICT in the Context of International Security', UN.

88 Indonesia, 'Indonesia's submission: Views on scopes, objectives and structures (elements) to the Ad-Hoc Committee to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes', UN, October 2021, online.

89 Ministry of Defence, *Buku Putih 2015*, Indonesian Government, 2015, online.

90 'Statement by HE Ambassador Dian Triansyah Djani: United Security Council Arria-formula Meeting on Cyber Attacks against Critical Infrastructure', UN, 26 August 2020, online.

91 Deepak Nair, 'Saving face in diplomacy: a political sociology of face to-face interactions in the Association of Southeast Asian Nations', *European Journal of International Relations*, 2019, 25(3):672–697.

92 Based on Indonesia's statements in its annual *ARF security outlooks*.

93 Directorate General of Legal Affairs and International Treaties, 'Treaty Room', Ministry of Foreign Affairs, Indonesian Government, online.

94 For this perspective, see Indonesia's submissions on cyber diplomacy, such as its statement on the pre-draft of the OEWG, online.

95 'Indonesia's response on the pre-draft report of the UN OEWG on Developments in the Field of ICT in the Context of International Security', UN; 'NAM working paper for the Second Substantive Session of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (OEWG)', Non-Aligned Movement.

96 See, for example, Indonesia's October 2021 statement to the Ad Hoc Committee and its bilateral cyber agreements with Australia; Australian Government, 'Memorandum of understanding between the Government of the Republic of Indonesia and the Government of Australia on cyber and emerging cyber technology cooperation', September 2021, online.

97 'Indonesia's statements at the First and Second Substantive Sessions of the OEWG', *United Nations TV*, 2020, online.

98 Katitza Rodriguez, 'Indonesia's proposed online intermediary regulation may be the most repressive yet', *EFF*, 16 February 2021, online.

99 Cindy Mutia Annur, 'Nearly 400 people charged with ITE Law in the last 9 years' [Hampir 400 Orang Dituntut dengan UU ITE dalam 9 Tahun Terakhir], *Databoks*, 18 July 2022, online.

100 National Centre of Incident Readiness and Strategy for Cybersecurity, 'Japan's Cybersecurity Strategy 2021', Japanese Government, 2021, online.

101 Specifically, the Budapest Convention on Cybercrime, 2001, and recently discussed cybercrime norms.

102 In practice, this is perhaps more likely to be the countries that are still in the process of strengthening their cybersecurity capacities as well as those that are more likely to adopt authoritarian norms and practices such as cybersurveillance and a government-controlled internet.

103 Public Security Intelligence Agency, 'Overview of threats in cyberspace 2022', Japanese Government, 2022, online.

104 In comparison, the US attributed 109, Germany 32 and Australia 17. See Christina Rupp, Alexandra Paulus, *Official public political attribution of cyber operations*, Stiftung Neue Verantwortung, Berlin, 2023, online.

105 The other three are the Nuclear Suppliers Group, the Australia Group for chemical and biological weapons, and the Missile Technology Control Regime.

106 'Jinken shingai de yushutsu kisei, rūru-ka, beiō to renkei, seifu kentō,-gao ninshō gijutsu nado taishō' [Export controls on human rights violations, rule-making, cooperation with the US and Europe: government consideration, targeting facial recognition technology, etc.], *Nikkei Shimbun*, 24 December 2021, online; see also US–Japan Economic Policy Consultative Committee, 'Joint statement of the US–Japan Economic Policy Consultative Committee', Japanese Government and US Government, 2022, online.

107 Ministry of Economy, Trade and Industry (METI), 'Security export control', Japanese Government, 2022, online.

108 METI, 'Relevant materials: End User List', Japanese Government, 2022, online.

109 Ministry of Defense, 'Defence Buildup Program', Japanese Government, 2022, online.

110 See, for instance, 'World Digital Competitiveness Ranking: 2023 results', *IMD*, 2023, online.

111 National Centre of Incident Readiness and Strategy for Cybersecurity, 'Japan's Cybersecurity Strategy 2021', Japanese Government, 2021, online.

112 Ministry of Defense, 'Defense of Japan 2023', Japanese Government, 2023, online.

113 METI, Information-technology Promotion Agency, 'Cybersecurity Management Guidelines ver. 3.0', Japanese Government, 2023, online.

114 'Joint statement of the US–Japan Economic Policy Consultative Committee'.

