10. Singapore

As a world leader in digital transformation, Singapore has developed sound civilian cyber policies and moved with considerable determination to build a robust cyber-security architecture. Domestically, the city-state has very strong digital-surveillance capabilities, and in 2022 it established a fourth military service, the Digital and Intelligence Service (DIS). Cyber command-and-control arrangements lie primarily with the cabinet and are divided between the Cyber Security Agency (CSA) of Singapore (for the civilian sector) and the DIS (for the military realm). Singapore's cyber-intelligence capabilities are a judicious mix of home-grown talent development and procurement of foreign technologies and services. The republic's strong digital economy is underpinned by substantial public investments, strong political will and robust infrastructure. Motivated by the 2018 data breach of its healthcare institutions, Singapore has since adopted an 'assume-breach' posture that is accompanied by a suite of comprehensive cyber-security policies ranging from talent development and R&D to fostering tighter cooperation with critical information infrastructure stakeholders. Through active participation and leadership in various platforms for international cyberspace affairs, Singapore has demonstrated strong commitment to promote the implementation of norms and international law in cyberspace amidst rising geopolitical tensions. The republic does not publicly acknowledge it possesses offensive cyber capabilities, but these are likely to exist at a basic level. Though Singapore has punched above its weight in several areas, we assess it to be a third-tier cyber power largely because of its relatively small-scale cyber capabilities.

Strategy and Doctrine

The government's Infocomm Security Masterplan released in 2005 was a world-leading effort and formed a solid base for subsequent adjustments in cyber policy.[1] In 2015, the CSA, newly established under the Prime Minister's Office, took responsibility for Singapore's cyber security. The agency published its first Cybersecurity Strategy in 2016 and released the Cybersecurity Strategy 2021 five years later.[2] The updated strategy took a more proactive stance to address threats, to simplify cyber security for end-users, as well

List of Acronyms

C4I	Command, Control, Communications, Computers and Intelligence
CCoP	Cybersecurity Codes of Practice
CDG	Cyber Defence Group
CISS	Critical Infrastructure Security Showdown
CSA	Cyber Security Agency
CSTF	Cybersecurity Task Force
DCO	Defence Cyber Organisation
DDC	Digital Defence Command
DIS	Digital and Intelligence Service
DOTC	Digital Ops-Tech Centre
DSO	Defence Science Organisation
DSTA	Defence Science and Technology Agency
DTC	DIS Training Command
GFCE	Global Forum on Cyber Expertise
IGCI	INTERPOL Global Complex for Innovation
ISD	Internal Security Department
iSSWG	Online Industry Safety and Security Watch Group
JDCD	Joint Digital and C4 Department
JIC	Joint Intelligence Command
JID	Joint Intelligence Directorate
MHA	Ministry of Home Affairs
MINDEF	Ministry of Defence
MSD	Military Security Department
OT	Operational Technology
SAF	Singapore Armed Forces
SAFC4COM	SAF C4 Command
SICW	Singapore International Cyber Week
SID	Security and Intelligence Division
TRM	Technology Risk Management
WLS	Work-Learn Scheme

as to build deeper partnerships for the government with industry, providers of essential services, the workforce and academia.[3] The strategy laid out three pillars: building a resilient infrastructure; enabling a safer cyberspace; and enhancing international cyber cooperation. The document also listed two foundational enablers in developing a vibrant cyber-security ecosystem and growing a robust cyber-talent pipeline. Cybersecurity Strategy 2021 deemed as challenges the following: risks from emerging and disruptive technologies; cyber-physical risks;[4] expansion of attack surfaces resulting from ubiquitous digital connectivity; and increasing geopolitical tensions in cyberspace.[5] Various masterplans have been built on the Cybersecurity Strategy to implement and operationalise its priorities.[6] Excluded from the strategy's purview is disinformation which is covered under the Protection from Online Falsehoods and Misinformation Act 2019.[7] The latter seeks to counter foreign interference in domestic politics through hostile information campaigns and local proxies.[8]

While no cyber strategy specific to the military domain has been published, statements by the Ministry of Defence (MINDEF) and organisational changes indicate the growing role of the Singapore Armed Forces (SAF) in defending against foreign cyber threats. MINDEF has indicated that military use of cyber capabilities is purely defensive.[9] Defending SAF networks had been part of the responsibility of the SAF Command, Control, Communications, Computers and Intelligence (C4I) community established in 2012. However, the significant growth in state-based cyber threats against military and defence organisations, manifested in the targeted breach of MINDEF's I-net system in March 2017,[10] prompted the establishment of the Defence Cyber Organisation (DCO) at the MINDEF level the same year.[11] The DCO represents Singapore's first effort to centralise defence against cyber threats across various entities in the republic's defence edifice. To bolster the defence of military networks, the SAF inaugurated in 2017 the Command, Control, Communications, Computers (C4) Command that integrated the existing C4 Operations Group (part of SAF C4I) with a newly created Cyber Defence Group (CDG). Even though it is part of the SAF, the CDG reports to the DCO on long-term capability development in cyber defence.[12]

