13. Indonesia

Indonesia's first formal strategy for civil-sector cyber security emerged only in 2018, one year after its principal cyber agency was created. Cyber-related institutional changes within the armed forces began around 2014 but have not yet given rise to a published military cyber strategy or doctrine. Political control of cyber policy is exercised through the president. Indonesia has only limited cyber-intelligence capabilities but has been investing in cyber surveillance for domestic security. It is more engaged than most developing countries in cyber security and in employing digital technologies. On international cyberspace policy, it participates actively in the G20, the Asia-Pacific Economic Cooperation, the Association of Southeast Asian Nations and the Organisation of Islamic Cooperation. Indonesia has some cyber-surveillance and cyber-espionage capabilities, but there is little evidence of it planning for, or having conducted, offensive cyber operations. Overall, Indonesia is a third-tier cyber power. Given that it is expected to become the fourth-largest economy in the world by around 2030, it could be well placed to rise to the second tier if the government decides that strategic circumstances demand greater investment in the cyber domain.

Strategy and doctrine

Until 2017, cyberspace policy in Indonesia was largely undeveloped. Institutions, coordination and legal foundations were all weak and there was no overall national strategy.[1] Only some basic institutional foundations were in place: the National Crypto Agency (founded in 1946) had been strengthened to some extent; a Computer Emergency Response Team (CERT) had been created in 1998 through a private initiative; there was a government infrastructure-incident-response team (another CERT, in practice), set up in 2007;[2] 14 additional CERTs were in place by 2016; and some relevant laws and regulations had been refined.[3]

The principal development in 2017 was the establishment, by presidential decree, of the National Cyber and Crypto Agency (BSSN),[4] replacing the National Crypto Agency.[5] Also in 2017, the national police force announced the expansion of its cyber-crime unit from 40 to 100 personnel.[6] The country began to frame its cyber defence in very broad terms as part of its concept of 'total defence'.[7]

The first national cyber-security strategy was published by the BSSN in 2018, setting out five objectives: cyber resilience, security of public services, enforcement of cyber law, a culture of cyber security, and cyber security in the digital economy.[8] The strategy was also intended to support the country's counter-terrorism policies. Its stated goals included the promotion of multi-stakeholder engagement and fostering global trust in Indonesia's management of its cyberspace. As in most countries, the publication of a formal strategy

List of acronyms

ASEAN	Association of Southeast Asian Nations
BSSN	National Cyber and Crypto Agency
MoD	Ministry of Defence
OIC	Organisation of Islamic Cooperation
TNI	Indonesian Armed Forces

provided a foundation for further measures. Later in 2018, for example, the national police force set up a Cyber Crime Directorate to counter disinformation spread though digital media.[9]

In December 2020 the BSSN released the draft of a new national cyber-security strategy for public consultation.[10] It places greater emphasis on nationally significant cyber incidents and focuses on seven specific areas: risk management in national cyber security; preparedness and resilience; critical information infrastructure; capacity-building; increasing awareness; legislation and regulation; and international cooperation. Other stated objectives include protecting the country from any interference in cyberspace that might disrupt public order, and building on improved cyber security to expand the potential of the digital economy. The new draft follows Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions,[11] which raised the status of the cyber-security strategy by declaring it to be part of national-security policy.

Given the deteriorating security situation in Indonesia, one of the government's priorities has been to counter domestic terrorism and online extremism, as well as to clamp down on political protest. For example, after a large protest in October 2020, disinformation laws were invoked to allow the police to take action online against political activists[12] and Islamist groups, including the Muslim Cyber Army hacker group responsible for spreading religious intolerance online.[13] There is now a debate in Indonesian politics about the extent to which government policy should involve censoring cyberspace.[14]

On military cyber policy, the debates and analyses have generally been more advanced than those in the civil sector but have not always led to concrete progress.

The Ministry of Defence (MoD) laid out comprehensive guidelines for national cyber defence in 2014,[15] with the focus more on securing defence assets against cyber attacks rather than on any concept of sustained cyber-enabled warfare. Besides acknowledging the need for counter-attack capabilities for the purpose of deterrence, the guidelines did not cover offensive cyber.

A 2015 defence white paper went further, presenting cyber defence as one of four pillars of Indonesia's overall defence posture, alongside air defence, strategic strike and electronic warfare.[16] It described cyber security as central to national defence capabilities, highlighted the importance of integrating cyber with all other instruments of national power,[17] and declared a commitment to modernising the country's cyber capabilities.[18]

In 2017 the MoD began promoting a 'civil-defence concept' in coordination with the National Development Planning Agency, aiming to ensure that methods of 'non-military defence' – including in cyberspace – were adopted by all ministries and state institutions.[19] The initiative was widely seen in defence circles as consistent with the country's concept of total defence in which all citizens are regarded as potential combatants, including in cyberspace.

