

Issue

Brief

ISSUE NO. 604
JANUARY 2023



The Future of Cyberwarfare in the Indo-Pacific

Bart Hogeveen

Abstract

The rapid growth in military cyber capabilities of the countries in the Indo-Pacific combined with the use of assets from the cyberwarfare toolbox—in domestic and interstate contexts—is adding uncertainty to already competitive political, military, and economic relations. This issue brief assesses the cyberwarfare context in the Indo-Pacific, and reviews the military cyber capabilities of the region's countries and their commitment to international rules and norms. It also looks at three regional developments that will determine the future impact of cyberwarfare in the Indo-Pacific: the speed of digital transformation of the economy; governments' reflexive and restrictive regulatory approaches to cybersecurity concerns; and the build-up of cyber defence forces.

When Russian forces illegally crossed Ukraine’s sovereign borders in February 2022, the world anxiously anticipated a cyber war would unfold. “When countries send code into battle, their weapons move at the speed of light,” is how Microsoft President and Vice Chair Brad Smith described the nature of the risk.¹ While the world seems to have been spared a digital doomsday, both sides have been fighting one another heavily in the digital domain. Russian security agencies deployed a series of offensive cyber tools for the purpose of reconnaissance and to manipulate, deny, disrupt, degrade, or destroy targeted Ukrainian computers, information systems, and networks.² On the Ukrainian side, the internet community shored up their defences, seemingly successfully, by rallying global support from various foreign government, industry, and non-government entities in what has come to be known as the IT Army.³

In this fog of war, the exact details will only reveal themselves after a while, but analysts, officials and government leaders have already started to formulate predictions of the possible security implications in the Indo-Pacific. At the June 2022 NATO summit—which also saw the participation of the grouping’s four Asia-Pacific partners Australia, New Zealand, Japan, and South Korea—the heads of governments called out China’s systemic challenge to the rules-based international order alongside cyber, space, hybrid and other threats, and its malicious use of emerging and disruptive technologies.⁴ Evidently, key areas of concern are the lessons Beijing’s strategic policy elite may learn from the Russian military’s kinetic, hybrid, and digital campaign; the subsequent Euro-Atlantic resolve to reinvest in defence and political solidarity; and the role of cyberwarfare and use of ICT tools in a potential future conflict in the Indo-Pacific region.

Cyberwarfare in the Regional Context

To date, cyberwarfare is generally perceived through the lens of state-to-state conflicts where one state uses computer technology to deliberately disrupt, manipulate, degrade, or destroy the information and communications technology (ICT) systems of another state for strategic, political, or military purposes.⁵ Such activities can be conducted by entities within the national security and intelligence community or by third parties acting on behalf of a government.

However, this prism overlooks two other important dimensions. One involves the effort to misinform or manipulate public opinion in a given territory, for instance, through disinformation campaigns. In strategies pursued by countries such as China and Russia, the information environment is an integral part of their broader hybrid and cyberwarfare doctrine. It is also an area in which these countries have developed sophisticated capabilities at an industrial scale.⁶

A second overlooked dimension are strategies that consequentially seek to undermine an adversary's economic prosperity. Considering the digital transformation of our economies, the operations of businesses are the first to be affected by any cyber incident. More specifically, targeted efforts to steal intellectual property, business information or trade secrets from entities in foreign economies not only provide aggressors with an unfair competitive advantage, potentially leapfrogging years of research and development investments, but can potentially degenerate a victim nation's long-term prosperity.

The digital domain has made these state practices easier, less costly, largely invisible, and highly deniable. Given China's dominance in IT products and technology infrastructure, many nations in the Indo-Pacific now find themselves in a position of dependence.⁷ In addition, China is generally considered a state that is sponsoring cyber operations quite assertively and in support of its centralised political, military, and economic agenda.