115 National Centre of Incident Readiness and Strategy for Cybersecurity, 'Japan's Cybersecurity Strategy 2021', Japanese Government, 2021, online.

116 'Joint statement on efforts to counter the proliferation and misuse of commercial spyware', The White House, Washington DC, 2024, online.

117 The National Police Agency is central in investigating cyberattacks and has frequently been cited in public attributions, such as Unit 61419 of the Chinese People's Liberation Army in the case of the cyberattack against the Japan Aerospace Exploration Agency.

118 Alexander Martin, 'Japan formally joins NATO cyber cooperation center', *Recorded Future News*, 4 November 2022, online.

119 Cabinet Secretariat, 'National Security Strategy of Japan', Japanese Government, 2022, online.

120 For a detailed analysis of the current state of the debate in Japan, see 'Japan cybersecurity bill delayed amid postelection uncertainty', *The Mainichi*, 3 November 2024, online. See also Wilhelm Vosse, 'Japan's gradual shift from passive to active cyber defense: evidence from the domestic discourse and international cooperation', *Études françaises de renseignement et de cyber*, 2024, online.

121 Vosse, 'Japan's gradual shift from passive to active cyber defense: evidence from the domestic discourse and international cooperation'.

122 Takeshi Akahori, 'Statement by Japan to the Open Ended Working Group on Information and Communications', Japanese Mission to the UN, 2019, online.

123 Ministry of Foreign Affairs (MOFA), 'Basic position of the Government of Japan on international law applicable to cyber operations', Japanese Government, 2021, online.

124 See Section 2 of National Centre of Incident Readiness and Strategy for Cybersecurity, 'Japan's Cybersecurity Strategy 2021', Japanese Government, 2021, online. Additionally, Japan is the initiator of the G20 Osaka Track, based on its Data Free Flow with Trust, which has the aim of securing trust in data security and privacy, AI, quantum computing and blockchain.

125 'Basic position of the Government of Japan on international law applicable to cyber operations'.

126 Japan also stresses that a cyber operation conducted by a non-state actor is, in principle, attributable to a state only if the person or group of persons is acting on the instructions of, or under the direction or control of, that state in carrying out the conduct. See Article 8 of the ILC's Articles on State Responsibility.

127 See Article 5 of 'Basic position of the Government of Japan on international law applicable to cyber operations'.

128 MOFA, 'G7 principles and actions on Cyber', Japanese Government, May 2016, online.

129 Patpicha Tanakasempipat, 'Southeast Asian cyber security center opens in Thailand', *Reuters*, 14 September 2018, online.

130 See, for instance, these principles referred to in MOFA, 'Second Japan–India Cyber Dialogue, New Delhi', Japanese Government, 2017, online.

131 See, for instance, these principles referred to in MOFA, 'Osaka Declaration on Digital Economy', Japanese Government, 2019, online.

132 Ministry of Information Technology and Telecommunication (MITT), 'National Cyber Security Policy 2021'. Pakistan Government, July 2021, online.

133 MITT, 'National Cyber Security Policy 2021', Pakistan Government, July 2021, online.

134 'Senate Committee proposes 7-point action plan for cyber secure Pakistan', *Dawn*, 8 July 2013, online.

135 'MITT, National Cyber Security Policy 2021'.

136 ‘Despite ban, Pakistan Govt agencies used Israeli cyber tech forensic tools: report’, *The Wire*, 3 August 2023, online.

137 ‘Hacking team in Pakistan’, *Bolo Bih*, 15 July 2015, online.

138 ‘World report 2024: Pakistan’, *Human Rights Watch*, 2024, online.

139 Ahmed, Zahid Shahab, Ihsan Yilmaz, Shahram Akbarzadeh, Galib Bashirov, *Digital authoritarianism and activism for digital rights in Pakistan*, European Center for Populism Studies, 16 August 2023, online.

140 Federal Investigation Agency, ‘About National Response Centre for Cyber Crime’, Pakistan Government, online.

141 ‘Pakistan’s position on the application of international law in cyberspace’, UN Office for Disarmament Affairs, 3 March 2023, online.

142 ‘Cyber Operations Tracker’, Council on Foreign Relations, online.

143 Dhairya Maheshwari, ‘Pakistani hackers “retaliate” with attacks on MoS website, Indian diplomats; mock Modi’, *National Herald*, 14 January 2019, online; Shashank Shekhar, Arvind Ojha, ‘Indian intel unearths ISI’s social media honey trap designed to snare defence personnel’, *India Today*, 12 October 2016, online; ‘Cybercops hampered by limited access’, *Times of India,* 16 August 2010, online.