Also in 2017, the armed forces carried out their first major institutional reform by setting up a cyber unit – Satuan Siber, or Satsiber – to develop doctrine, policy, procedures and tactics to deal with cyber threats.[20] Its primary mission is to ensure the cyber security of defence-related critical national infrastructure, though there is a long-term plan to develop offensive capability.[21] Satsiber has also been assigned an early-warning role in monitoring foreign-military movements (especially those of units equipped with missiles) in the immediate region. The development of military cyber strategy and doctrine appears embryonic and there is no substantive evidence of it in unclassified sources.

Governance, command and control

The BSSN, the principal cyber-security agency, operates within the framework of the Coordinating Ministry for Political, Legal and Security Affairs and reports directly to the president.[22] The head of the BSSN has four deputies, responsible for threat identification and detection, protection, response and recovery, and technical policies for monitoring and control.[23] The BSSN set up the first government CERT in 2018,[24] building on the previously existing private CERT and the government's incident-response team.

In the Indonesian armed forces (TNI)[25] there has been clear organisational cyber command and control since the creation of Satsiber in 2017, though the command arrangements are split between the Commander TNI, when Satsiber undertakes military operations,[26] and the Chief of the General Staff, for day-to-day management.

Satsiber has subordinate cyber units in each of the three armed services.[27] Complementing the work of Satsiber, the Cyber Defence Centre[28] operates under the command of the Defence Intelligence Agency within the Ministry of Defence.[29] The technical means for undertaking operational cyber command and control, however, probably mirror the weaknesses in communications systems reported elsewhere in the armed forces.[30]

The Ministry of Foreign Affairs set up its own Digital Command Centre for the twin purposes of improving crisis-management procedures for national emergencies in cyberspace and managing Indonesia's international diplomacy on cyber matters. The combining of two such different functions in one entity is unusual, since crisis management of cyber incidents requires a very different skill set from conducting cyber diplomacy, with little crossover in the day-to-day work of the two missions.

Changes in doctrine, technology and personnel planning are needed if Indonesia is to establish a basic capability for cyber warfare. So too is greater cohesion, as divergent views have been observed among policymakers and those responsible for implementing the development of cyber defence.

Core cyber-intelligence capability

The lead coordinating agency for national civil-sector cyber intelligence is the BSSN.[31] The body mainly responsible for foreign and military intelligence is the Strategic Intelligence Agency (BAIS),[32] which has proved capable of assisting the police by, for example, conducting cyber surveillance against potential threats to the 2018 regional elections.

The BSSN was allocated 2.2 trillion rupiah (US$127 million) in the 2020 budget but its director at the time said 3trn rupiah (US$190m) would be needed to achieve its objectives.[33] The goals he mentioned included developing indigenous technology and the National Cyber Security Operations Centre (tasked with monitoring the digital networks of Indonesia's critical national infrastructure, including the energy, communications and transport systems) and recruiting graduates of the required calibre.[34] This suggests that Indonesia's cyber-intelligence capabilities are relatively unsophisticated and that any wider intelligence reach, beyond the focus on domestic terrorism, is severely under-resourced.

Cyber empowerment and dependence

By 2020 Indonesia had established itself as a rising digital power within the G20, albeit still at a lower level than most other members and with a long way to go to achieve its ambitions in the sector.[35] The government has launched ambitious education programmes, attempted to attract talent through its immigration policies, and promoted a start-up culture.[36] The digital economy was projected to reach double-digit annual growth (11%) in 2020.[37] E-commerce remains the main driver of growth in the economy as a whole. Three of Indonesia's start-ups (Gojek, Tokopedia and Traveloka) have reached high capitalisation levels (US$10.5 billion, US$7.5bn and US$2.75bn respectively), largely by having expanded internationally.[38] The country aspires to become a global hub for Islamic finance, though in that respect it is still in fourth place (behind Malaysia, Saudi Arabia and the United Arab Emirates) in terms of annual value traded.[39]

The average level of digital skills among the Indonesian population does not match the government's ambitions

Although the overall internet penetration rate is quite high (73% of the population in mid-2020),[40] there is a wide gap between Java and all the other islands.[41] There are individual cities with particularly high figures, for example Jakarta (85%), Surabaya (83%) and Bandung (82.5%).[42] More than 90% of Indonesians who use the internet do so via mobile phone. The country was ranked 85th in the 2020 Global Innovation Index, which indicates the weak foundations of its digital economy.[43] The digital sector accounts for only 12% of GDP according to a 2020 estimate,[44] though the government hopes to see that figure rise to 15% by 2025.[45]

The average level of digital skills among the population does not match the government's ambitions.[46] Research commissioned by Amazon Web Services in six Asia-Pacific countries found that only 19% of