Acts of cyberwarfare, often coined as offensive cyber operations, can come in different shapes and forms. The most prevalent are acts connected to espionage, reconnaissance, and other clandestine forms of gathering information and sensitive data. Of all known state-sponsored cyber operations, more than 80 percent is currently associated with cyber-enabled espionage. Indo-Pacific states such as the US, China, North Korea, Russia, Australia, Japan, South Korea, and Singapore are among the world's leaders in signals intelligence.⁸

Cyberwarfare in the Regional Context

The use of cyber capabilities by security and intelligence agencies in a domestic context must be added to this equation. Any compromises of the internet's technical layers or deployment of malware will likely have adverse transboundary effects.

In efforts to stem discontent, surveil political opposition, demoralise insurgency groups, and control the flow of information and data, security agencies have imposed crude tactics that will easily fit the toolbox of cyberwarfare. Examples include internet shutdowns such as in India, Myanmar, and Indonesia, where governments are abusing their authority over internet service providers; attempts to establish national internet gateways—a system of controlled entry points for cross-boundary internet connections—in countries like Myanmar and Cambodia (although the latter has been suspended for now⁹); and the (mis)use of cybersecurity, cybercrime and misinformation laws to stem civil society voices and create an environment of self-censorship.¹⁰ These practices severely affect citizens' security, privacy, human rights, and fundamental freedoms.

However, decisions to use assets from the cyberwarfare toolbox do not occur in isolation and tend to be connected to (pre-)existing political tensions, military confrontations, and economic competition. In terms of inter-state relations, cyberwarfare acts have been observed in long-time military stand-offs on the Korean Peninsula, coercive actions around the South and East China Seas disputes, around Taiwan, and in the border conflicts between India and Pakistan and India and China. North Korea has also shown a propensity to undertake 'standalone' cyberattacks. For instance, in 2016, North Korean hackers successfully found access to the Central Bank of Bangladesh's messaging system and funnelled away billions of dollars through the Philippines.¹¹

Growing Military Cyber Capabilities

The US-China strategic competition is the overriding issue that casts a shadow over many Indo-Pacific regional security issues, including in the cyber domain. China, by now, is seen as an assertive and, at times, aggressive actor using its various advanced cyber capabilities in combination with proxy agents to seek political, military, and economic intelligence advantages, exert coercive influence over foreign government elites, and disrupt social and economic life in opponent states.¹²

The global focus on China, however, seems to have offered developing nations in the Indo-Pacific free reign to build and develop their military cyber capabilities without much outside scrutiny. By now, almost all militaries possess some form of cyber capability, and most claim to be able to deploy cyberwarfare tools (see Table 1).

**Table 1:
Overview of Military and National Security Cyber Capabilities of Indo-Pacific Countries**

State	Capabilities	Mandate
India	Defence Cyber Agency (est. 2018)	To formulate a cyberwarfare doctrine to develop and maintain relevant capabilities to deter, defend and disrupt an opponent's cyber operations.
Australia	- Australian Defence Force (ADF) Information Warfare Division (est. 2017) - Australian Signals Directorate (ASD; cyber capabilities established prior to 2010)	The ADF's cyber capabilities have two distinct functions: cybersecurity of the ADF and cyber operations. The offensive cyber capability rests with ASD. Offensive cyber capacity in support of military operations is a civil-military partnership. ¹³
Japan	Self-Defense Forces' (SDF) Cyber Defense Unit (est. 2022)	The unit's primary function is to oversee the cyber defences for the entire SDF. Reportedly, the SDF has no offensive capability or mandate. ¹⁴