144 ‘Pakistan’s position on the application of international law in cyberspace’.

145 ‘Pakistan’s position on the application of international law in cyberspace’.

146 ‘Pakistan’s position on the application of international law in cyberspace’.

147 ‘Press release of Ambassador Munir Akram’s statement at the First Substantive Session of the Open-ended Working Group (OEWG) on the security of and in the use of information and communication technologies in the United Nations’, Pakistan Mission to the UN, 13 December 2021, online.

148 ‘Pakistan’s position on the application of international law in cyberspace’.

149 Hsini Huang, Tien-Shen Li, ‘A centralised cybersecurity strategy for Taiwan’, *Journal of Cyber Policy*, 2018, online; Hsini Huang, ‘A collaborative battle in cybersecurity? Threats and opportunities for Taiwan’, *Asia Policy*, 2020, online.

150 Administration for Cyber Security, ‘Cyber security policies and regulations’, Ministry of Digital Affairs, Taiwanese Government, 2022, online.

151 Ministry of Justice, ‘Cybersecurity Management Act 2018’, Taiwanese Government, 2018, online.

152 Ministry of Justice, ‘Cybersecurity Management Act 2018’.

153 In addition to the Cybersecurity Management Act, the Taiwanese Government has also set a ‘positive responsibility’ through industry-focused plans to boost investment in cybersecurity research and development, product and service business model design, and build-up of the cybersecurity industrial ecosystem.

154 Ministry of Justice, ‘Regulations on Classification of Cyber Security Responsibility Levels’, Taiwanese Government, 2021, online.

155 Adrian Rauchfleisch, Tzu-Hsuan Tseng, Jo-Ju Kao, Yi-Ting Liu, ‘Taiwan’s public discourse about disinformation: the role of journalism, academia, and politics’, *Journalism Practice*, 2022, online.

156 Amber Lin, ‘An assessment of the PRC fifth column network within Taiwan’, *Global Taiwan Brief*, 15 May 2024, online.

157 Hseubing Lu, ‘Draft Counterintelligence Act turns out unsupported, falling flat on investigative bureau’s face’, *Upmedia*, 27 March 2017, online.

158 The Ministry of Digital Affairs was established on 27 August 2022. The International Trade Administration and the Industrial Development Administration of the Ministry of Economic Affairs are the main bodies in Taiwan in charge of reviewing the export control list to keep pace with the Wassenaar Arrangement. Taiwan has specifically named cybersecurity items under the category of ‘strategic materials’ in the export control list since 2017. See Ministry of Economic Affairs, ‘Ministry of Economic Affairs announced to adjust export control list in accordance with the Wassenaar Arrangement’, Taiwanese Government, July 2017, online.

159 International Trade Administration, ‘Taiwan to add to high-tech export control list against Russia’, Taiwanese Government, 12 April 2022, online.

160 Chen Yu-fu, ‘Report details why Chinese products banned at agencies’, *Taipei Times*, 25 October 2022, online.

161 Huang Yenfen, ‘Encourage industry players to actively invest US Cybersecurity Maturity Model Certification (CMMC): key to building Taiwan’s defense industry with an output value of 100 billion’ [鼓勵業者積極投入美國網路安全成熟度模型認證（CMMC）打造臺灣國防產業千億產值的關鍵], *iThome*, 5 December 2022, online. See also Yisuo Tzeng, ‘US CMMC: Opportunity and challenge for Taiwan’, *Defense and Security Biweekly*, Institute for National Defense and Security Research, 18 November 2022, online.

162 Hon-min Yau, ‘An assessment of cyberpower within the triangular relations of Taiwan–US–China and its implications’, *International Journal of Taiwan Studies*, 2019, online.

163 Charles KS Wu, Hsuan-yu Lin, Yao-yuan Yeh, ‘Cybersecurity in Taiwan: challenges and responses’, in Andris Sprūds, Una Aleksandra Bērziņa-Čerenkova, Sintija Broka (eds), *Hybrid threats in Baltics and Taiwan: commonalities, risks and lessons for small democracies*, Latvian Institute of International Affairs and The Asia Programme, Riga, 2022; Enescan Lorci, ‘The nexus of cybersecurity and national security: Taiwan’s imperatives amidst escalating cyber threats’, *Global Taiwan Brief*, 20 March 2024, online.