Indonesian respondents use digital skills in their jobs – very different from Australia and Singapore, for example, where the corresponding figures are 64% and 63% respectively.[47] The skills shortage could inhibit the development of the indigenous digital industry. Indonesia's reliance on foreign suppliers for its telecommunications infrastructure was highlighted in 2019 during the Huawei controversy, which led a senior official in the Coordinating Ministry for Political, Legal and Security Affairs to declare the need for 'a special, reliable, integrated and secure telecommunications system against cyber threats both from within the country and abroad', and to admit that the existing system had not been able to 'answer the need for national information security'.[48]

Although Indonesia's research in artificial intelligence (AI) is growing, it is still a relative newcomer to the field. It has accelerated efforts to improve collaboration between academia and industry on AI research, for example between the University of Indonesia and Tokopedia[49] and between the Bandung Institute of Technology and Bukalapak.[50] Meanwhile, investment by Indonesian companies in AI solutions is still much lower (US$0.20 per capita) than in more developed economies such as Singapore (US$68 per capita).[51] Nevertheless, it was reported in August 2020 that Indonesia had 74 AI-focused start-ups.[52] Also in August 2020, the government launched a National Strategy for Artificial Intelligence aimed at guiding the development of AI through to 2045.[53] The strategy foreshadows a focus on applying AI to social services, education and research, health services, food security, mobility, smart cities and public-sector reform.[54]

China looks set to make a large contribution to the development of Indonesia's digital economy. Following India's implementation of rules to restrict Chinese takeovers in early 2020, Chinese venture-capital and tech investors have switched their focus to Indonesia, contributing to a 55% surge in investment in the country's tech sector in the first half of 2020.[55] Huawei has forged links with several Indonesian government agencies to help accelerate their digitisation, including through cloud-based infrastructure for storing national data.[56] Besides offering its technology, Huawei has committed to nurture digital talent and boost cyber-security skills in the country.[57] In January 2021, China and Indonesia signed a memorandum of understanding on cooperation and investment in the ICT sector, with a focus on security.[58] While Chinese companies have a large slice of the Indonesian market, they face competition from well-established US, Japanese and European firms. For example, early in 2021, Microsoft announced plans to provide training in digital skills for an additional 3m Indonesians, continuing a commitment in that area that has already lasted for more than 25 years. The initiative is based on a shared project with the Ministry of Communication and Information Technology and four universities, aimed at educating Indonesians in AI, cyber security and data science through a digital-literacy curriculum.[59]

Cyber security and resilience

Indonesian views on cyber security were strongly influenced by the 2013 Edward Snowden leaks about Australia's cyber capabilities, including its monitoring of Indonesia's leaders. Though the country's security agencies were already aware of Australia's espionage activity to some degree, the revelations were a shock to the Indonesian public. The government's response has included the Secretariat General of the National Resilience Council drawing up a national contingency plan against cyber attacks in 2016,[60] and cyber-emergency exercises such as the drill conducted by the national CERT ahead of the 2018 Asian Games in Jakarta.[61] Indonesian specialists have identified high-priority assets that need the strongest protection, including telecommunications and banking networks, online-payment systems and key government, military and private-sector closed networks and data centres.[62] The country's basic cyber defences and incident-response capability are still not highly developed, however.

Indonesia experienced a sixfold increase in cyber attacks between January and October 2020, with its e-commerce firms the major targets. Tokopedia suffered an attack that caused the personal data of 91m users to be leaked, while Bhinneka announced that 1.2m of its accounts had been accessed by hackers.[63] According to a survey by Palo Alto Networks, 84% of Indonesian companies plan to increase their IT budgets, of which

44% intend to allocate more than half of those funds to cyber-security investment.[64]

Apart from launching a public consultation on the new cyber-security strategy in 2020, the government has been pursuing a raft of additional reforms. In February 2021 the BSSN launched a national Computer Security Incident Response Team (CSIRT) that will also serve as the national and the government CSIRT.[65] Fifteen lower-level CSIRTs[66] had already been established in 2020,[67] and the government aims to set up another 27 across its ministries and other public-sector bodies in 2021.[68] In 2020 the BSSN participated in several cyber drills,[69] and in early 2021 it took part in training events on Internet of Things security-testing that were jointly organised with the United States Embassy and Carnegie Mellon University.[70] The BSSN is working with several government agencies in preparing a Draft Presidential Regulation on Vital Information Infrastructure Protection, which will cover the designation of strategic sectors and measures to protect critical information infrastructure, increase cyber readiness and accelerate recovery from cyber incidents.[71] The BSSN has also engaged all relevant owners and operators to ensure their familiarity with the regulations and policies concerning the country's critical information infrastructure.[72]

Despite ambitious policy declarations, Indonesia suffers from a severe shortage of cyber skills. A 2016 study by Oxford University found that the country lacked 'minimal educational programmes in cybersecurity', 'accreditation in cybersecurity education' and a 'national budget to support the cybersecurity capacity programmes'; that there were 'few professional instructors in cybersecurity'; and that knowledge transfer from trained cyber-security employees in the private sector existed only 'on an ad hoc basis'.[73] In 2020, commenting on the national skills shortage, the head of the BSSN reported that typically it took six months for the organisation to fill a cyber-security position.[74] It might therefore take Indonesia two decades or more to develop a sovereign capability for military cyber defence, given the number of sensitive posts requiring cyber expertise that would be needed.