Growing Military Cyber Capabilities

State	Capabilities	Mandate
China	<p>People’s Liberation Army Strategic Support Force (SSF; est. 2015)</p> <p>Ministry of State Security (MSS)</p>	<p>Focused on ‘information dominance’, the SSF concentrates on information operations, which include synchronisation of cyber, electronic, and psychological warfare components. The SSF aims to develop and deploy significant cyber fires.¹⁵</p> <p>The MSS’ activities appear to focus on cyber-enabled intelligence for strategic, political, and economic purposes, typically operating through proxies in the form of advanced persistent threats.¹⁶</p>
Singapore	Digital and Intelligence Service (est. 2022)	A division-sized entity to effectively navigate cyber threats from external aggressors. Its mandate is to provide accurate, relevant, and timely early warning and operational intelligence for the Singapore military to operate as a networked force.
Indonesia	Tentara Nasional Indonesia (TNI) Satuan Siber (est. 2017)	To keep the TNI’s information resources safe from interference and misuse or use by other parties; provide protection for strategic data; collect information on threats and disturbances; and be able to build the cyber defence capacity of the TNI in the form of deterrence, prosecution, and recovery capabilities. ¹⁷
Malaysia	<p>Cyber Command (est. 2019)</p> <p>Cyber Warfare Signals Regiment (99 RSPS; est. 2021)</p>	<p>To enhance cyber operations by conducting cyber defence operations, cyber exploitation operations, cyber-attack operations and developing cyber expertise, in line with the active defence concept as stipulated in Malaysia’s Cyber Security Strategy.¹⁸</p> <p>To strengthen the Malaysian Armed Forces’ capacity and preparedness in the face of cybersecurity challenges and cyber threats from various domains, including by considering the acquisition of the latest assets and systems.¹⁹</p>

Growing Military Cyber Capabilities

State	Capabilities	Mandate
Philippines	Armed Forces of the Philippines Cyber Group (est. > 2017)	To defend the country from cyberattacks; gather foreign cyber threat intelligence and determine attribution; secure national security and military systems; support national protection, prevention, mitigation of and recovery from incidents; and investigate cybercrimes under military jurisdiction. ²⁰
	Cyber Battalion, Philippine Army (est. 2020)	To support the army’s compliance with adopting cyberspace as another domain of operations. It aims to conduct active and defensive cyber operations to protect army cyber assets and defend it from cyberattacks across its different domains of operations.
Vietnam	People’s Army of Vietnam, Cyber Operations Command (est. 2018)	To protect the country from cyberattacks, focusing on ensuring national cyberspace security and fighting high-tech crimes, contributing to the defence of national sovereignty over the mainland, airspace, seas, and cyberspace. ²¹
	Force 47 (est. 2017)	To scour and collect information on social media, participate in online debates to maintain “a healthy cyberspace” and counter any “wrongful opinions” about the regime and protect it and the public from “toxic information”. ²²

Arguably, most cyber activities of South and Southeast Asian countries’ military focus on the defensive side, concentrated on protecting their ICT networks in peacetime and during armed conflict. But Southeast Asian defence strategists have now started to talk about capabilities to conduct “cyber exploitation operations” and “cyber-attack operations” as well.²³

This cyberwarfare discourse goes hand in hand with a surge in the establishment of new institutions. For instance, in March 2022, Singapore announced a plan to establish a Digital and Intelligence Service in the Defence Force as “the digital domain has grown into a full-fledged arena of conflict and contestation”,²⁴ and Japan launched a new cyber defence unit within the Self Defence Forces.²⁵ In April, Indonesia’s Chief of Defence reflected on the TNI Cyber Unit’s role in mounting cyber defences that can respond to threats from overseas.²⁶

Growing Military Cyber Capabilities

The US and China have also enhanced their cyberwarfare capabilities in recent years. In 2018, under the Trump administration, the US Cyber Command launched the concept of ‘persistent engagement’, which centres on the idea of seizing and maintaining “the initiative in cyberspace by continuously engaging and contesting adversaries and causing them uncertainty wherever they manoeuvre”.²⁷ After the reorganisation of the People’s Liberation Army Strategic Support Force in 2015, China prioritised boosting its cyberwarfare capabilities, in part, by a ‘fusion’ of military and civilian cyber assets. As a testament, China reportedly managed to enhance its ability to exploit software zero-day vulnerabilities by six-fold in 2021 compared to 2020.²⁸

In this competitive environment, other countries may feel compelled to make substantial investments in their indigenous cyber capabilities. For instance, in response to various cyber-enabled intrusions that were attributed to the Chinese state, the Australian government announced an AUD 1.35-billion investment in its defence apparatus’ cyber capabilities in 2020.²⁹

The establishment of military cyber (defence) entities, in some cases accompanied by significant financial stimulus, illustrate that cyber is a domain of warfare and that more countries are raising their political-military cyber posture.