164 This is based on the amendment of National Intelligence Operations Act in 2020.

165 ‘Ministry of National Defense launches new cybersecurity command’, *New Southbound Policy Portal*, 3 July 2017, online.

166 ‘Ministry of National Defense launches new cybersecurity command’.

167 Ministry of National Defense, *ROC national defense report 2023*, Taiwanese Government, 2023, online.

168 Chih-Hsiang Chang, ‘How does the Tallinn Manual 2.0 shed light on the threat of cyber attacks against Taiwan?’, Proceedings of the 22nd European Conference on Cyber Warfare and Security, 2023, online.

169 IGF clip, online.

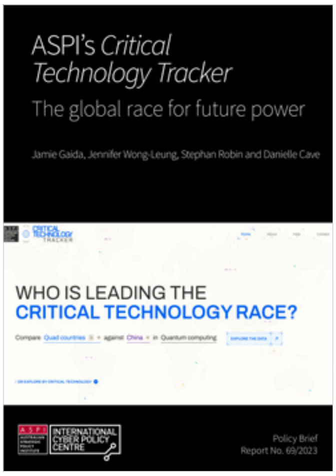
170 Gil Baram, ‘Securing Taiwan’s satellite infrastructure against China’s reach’, *Lawfare*, 14 November 2023, online.

171 ‘Taiwan–US Joint cyber security offensive and defensive exercise—first of its kind in international collaboration on cyber security’, National Center for High-Performance Computing, 11 June 2019, online.

Acronyms and abbreviations

ACD	active cyber defence
AI	artificial intelligence
ASEAN	Association of Southeast Asian Nations
BSSN	*Badan Siber dan Sandi Negara* (National Cyber and Crypto Agency, Indonesia)
CCB	cyber capacity-building
CERT	computer emergency response team
CERT-In	Computer Emergency Response Team—India
CI-CERT	Critical Infrastructure Computer Emergency Response Team (Fiji)
CMMC	Cybersecurity Maturity Model Certification (US)
DCA	Defence Cyber Agency (India)
DNA	deoxyribonucleic acid
HUMINT	human intelligence
ICT	information and communications technology
IT	information technology
ITE Law	Information and Electronic Transaction Law (Indonesia)
METI	Ministry of Economy, Trade and Industry (Japan)
NATO	North Atlantic Treaty Organization
NIG	National Internet Gateway (Cambodia)
NSS	National Security Strategy (Fiji)
OEWG	UN Open-ended Working Group on the security and use of information and communications technologies
PIF	Pacific Islands Forum
PSIA	Public Security Intelligence Agency (Japan)
QSA	quasi-state actor
TNI	*Tentara Nasional Indonesia* (Indonesian Armed Forces)
UN	United Nations
UN GGE	UN Group of Governmental Experts
WMDs	weapons of mass destruction

Some previous CTS publications



ASPI's *Critical Technology Tracker*

The global race for future power

Jamie Gaida, Jennifer Wong-Leung, Stephan Robin and Danielle Cave

WHO IS LEADING THE CRITICAL TECHNOLOGY RACE?

Policy Brief
Report No. 69/2023

Negotiating technical standards for artificial intelligence

A techdiplomacy playbook for policy-makers and technologists in the Indo-Pacific

BART HOGEVEEN
ARINDRAJIT BASU
ISHA SURI
BAANI GREWAL

JUNE 2024

Policy Brief

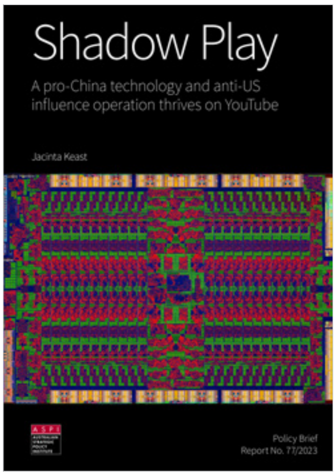
Persuasive technologies in China:

Implications for the future of national security

DARIA IMPIOMBATO, DR NATHAN ATTRILL, ALBERT ZHANG, FERGUS RYAN & BETHANY ALLEN

NOVEMBER 2024

Policy Brief



Shadow Play

A pro-China technology and anti-US influence operation thrives on YouTube

Jacinta Keast

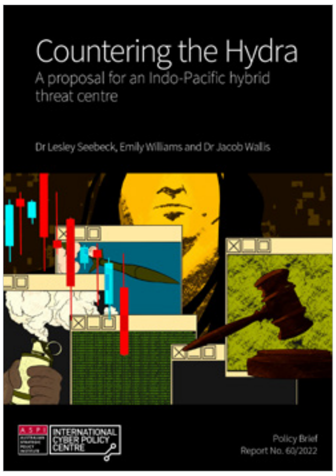
Policy Brief
Report No. 77/2023

ASPI's two-decade Critical Technology Tracker:

The rewards of long-term research investment

JENNIFER WONG LEUNG
STEPHAN ROBIN
DANIELLE CAVE

AUGUST 2024



Countering the Hydra

A proposal for an Indo-Pacific hybrid threat centre

Dr Lesley Seebeck, Emily Williams and Dr Jacob Wallis

Policy Brief
Report No. 60/2022

Australia and South Korea:

Leveraging the strategic potential of cooperation in critical technologies

AFEEYA AKHAND
ATITAYA (ANGELA) SURIYASENEE

DECEMBER 2024

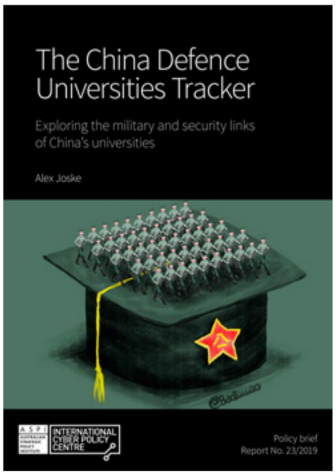
Policy Brief

Buying and selling extremism

New funding opportunities in the right-wing extremist online ecosystem

Ariel Bogle

Policy Brief
Report No. 49/2021



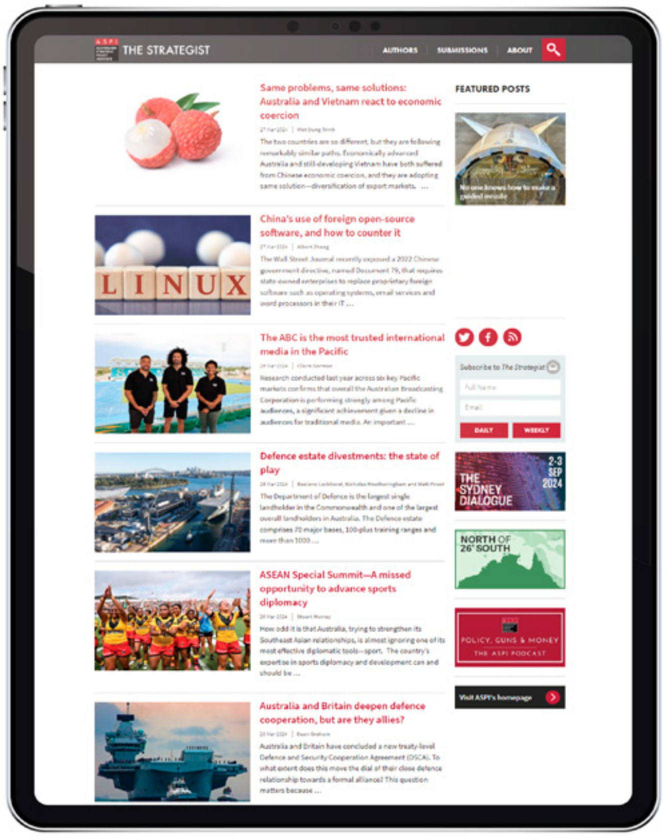
The China Defence Universities Tracker

Exploring the military and security links of China's universities

Alex Joske

Policy brief
Report No. 23/2019

WHAT'S
YOUR
STRATEGY?


THE STRATEGIST
AUTHORS
SUBMISSIONS
ABOUT
FEATURED POSTS
No one knows how to make a guided missile
Subscribe to The Strategist
Full Name
Email
DAILY
WEEKLY
THE SYDNEY DIALOGUE
2-3 SEP 2024
NORTH OF 26° SOUTH
POLICY, GUNS & MONEY
THE ASPI PODCAST
Visit ASPI's homepage

ASPI
AUSTRALIAN
STRATEGIC
POLICY
INSTITUTE

RUSI

ISSN 2209-9689