Given that Indonesia is a nation of islands, maritime cyber security is of particular importance. The BSSN has been working on increasing the cyber-security capacity of the Maritime Information Centre.[75] The Indonesian Navy has carried out cyber-defence training since 2016, including a major eight-day exercise in 2018[76] that involved more than 500 personnel and had three main aspects: denial, countermeasures and cyber support for operations.[77] In 2019 the navy added a cyber dimension to its largest annual exercise, *Armada Jaya*.

In the International Telecommunication Union's 2018 Global Cybersecurity Index, Indonesia was ranked 41st out of 175 countries, a low position relative to its wealth and economic ambition.[78]

Global leadership in cyberspace affairs

Since about 2005 the Indonesian government has worked within the frameworks of the Association of Southeast Asian Nations (ASEAN), the ASEAN Regional Forum, the Asia-Pacific Economic Cooperation, the United Nations and the Organisation of Islamic Cooperation (OIC) on various aspects of fighting cyber crime, especially cyber terrorism, and on efforts to build international governance frameworks to promote strategic stability in cyberspace through discussion of cyber norms.

Indonesian specialists who had set up the country's first private CERT worked with Australian and Japanese counterparts to set up the Asia-Pacific CERT (APCERT) in 1998. Indonesia is also a member of the OIC's CERT, of which it became deputy chair in 2018,[79] and has participated in international cyber exercises such as the China–ASEAN Network Security Emergency Response Capacity Building Seminar in 2018.[80] In 2019 Indonesia joined the UN's Group of Governmental Experts[81] on cyber norms, and since 2015 it has staged an annual international cyber conference, CodeBali.[82] In 2020 it participated in the G20 Digital Economy Ministers Meeting that issued a wide-ranging development agenda in the sector, including many security aspects. It has collaborated with China in fighting cyber crime, including by deporting hundreds of Chinese citizens alleged to have been conducting attacks from Indonesia against targets in China.

Offensive cyber capability

Indonesia has reasonably well-developed capabilities for domestic cyber surveillance. For example, a special counter-terrorism unit in the police, Detachment 88, has

been building its cyber-surveillance capabilities with the support of international partners such as Australia.[83]

The available information on any wider offensive cyber capability is patchy, but it suggests Indonesia is weakly positioned to use cyber means to respond during any crisis or period of hostility. The prospect of Indonesia catching up with the offensive cyber capabilities of the states of particular interest to it – such as Australia, China, Malaysia and Vietnam – seems a distant one.

Notes

1 Yudhistira Nugraha, 'The future of cyber security capacity in Indonesia', Oxford Internet Institute, 2016, https://ora.ox.ac.uk/objects/uuid:70392ace-4bd6-4066-818e-a3adc1eeedf3.

2 Its full name is the Indonesia Security Incident Response Team on Internet and Infrastructure/Coordination Center (ID-SIRTII/CC). See 'History Id-SIRTII/CC', https://idsirtii.or.id/en/page/history-id-sirtii-cc.html.

3 Leonardus K. Nugraha and Dinita A. Putri, 'Mapping the Cyber Policy Landscape: Indonesia', Global Partners Digital, November 2016, pp. 14–15, https://www.gp-digital.org/wp-content/uploads/2017/04/mappingcyberpolicy_landscape_indonesia.pdf.

4 Badan Siber Dan Sandi Negara. See https://bssn.go.id/tentang.

5 More precisely, the BSSN took on the responsibilities of the National Crypto Agency, the Security Incident Response Team on Internet and Infrastructure, and the Information Security Directorate of the Ministry of Communication and Information Technology.

6 Marguerite Afra Sapiie, 'Police Playing Tough in Combating Cybercrimes in Indonesia', *Jakarta Post*, 6 February 2017, https://www.thejakartapost.com/news/2017/02/06/police-playing-tough-in-combating-cybercrimes-in-indonesia-.html.

7 'Kemhan Dorong Pertahanan Nirmiliter Jadi Program Nasional', Antara, 8 May 2019, https://www.antaranews.com/berita/860413/kemhan-dorong-pertahanan-nirmiliter-jadi-program-nasional.

8 Badan Siber Dan Sandi Negara, 'Indonesian Cyber Security Strategy', https://bssn.go.id/strategi-keamanan-siber-nasional.

9 Cabinet Secretariat of the Republic of Indonesia, 'Cyber Crime Directorate Established to Combat Fake News', 4 October 2018, https://setkab.go.id/en/cyber-crime-directorate-established-to-combat-fake-news.