The Indo-Pacific military cyber posture currently sees a sharp divide between the highly developed and developing nations. For the latter, their stance will, at least for the time being, remain of a defensive nature—in declared policy if not action—and serve a predominantly domestic imperative. Nonetheless, the build-up signals an increasing militarisation of the Indo-Pacific digital domain, which comes with the risk of unintended and immature cyber activities that may spill across borders, particularly from those jurisdictions where political caution and legal scrutiny are less firmly embedded.

Understanding the Cybersecurity Landscape

Most of the developing cyber nations in the Indo-Pacific have been turning a blind eye to the regional security implications of growing military cyber capabilities, perhaps because they consider such issues the concern of bigger cyber powers. Even within the cybersecurity portfolio of ASEAN, for example, most attention goes to issues like cybercrime, misinformation campaigns, and data security. Other economic and security issues enabled by ICTs and digital connectivity, such as reliable energy, food security, maritime security, and post-Covid-19 economic recovery, take precedence in these countries.

There is also a systemic lack of transparency and willingness to share information in the Indo-Pacific region. Among the advanced cyber nations, China, for instance, does not acknowledge its military cyber capabilities despite overwhelming evidence and does not disclose its policies, doctrine, and command and control mechanisms.³⁰ On the other hand, Canada, Australia, New Zealand, the UK, and the US, which comprise the Five Eyes intelligence alliance, have acknowledged their offensive cyber capabilities and willingness to use these,³¹ but struggle to form reciprocal and trusted partnerships with others in the region.

Sharing cyber threat information through non-political platforms, such as the Asia-Pacific Computer Emergency Response Team, remains challenging. Not only are national cybersecurity authorities very sparse with their reporting, but disclosed data often lacks methodological rigour and paints a biased picture. Global cybersecurity firms, which fill in part of the puzzle in other parts of the world, face a lack of data points and analytical depth in the Indo-Pacific.³² This weakness in a collective (critical) understanding of the regional cybersecurity threat environment produces a political and policy environment in which cybersecurity risks are either under- or overestimated in terms of effects on the economy and regional stability.

International Law and Norms in Cyberspace

The build-up of military capabilities in an area where poor situational awareness pervades is not unique to the cyber domain. To seek reassurance and mitigate the greatest risk, the global community typically relies on existing principles of international law and the responsibility of states to follow agreed norms.

In regard to cybersecurity developments that affect international peace and security, the UN General Assembly recognised in 2013 that international law applies to states' actions in cyberspace. This recognition is part of a normative framework of responsible state behaviour that includes norms of responsible behaviour such as not attacking critical infrastructure, not allowing your territory to be misused for malicious cyber activities, and reporting ICT vulnerabilities responsibly (see Figure 1).

Figure 1:
UN Norms of Responsible State Behaviour in Cyberspace



Source: Australian Strategic Policy Institute³³

International Law and Norms in Cyberspace

The UN Security Council's permanent members have driven this process of establishing legal and normative boundaries since the late 1990s, but other countries have also contributed. For example, ASEAN member states collectively embraced the UN framework in 2018 and are taking steps at the regional level to strengthen cyber stability by enabling a platform for sharing information and good practices and offering capacity-building assistance.³⁴

While high-level commitments are essential, a gap remains in a shared Indo-Pacific commitment to the outcomes of this UN-centred process. For instance, many states have yet to submit their views on how they see international law being applied to state conduct in cyberspace. Singapore,³⁵ Australia,³⁶ Japan,³⁷ and the US³⁸ have published their statements, and Malaysia announced an intent to do so,³⁹ but countries such as India, Pakistan, Indonesia, South Korea, the Philippines, Vietnam, and China have not. And most Indo-Pacific nations are yet to attest that they are following agreed UN norms and describe how they observe them.

In the ongoing diplomatic contest of values and interests, the Non-Aligned Movement has formed a position that argues against 'the militarisation of cyber space'.⁴⁰ India, for example, has called on the international community to "unilaterally declare to refrain from militarisation or offensive use of ICTs".⁴¹

Such positions not only look out of touch with the reality of our external environment but also with domestic developments; cyberspace has become a national security issue. Furthermore, this position on non-militarisation keeps holding a tendency in place by some countries to refrain from acknowledging and disclosing their capabilities. This undermines the effective application of international law and adherence to norms. Any steps that help take away legal ambiguity and reinforce multilaterally agreed rules should be seen as serving the interests of emerging digital powers and those states intend on acting responsibly.

A Regional Outlook on Cyberwarfare

Geostrategic competition between the US and China will impact the future of cyberwarfare in the Indo-Pacific. However, a few distinct developments in the region may determine how the use of offensive cyber tools and tactics will play out there.

First, the process of digital transformation of the region's economies and societies is creating a new balance of influence and cyber power. Singapore, Japan, and South Korea are world-leading digital economies; India is a software development powerhouse; China is a global provider of accessible technology and manufacturing resources; and most Southeast Asian countries have embraced ambitious digital economy strategies relying on the Indo-Pacific's burgeoning youth and grassroots tech ecosystems. This trend will continue, albeit at different paces, and digital trade will account for a growing percentage of countries' GDP.

Next, governments in the region are slated to continue to press ahead with reflexive and restrictive regulatory approaches in the cybersecurity, technology, and online information environments. The popularity of social media platforms, in combination with the (mobilising) power of the smartphone, is perceived as a challenge to stability by some states and to regime survival or social cohesion by others. Despite a variety in political regimes and levels of prosperity and diverging approaches to internet governance and regulation across the Indo-Pacific, governments in the region, to varying degrees, seem to be on a trajectory where they seek to impose sovereign borders on the different layers that make up the cyber domain.


With the new cyber defence forces that have been formed, discussions of conflicts in Indo-Pacific's cyberspace now enter a new era. The earlier established cyber units have secured a central place in their countries' overall national security posture. The newer cyber defence forces can rely on political interest, and their mandates and influence are more likely to grow. A key determinant of a state's future cyber behaviour will be the extent to which appropriate checks and balances in the context of civilian oversight and control of the cybersecurity agencies can be established.

A Regional Outlook on Cyberwarfare

It is essential to recognise that all three trends can be managed constructively and should concern all stakeholders in the Indo-Pacific equally. Security in the region will remain competitive in the years ahead with suppressed inter-state conflicts and contested national ICT domains. The internet governance communities will have to find an intricate balance between encouraging digital innovation, adequate cybersecurity, a permissive online information environment, and a responsible role for the various security and intelligence services.

“Geostrategic competition between the US and China will impact the future of cyberwarfare in the Indo-Pacific. But a few distinct developments in the region, such as the digital transformation of the region’s economies and societies, could determine how the use of offensive cyber tools and tactics will play out there.”

Conclusion

The securitisation and militarisation of the cyber domain will continue, and it is important that the Indo-Pacific policy elite acknowledges this at face-value. In fact, most governments in the region play their part in this, and the onus of mitigating the risks of misuse or irresponsible use of cyberwarfare tools also lies with them. While nations should be discouraged from entering a ‘cyber capabilities arms race’, the strengthening of national cybersecurity postures will be seen as critical national interests. Legal and responsible development and use of cyber assets—in a domestic and international context—means that national and defence leaders, civil society advocates, technicians, and industry experts must keep a close watch on the precise nature of malicious incidents and potentially destabilising trends in capability development, but also be better prepared to call out irresponsible behaviour, and engage in meaningful and constructive bilateral and multilateral dialogues. 