10 Badan Siber Dan Sandi Negara, 'Strategi Keamanan Siber Nasional', 14 December 2020, https://cloud.bssn.go.id/s/qQZmyWaFf8ooc26/download.

11 Karis Kuniaran, 'Ini Strategi BSSN Perkuat Keamanan Siber Nasional', Merdeka, 14 December 2020, https://www.merdeka.com/peristiwa/ini-strategi-bssn-perkuat-keamanan-siber-nasional.html.

12 Usman Hamid and Ary Hermawan, 'Indonesia's Shrinking Civic Space for Protests and Digital Activism', Carnegie Endowment for International Peace, 17 November 2020, https://carnegieendowment.org/2020/11/17/indonesia-s-shrinking-civic-space-for-protests-and-digital-activism-pub-83250.

13 Thomas Paterson, 'Indonesian cyberspace expansion: A double-edged sword', *Journal of Cyber Policy*, vol. 4, no. 2, 2019, pp. 216–34, https://www.tandfonline.com/doi/pdf/10.1080/23738871.2019.1627476?needAccess=true.

14 *Ibid*., p. 217.

15 Peraturan Menteri Pertahanan Republik Indonesia, Nomor 82 tahun 2014 tentang, Pedoman Pertahanan Siber, https://www.kemhan.go.id/pothan/wp-content/uploads/2016/10/Permenhan-No.-82-Tahun-2014-tentang-Pertahanan-Siber.pdf.

16 Defence Ministry of the Republic of Indonesia, 'Defence White Paper 2015', November 2015, p. 109, https://www.kemhan.go.id/wp-content/uploads/2016/05/2015-INDONESIA-DEFENCE-WHITE-PAPER-ENGLISH-VERSION.pdf.

17 *Ibid*., p. 110.

18 *Ibid*., p. 45.

19 'Kemhan Dorong Pertahanan Nirmiliter Jadi Program Nasional', Antara.

20 Satsiber, 'Sejarah', https://satsiber-tni.mil.id/sejarah-20181230304.

21 Sri Hidayati and Rudi A.G. Gultom, 'Analisis Kebutuhan Senjata Siber Dalam Meningkatan Pertahanan Indonesia Di Era Peperangan Siber', *Teknologi Persenjataan*, vol. 1, no. 1, 2020, p. 90, http://139.255.245.7/index.php/TPJ/article/viewFile/474/451.

22 'Jokowi Strengthens Role of Cyber Agency', *Tempo*, 3 January 2018, https://en.tempo.co/read/914520/jokowi-strengthens-role-of-cyber-agency.

23 Badan Siber Dan Sandi Negara, 'Pimpinan Badan Siber Dan Sandi Negara', https://bssn.go.id/pejabat.

24 Mehda Basu and Yun Xuan Poon, 'Five steps in Indonesia's cyber battle plan: Interview with Lieutenant General (ret) Hinsa Siburian, Head of the National Cyber and Encryption Agency (BSSN),

Indonesia', GovInsider, 17 September 2020, https://govinsider.asia/security/bssn-five-steps-in-indonesias-cyber-battle-plan.

25 Tentara Nasional Indonesia

26 TNI, 'Organizational Structure', https://int.tni.mil.id/struktur.html. See also Sekretariat Kabinet Republik Indonesia, 'Inilah Perpres No. 62 Tahun 2016 Tentang Susunan Organisasi Tentara Nasional Indonesia (1)', 19 January 2017, https://setkab.go.id/inilah-perpres-no-62-tahun-2016-tentang-susunan-organisasi-tentara-nasional-indonesia-1.

27 The Satsiber unit within the Indonesian Air Force was formally inaugurated only in September 2020. See Achmad Nasrudin Yahya, 'Bentuk Peperangan Makin Tak Dapat Diprediksi, TNI AU Bentuk Satuan Siber', *Kompas*, 17 September 2020, https://nasional.kompas.com/read/2020/09/17/07393261/bentuk-peperangan-makin-tak-dapat-diprediksi-tni-au-bentuk-satuan-siber.

28 Pushansiber. See Kementerian Pertahanan Republik Indonesia, 'Kapushansiber', https://www.kemhan.go.id/bainstrahan/kapushansiber.

29 See Kementerian Pertahanan Republik Indonesia, 'Badan Instalasi Strategis Pertahanan', https://www.kemhan.go.id/bainstrahan.

30 Alex Firmansiyah Rahman, Syaiful Anwar and Arwin Datumaya Wahyudi Sumari, 'Analisis Minimum Essential Force (MEF) Dalam Rangka Pembangunan Cyber-Defense', *Jurnal Pertahanan & Bela Negara*, vol. 5, no. 3, 2018, pp. 63–85, http://jurnal.idu.ac.id/index.php/JPBH/article/view/370.