(This brief was first published in the GP-ORF Series ‘Future Warfare and Technologies: Issues and Strategies’.)

Bart Hogeveen is Head of Cyber Capacity Building at the Australian Strategic Policy Institute’s International Cyber Policy Centre.

- 1 Brad Smith, “Defending Ukraine: Early Lessons from the Cyber War,” Microsoft on the Issues, June 22, 2022, <https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/>
- 2 Microsoft, *Defending Ukraine: Early Lessons from the Cyber War*, 22 June 2022, <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK>
- 3 Monica Kaminska, James Shires, and Max Smeets, *Cyber Operations during the 2022 Russian invasion of Ukraine: Lessons Learned (so far)*, European Cyber Conflict Research Initiative, Tallinn Workshop Report, July 2022, : https://eccri.eu/wp-content/uploads/2022/07/ECCRI_WorkshopReport_Version-Online.pdf
- 4 NATO, *Madrid Declaration*, paragraph 6, 29 June 2022, https://www.nato.int/cps/en/natohq/official_texts_196951.htm
- 5 Australian Cyber Security Centre, *Glossary: cyber warfare*, <https://www.cyber.gov.au/acsc/view-all-content/glossary/cyber-warfare>. See also: Tom Uren, Bart Hogeveen and Fergus Hanson, Defining offensive cyber capabilities, *Report for the Global Commission for the Stability of Cyberspace*, July 2018, <https://www.aspi.org.au/report/defining-offensive-cyber-capabilities>
- 6 Nikolay Bozhkov, *China’s Cyber Diplomacy: A Primer*, Digital Dialogue, EU Cyber Direct, March 2020, <https://eucd.s3.eu-central-1.amazonaws.com/eucd/assets/-GX150Cl/bozhkov-digital-dialogue-final.pdf>; Janne Hakala, Jazlyn Melnychuk, *Russia’s Strategy in Cyberspace*, NATO Strategic Communications Centre of Excellence, June 2021, <https://stratcomcoe.org/publications/russias-strategy-in-cyberspace/210>
- 7 Dirk van der Kley, Benjamin Herscovitch, and Gatra Priyandita, *China Inc. and Indonesia’s Technology Future*, ANU National Security College, July 2022, https://nsc.crawford.anu.edu.au/sites/default/files/publication/nsc_crawford_anu_edu_au/2022-07/web_nsc_pop_indonesia_education_no.27_1.pdf
- 8 Gatra Priyandita, Bart Hogeveen and Ben Stevens, *State-sponsored economic cyberespionage for commercial purposes. Tackling an invisible but persistent threat to prosperity*, Australian Strategic Policy Institute, Policy Brief 67, 2022, page 11; Rory Medcalf, *Contest for the Indo-Pacific: Why China Won’t Map the Future*, La Trobe University Press (3 March 2020)
- 9 Sebastian Strangio, Cambodia Puts Controversial National Internet Gateway Plan on Hold, *The Diplomat*, 16 February 2022, <https://thediplomat.com/2022/02/cambodia-puts-controversial-national-internet-gateway-plan-on-hold/>
- 10 Janjira Sombatpoonsiri and Sangeeta Mahapatr, *COVID-19 Intensifies Digital Repression in South and Southeast Asia*, Carnegie Endowment for International Peace, 19 October 2022, <https://carnegieendowment.org/2021/10/19/covid-19-intensifies-digital-repression-in-south-and-southeast-asia-pub-85507>

- 11 Neha Banka, Explained: The story of how North Korea hackers stole \$81 million from Bangladesh Bank, *The Indian Express*, 30 June 2021, <https://indianexpress.com/article/explained/bangladesh-bank-robbery-north-korea-lazarus-heist-7375441/>
- 12 Institute for International and Strategic Studies, *Asia Pacific Regional Security Assessment 2019*, Chapter Five: China's cyber power in a new era, May 2019, <https://www.iiss.org/publications/strategic-dossiers/asiapacific-regional-security-assessment-2019/rsa19-07-chapter-5>
- 13 Fergus Hanson and Tom Uren, *Australia's offensive cyber capability*, Australian Strategic Policy Institute, 2018, <https://www.acs.org.au/carousel-pages/policy-brief-australia-offensive-cyber-capability.html>
- 14 Aimee Chanthadavong, *Japan to bolster national cybersecurity defence with 800 new hires: Report*, ZDNet, 5 July 2021, <https://www.zdnet.com/article/japan-to-bolster-national-cybersecurity-defence-with-800-new-hires-report/>
- 15 The Hague Centre for Strategic Studies, *Cyber Arms Watch: An Analysis of Stated & Perceived Offensive Cyber Capabilities*, May 2022, <https://hcss.nl/wp-content/uploads/2022/05/Cyber-Arms-Watch-HCSS-2022-1.pdf>
- 16 Institute for International and Strategic Studies, *Asia Pacific Regional Security Assessment 2019*, Chapter Five: China's cyber power in a new era, May 2019, <https://www.iiss.org/publications/strategic-dossiers/asiapacific-regional-security-assessment-2019/rsa19-07-chapter-5>
- 17 Ministry of Communication, Government of Indonesia, *TNI bentuk Satsiber*, https://m.kominfo.go.id/content/detail/10997/tni-bentuk-satsiber/0/sorotan_media
- 18 Ministry of Defence, Government of Malaysia, *Defence White Paper*, paragraph 38, 2020. <https://www.mod.gov.my/images/mindef/article/kpp/DWP-3rd-Edition-02112020.pdf> para 38.
- 19 "Malaysian Armed Forces to set up cyber warfare regiment to strengthen cyber defence, says army chief," *MalayMail*, 2 March 2021, <https://www.malaymail.com/news/malaysia/2021/03/02/malaysian-armed-forces-to-set-up-cyber-warfare-regiment-to-strengthen-cyber/1954285>
- 20 Department of ICT, Government of The Philippines, *National Cyber Security Plan 2022*, <https://dict.gov.ph/national-cybersecurity-plan-2022/>
- 21 People's Army Newspaper, *MND debuts Cyberspace Operations Command*, 9 January 2018, <https://en.qdnd.vn/military/news/mnd-debuts-cyberspace-operations-command-488684>
- 22 Dien Nguyen An Luong, "How The Vietnamese State Uses Cyber Troops to Shape Online Discourse", *ISEAS Perspective 2021/22*, 3 March 2021, <https://www.iseas.edu.sg/articles-commentaries/iseas-perspective/2021-22-how-the-vietnamese-state-uses-cyber-troops-to-shape-online-discourse-by-dien-nguyen-an-luong/>