31 Margareth S. Aritonang, 'Police to Support National Cyber Agency', *Jakarta Post*, 4 January 2017, https://www.thejakartapost.com/news/2017/01/04/police-to-support-national-cyber-agency.html.

32 Badan Intelijen Strategis

33 'DPR "Ngotot" Perjuangkan Dana Rp20 Triliun Untuk BSSN', CNN Indonesia, 13 November 2019, https://www.cnnindonesia.com/teknologi/20191113191757-185-448102/dpr-ngotot-perjuangkan-dana-rp20-triliun-untuk-bssn.

34 *Ibid*.

35 European Center for Digital Competitiveness, 'Digital Riser Report 2020', September 2020, https://digital-competitiveness.eu/wp-content/uploads/ESCP_Digital-Riser-Report_2020-1.pdf.

36 *Ibid*., p. 7.

37 'e-Conomy SEA 2020 – At full velocity: Resilient and racing ahead', Google, Temasek, Bain & Company, November 2020, p. 32, https://www.thinkwithgoogle.com/_qs/documents/10614/e-Conomy_SEA_2020_At_full_velocity__Resilient_and_racing_ahead_bMmKO5b.pdf.

38 For Gojek and Tokopedia valuations, see 'Indonesia's Gojek Mulls $18 Billion Merger With Tokopedia', PYMTS.com, 5 January 2021, https://www.pymnts.com/news/partnerships-acquisitions/2021/indonesias-gojek-mulls-18-billion-merger-with-tokopedia. For a Traveloka valuation, see Yoolim Lee, 'Traveloka Nears Fundraising at Lower Valuation', Bloomberg Quint, 10 July 2020, https://www.bloombergquint.com/business/traveloka-is-said-near-fundraising-at-sharply-lower-valuation.

39 Fauziah Rizki Yuniarti, 'Indonesia could be Asia's next Islamic finance hub', *Jakarta Post*, 12 January 2021, https://www.thejakartapost.com/academia/2021/01/12/indonesia-could-be-asias-next-islamic-finance-hub.html.

40 Eisya A. Eloksari, 'Indonesian internet users hit 196 million, still concentrated in Java: APJII survey', *Jakarta Post*, 11 November 2020, https://www.thejakartapost.com/news/2020/11/11/indonesian-internet-users-hit-196-million-still-concentrated-in-java-apjii-survey.html.

41 *Ibid*.

42 'Indonesian Internet Users Reach 200 Million Until 2Q of 2020', The Insider Stories, 10 November 2020, https://theinsiderstories.com/indonesian-internet-users-reach-200-million-until-2q-of-2020.

43 'Global Innovation Index 2020: Who Will Finance Innovation?', SC Johnson College of Business – Cornell University, INSEAD and WIPO, September 2020, p. 17, https://www.globalinnovationindex.org/Home.

44 Vience Mutiara Rumata and Ashwin Sasongko Sastrosubroto, 'The Paradox of Indonesian Digital Economy Development', IntechOpen, 27 May 2020, https://www.intechopen.com/online-first/the-paradox-of-indonesian-digital-economy-development.

45 'Incar Jawara Dunia, Inilah Strategi RI Dalam Ekonomi Digital', Kementerian Komunikasi dan Informatika Republik Indonesia, November 2018, http:///content/detail/15306/incar-jawara-dunia-inilah-strategi-ri-dalam-ekonomi-digital/0/sorotan_media.

46 Trisha Ray et al., 'The Digital Indo-Pacific: Regional Connectivity and Resilience', Quad Tech Network, ANU, CNAS, GRIPS, ORF, February 2021, p. 17, https://crawford.anu.edu.au/sites/default/files/publication/nsc_crawford_anu_edu_au/2021-02/thedigitalindopacific.pdf.

47 Eileen Yu, 'Cloud, Data amongst APAC Digital Skills Most Needed', ZDNet, 25 February 2021, https://www.zdnet.com/article/cloud-data-amongst-apac-digital-skills-most-needed/.

48 Coordinating Ministry for Political, Legal and Security Affairs, 'Tingkatkan Keamanan Informasi Nasional, Deputi VII Kominfotur Laksanakan FGD Merevival Kedaulatan Telekomunikasi', 27 June 2019, https://polkam.go.id/tingkatkan-keamanan-informasi-nasional-deputi-vii-kominfotur-laksanakan.

49 'UI Gandeng Tokopedia Bangun Pusat Penelitian Kecerdasan Buatan, Menristekdikti Harapkan Lulusan Indonesia Penuhi Kebutuhan SDM Perusahaan Startup', Ristek-Brin, 28 March 2019, https://www.ristekbrin.go.id/ui-gandeng-tokopedia-bangun-pusat-penelitian-kecerdasan-buatan-menristekdikti-harapkan-lulusan-indonesia-penuhi-kebutuhan-sdm-perusahaan-startup.