- 23 Ministry of Defence, Government of Malaysia, *Defence White Paper*, paragraph 38, 2020, <https://www.mod.gov.my/images/mindef/article/kpp/DWP-3rd-Edition-02112020.pdf>; and National Security Council, Government of Malaysia, *Malaysia Cyber Security Strategy, 2020-2024*, <https://asset.mkn.gov.my/wp-content/uploads/2020/10/MalaysiaCyberSecurityStrategy2020-2024.pdf>
- 24 Ministry of Defence, Government of Singapore, *Fact Sheet: Timely Establishment of Digital and Intelligence Service*, 2 March 2022, https://www.mindef.gov.sg/web/portal/mindef/news-and-events/latest-releases/article-detail/2022/March/02mar22_fs
- 25 “Japan’s Self-Defense Forces launch new cyberdefense unit,” *Japan Times*, 17 March 2022, <https://www.japantimes.co.jp/news/2022/03/17/national/sdf-cyberdefense-unit/>
- 26 Tempo, *TNI Commander Talks of Future Cyber Threats*, 28 May 2021, <https://en.tempo.co/read/1466510/tni-commander-talks-of-future-cyber-threats>
- 27 Jacqueline Schneider, Persistent Engagement: Foundation, Evolution and Evaluation of a Strategy, *Lawfare*, 10 May 2019, <https://www.lawfareblog.com/persistent-engagement-foundation-evolution-and-evaluation-strategy>
- 28 Patrick Howell O’Neill, How China built a one-of-a-kind cyber-espionage behemoth to last, *MIT Technology Review*, 28 February 2022, <https://www.technologyreview.com/2022/02/28/1046575/how-china-built-a-one-of-a-kind-cyber-espionage-behemoth-to-last/>
- 29 Jane Macmillan, Cybersecurity spending gets \$1.35 billion boost in wake of online attacks against Australia, *ABC*, 29 June 2020, <https://www.abc.net.au/news/2020-06-29/cyber-security-investment-link-attacks-scott-morrison/12404468>
- 30 Nigel Inkster, *China’s cyber power*, Institute for International and Strategic Studies, 2016.
- 31 Josh Gold, *The Five Eyes and Offensive Cyber Capabilities: Building a ‘Cyber Deterrence Initiative’*, NATO Cyber Cooperative Cyberdefence Centre of Excellence, 2020, <https://ccdcoe.org/uploads/2020/10/2020-Josh-Gold-Five-Eyes-and-Offensive-Cyber-Capabilities.pdf>
- 32 Author’s conversations.
- 33 “UN Cyber Norms”, Australian Strategic Policy Institute, <https://www.aspi.org.au/cybernorms>
- 34 ASEAN, *ASEAN Leaders’ Statement on Cybersecurity Cooperation*, 2018, <https://asean.org/asean-leaders-statement-on-cybersecurity-cooperation/>
- 35 Cyber Law Toolkit, National position of Singapore (2021), [https://cyberlaw.ccdcoe.org/wiki/National_position_of_Singapore_\(2021\)](https://cyberlaw.ccdcoe.org/wiki/National_position_of_Singapore_(2021))
- 36 Cyber Law Toolkit, National position of Australia, [https://cyberlaw.ccdcoe.org/wiki/National_position_of_Australia_\(2020\)](https://cyberlaw.ccdcoe.org/wiki/National_position_of_Australia_(2020))

Endnotes

- 37 Cyber Law Toolkit, National position of Japan, [https://cyberlaw.ccdcoe.org/wiki/National_position_of_Japan_\(2021\)](https://cyberlaw.ccdcoe.org/wiki/National_position_of_Japan_(2021))
- 38 Cyber Law Toolkit, National position of US, [https://cyberlaw.ccdcoe.org/wiki/National_position_of_the_United_States_of_America_\(2021\)](https://cyberlaw.ccdcoe.org/wiki/National_position_of_the_United_States_of_America_(2021))
- 39 National Security Council, Government of Malaysia, *Malaysia Cyber Security Strategy, 2020-2024*, <https://asset.mkn.gov.my/wp-content/uploads/2020/10/MalaysiaCyberSecurityStrategy2020-2024.pdf>
- 40 Paul Meyer, *A New Process for an Old Problem: Governing State Behaviour in Cyberspace*, Centre for International Governance and Innovation, 25 November 2019, <https://www.cigionline.org/articles/new-process-old-problem-governing-state-behaviour-cyberspace/>
- 41 Contributions of the Indian delegation to the UN Open-ended Working Group on ICT Security, 2019-2021.



Ideas . Forums . Leadership . Impact

20, Rouse Avenue Institutional Area,
New Delhi - 110 002, INDIA
Ph. : +91-11-35332000. Fax : +91-11-35332005
E-mail: contactus@orfonline.org
Website: www.orfonline.org