50 Arya Dipa, 'Bukalapak, ITB Launch AI, Cloud Computing Innovation Center', *Jakarta Post*, 2 February 2019, https://www.thejakartapost.com/news/2019/02/02/bukalapak-itb-launch-ai-cloud-computing-innovation-center.html.

51 Dylan Loh, 'ASEAN Faces Wide AI Gap as Vietnam and Philippines Lag Behind', *Nikkei Asia*, 9 October 2020, https://asia.nikkei.com/Business/Technology/ASEAN-faces-wide-AI-gap-as-Vietnam-and-Philippines-lag-behind2.

52 Hugh Harsono, 'Why Indonesia Is Poised to Become the Next AI Start-up Hub', *South China Morning Post*, 25 August 2020, https://www.scmp.com/tech/article/3098596/why-indonesia-poised-become-next-ai-start-hub.

53 Indonesia National Secretariat of Artificial Intelligence, 'Indonesia National Strategy for Artificial Intelligence', 10 August 2020, https://ai-innovation.id/strategi.

54 *Ibid*.

55 Mercedes Ruehl, 'China's Tech Investors Turn from India to Indonesia', *Financial Times*, 29 November 2020, https://www.ft.com/content/bcc935fd-ef40-4d6d-9939-ea18498e0283.

56 'Cybersecurity Becomes BSSN's Challenge in the Digitalization of Indonesia', Waktunya Merevolusi Pemberitaan, 28 August 2020, https://voi.id/en/technology/12457/cybersecurity-becomes-bssns-challenge-in-the-digitalization-of-indonesia.

57 The Huawei ASEAN Academy reportedly comprises business, technical and engineering colleges with 100 trainers, more than 3,000 courses and more than 100 mirroring environments.

58 Chris Devonshire-Ellis, 'Investment Infrastructure Projects in Indonesia Contributing to Improved Manufacturing Capability', ASEAN Briefing, 4 February 2021, https://www.aseanbriefing.com/news/investment-infrastructure-projects-in-indonesia-contributing-to-improved-manufacturing-capability.

59 'Microsoft to Establish First Datacenter Region in Indonesia as Part of Berdayakan Ekonomi Digital Indonesia Initiative', Microsoft Stories Asia, 25 February 2021, https://news.microsoft.com/apac/2021/02/25/microsoft-to-establish-first-datacenter-region-in-indonesia-as-part-of-berdayakan-digital-economy-indonesia-initiative/.

60 Arif Rahman and Oktarina Paramitha Sandy, 'Ini Urgensi UU Keamanan dan Ketahanan Siber' [interview with Colonel Arwin Datumaya Wahyudi Sumari], Cyberthreat.id, 26 April 2019, https://cyberthreat.id/read/305/Ini-Urgensi-UU-Keamanan-dan-Ketahanan-Siber.

61 Asia Pacific Computer Emergency Response Team, 'APCERT Annual Report 2018', p. 125, http://www.apcert.org/documents/pdf/APCERT_Annual_Report_2018.pdf.

62 Achmad Rouzni Noor, 'Strategi Indonesia Menjaga Kedaulatan Cyber', detikinet, 1 February 2016, https://inet.detik.com/cyberlife/d-3131768/strategi-indonesia-menjaga-kedaulatan-cyber.

63 'Covid-19 and Cyberattacks: Which Emerging Markets and Sectors Are Most at Risk?', Oxford Business Group, 17 February 2021, https://oxfordbusinessgroup.com/news/covid-19-and-cyberattacks-which-emerging-markets-and-sectors-are-most-risk.

64 Eisya A. Eloksari, 'Indonesian Businesses Ramp up Cybersecurity Budget amid Rampant Attacks', *Jakarta Post*, 23 July 2020, https://www.thejakartapost.com/news/2020/07/22/indonesian-businesses-ramp-up-cybersecurity-budget-amid-rampant-attacks.html.

65 'Kepala BSSN Resmikan Tim Tanggap Insiden Keamanan Siber (BSSN-CSIRT) Demi Tercipta Ruang Siber Yang Aman Dan Kondusif', Badan Siber Dan Sandi Negara, 25 February 2021, https://bssn.go.id/kepala-bssn-resmikan-tim-tanggap-insiden-keamanan-siber-bssn-csirt-demi-tercipta-ruang-siber-yang-aman-dan-kondusif/.

66 In 2020 the BSSN established CSIRTs in institutions including the Ministry of Finance and the Ministry of Education and Culture, and in provinces including Central Java, East Java, Gorontalo, Jakarta, the Riau Islands, West Java and West Sumatra. See 'BSSN Gandeng Pemprov DKI Jakarta Bentuk Tim Tanggap Insiden Keamanan Siber', Badan Siber Dan Sandi Negara, 23 December 2020, https://bssn.go.id/bssn-gandeng-pemprov-dki-jakarta-bentuk-tim-tanggap-insiden-keamanan-siber; and 'Resmikan Jogjaprov CSIRT, BSSN Harap Bisa Tekan Ancaman Siber di Yogyakarta', KOMPAS.com, 15 October 2020, https://biz.kompas.com/read/2020/10/15/133036728/resmikan-jogjaprov-csirt-bssn-harap-bisa-tekan-ancaman-siber-di-yogyakarta.

67 'Resmi Dibentuk, Kemenkeu-CSIRT Menutup Program Prioritas Strategis BSSN Di Tahun 2020', Badan Siber Dan Sandi Negara, 29 December 2020, https://bssn.go.id/resmi-dibentuk-kemenkeu-csirt-menutup-program-prioritas-strategis-bssn-di-tahun-2020.

68 *Ibid.*

69 These drills include the ITU Cyber Drill Exercise 2020, ASEAN Cert Incident Drill 2020, OIC Cert Cyber Drill 2020, Critical Information Infrastructure Cyber Exercise 2020, ASEAN Japan Cyber Exercise 2020 and APCERT Drill 2020. See Id-SIRTII/CC, 'Activity', 2020, https://idsirtii.or.id/en/activity/year/2020.html.

70 'APCERT Training: Implementing IoT Security Testing', ID-SIRTII/CC, 23 February 2021, https://idsirtii.or.id/en/activity/detail_year/2021/92/apcert-training-implementing-iot-security-testing.html; and 'Carnegie Mellon University: Unhide Hidden Cobra', ID-SIRTII/CC, 15 February 2021, https://idsirtii.or.id/en/activity/detail_year/2021/94/carnegie-mellon-university-unhide-hidden-cobra.html.

71 'BSSN Beserta 13 Lembaga Pemerintah Formulasikan Rancangan Perpres Perlindungan Infrastruktur Informasi Vital', Badan Siber Dan Sandi Negara, 10 February 2021, https://bssn.go.id/bssn-beserta-13-lembaga-pemerintah-formulasikan-rancangan-perpres-perlindungan-infrastruktur-informasi-vital.

72 'BSSN Gelar Diseminasi Peraturan dan Kebijakan Sektor Infrastruktur Informasi Kritikal Nasional (IIKN)', Badan Siber Dan Sandi Negara, 10 February 2021, https://bssn.go.id/bssn-gelar-diseminasi-peraturan-dan-kebijakan-sektor-infrastruktur-informasi-kritikal-nasional-iikn.

73 Nugraha, 'The future of cyber security capacity in Indonesia', pp. 12, 55.

74 Basu and Yun, 'Five steps in Indonesia's cyber battle plan: Interview with Lieutenant General (ret) Hinsa Siburian, Head of the National Cyber and Encryption Agency (BSSN), Indonesia'.

75 'BSSN Menerima Kunjungan Bakamla Dalam Rangka Kerjasama Keamanan Informasi', Badan Siber Dan Sandi Negara, 4 February 2021, https://bssn.go.id/bssn-menerima-kunjungan-bakamla-dalam-rangka-kerjasama-keamanan-informasi.

76 TNI, 'TNI AL Tingkatkan Kemampuan Pertahanan Siber', 6 November 2018, https://tni.mil.id/view-140439-tni-al-tingkatkan-kemampuan-pertahanan-siber.html.

77 Satsiber, 'Gubernor Aaal Hadiri Latihan Operasi Pertahanan Siber TNI AL 2018', 12 December 2018, https://satsiber-tni.mil.id/gubernur-aal-hadiri-latihan-operasi-pertahanan-siber-tni-al-2018-20181212674.

78 International Telecommunication Union, 'Global Cybersecurity Index 2018', p. 58, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

79 Asia Pacific Computer Emergency Response Team, 'APCERT Annual Report 2018', p. 128.

80 *Ibid.*, p. 88.

81 Since a UN General Assembly resolution in 2004, a UN Group of Governmental Experts (GGE) has convened for two-year terms to address international-security aspects of cyberspace. It was known as the GGE on 'Developments in the Field of Information and Telecommunications in the Context of International Security' until 2018, when it was renamed the GGE on 'Advancing Responsible State Behaviour in Cyberspace in the Context of International Security'. In cyberspace-policy circles it is common to refer to it simply as 'the GGE'. See UN Office for Disarmament Affairs, 'Developments in the field of information and telecommunications in the context of international security', https://www.un.org/disarmament/ict-security.

82 See 'CodeBali International Cyber Security Conference and Exhibitions' website, https://codebali.id.

83 Muhammad Nadjib and Hafied Cangara, 'Cyber Terrorism Handling in Indonesia', *Business and Management Review*, vol. 9, no. 2, November 2017, pp. 278–9, https://cberuk.com/cdn/conference_proceedings/conference_30092.pdf.