By the end of 2020, a Cybersecurity Task Force (CSTF) was established within the SAF under the Chief of C4I to centralise command and control of cyber-security operations across the defence sector. In 2022, the C4I community was restructured to form the new DIS.[13] With the creation of this dedicated cyber force in 2022, its mission was described as 'defend and dominate' with the latter word definitely invoking the prospect of offensive operations.[14] The evolving international cyber-threat environment had largely shaped Singapore's decision to establish the DIS. In a parliamentary speech in early 2022, the republic's defence minister noted that the establishment of the dedicated digital force was necessary to deal with external threats that were expected to 'grow in numbers, sophistication, and organisation'.[15] While Singapore has not detected any campaign in the digital domain that could undermine its national security and sovereignty, the establishment of the DIS could act as a deterrent against potential threat actors.[16] Beyond cyber threats, the service is also responsible for protection against electronic attacks on the SAF's combat capabilities and psychological defence against the use of disinformation in warfare.[17]

The mission of Singapore's new digital service: 'defend and dominate'

In 2023, the government identified the Russian war in Ukraine as one of several aggravating factors in the global cyber scene that was driving the government to serious adjustments in its cyber posture.[18] These adjustments included the establishment in 2022 of a Counter Ransomware Task Force chaired by CSA and bringing together the expertise and resources of key government agencies.[19]

Singapore has also stepped up its use of advanced technology to boost domestic security in cyberspace. The Home Team Science and Technology Agency, formed under the Ministry of Home Affairs (MHA) in 2019, develops technologies including cyber security, data science and AI, as well as digital and information forensics. Data science and AI, for instance, have been deployed in

policing and counter-terrorism operations.[20] The Online Industry Safety and Security Watch Group (iSSWG) is a collaboration between the Singapore Police Force and the Asia Internet Coalition, which comprises tech companies including Amazon, Apple, Google, Grab and Meta. Among other responsibilities, the Online iSSWG promotes relevant and timely data exchange between tech firms and the police to counter terrorism on digital platforms and other online security threats.[21] These capabilities provide a foundation for wider political surveillance than counter-terrorism needs would warrant.

Overall, Singapore's strategy against cyber and information threats is encapsulated in the term 'Digital Defence' that was introduced in 2019 as the sixth pillar of the 'Total Defence' concept.[22] Its strong cyber-security architecture is underpinned by close cooperation among various national agencies such as the DIS, MHA and CSA.

Governance, Command and Control

The CSA is the central body that oversees and coordinates all aspects of national cyber security, including developing and enforcing regulations, policies and practices in the field.[23] The agency also supervises the protection of critical information infrastructure (CII) sectors that support delivery of essential services. These sectors are banking and finance; energy; government; healthcare; information and communications; media; security and emergency services; transport (land, maritime and aviation domains), as well as water. In addition, the CSA monitors cyberspace for threats through the Singapore National Computer Emergency Response Team (SingCERT), and this entity collaborates with local and international CERTs to facilitate detection, resolution and prevention of cyber-security threats.[24] In the event of large-scale cyber incidents affecting multiple CII sectors, the CSA would act as the lead coordinator of cross-sector incident response at the national level. It would also deploy National Cyber Incident Response Teams to assist affected CII sectors.[25] Empowered by the Cybersecurity Act 2018, the CSA regulates CII owners through measures including codes of practice, frameworks for information sharing and licensing frameworks for cyber-security service providers.[26]

The chief executive of CSA is concurrently the commissioner of cyber security, who is responsible for the designation of specific computers or computer systems as CII and coordination of responses of the CII sectors when there is a cyber incident.[27] In addition, the CSA spearheads various policies to create a safer cyberspace for enterprises and individual end-users. The agency is also commissioned to strengthen the cyber-security profession, promote research and innovation of cyber-security technologies, facilitate international cooperation to shape norms of responsible state behaviour in cyberspace and build regional cyber-security capacity within the Association of Southeast Asian Nations (ASEAN).

Command and control of military cyber capabilities lies with the DIS chief, who is also the director of military intelligence. The director is supported by the service's chief of staff and chief expert, and is responsible for driving mission outcomes in the DIS.[28] The service comprises three main entities. One consists of the Joint Intelligence Directorate (JID), Joint Digital and C4 Department (JDCD) and Cyber Staff. Another comprises four commands: the Joint Intelligence Command (JIC); SAF C4 Command/Cybersecurity Taskforce (SAFC4COM/CSTF); Digital Defence Command (DDC); and the DIS Training Command (DTC). Finally, there is a separate Digital Ops-Tech Centre (DOTC). The DIS is also responsible for raising, training and sustaining digital forces and capabilities.[29]

Retaining the previous functions of the SAF C4I, the JID works with other armed services intelligence entities and the JIC to support MINDEF/SAF's decision-making.[30] Specifically, the JIC supports MINDEF/SAF intelligence requirements by providing early warning and operational intelligence. The JDCD leads in the digitalisation of the SAF towards its goal to operate as a networked force. The Cyber Staff sets cyber-defence strategies and policies to coordinate cyber security across the defence sector. Similarly, the SAFC4COM/CSTF operates and defends C4 capabilities for MINDEF/SAF.[31] In addition, the development of electronic-protection and psychological-defence capabilities will be carried out by the Electronic Protection Group and Psychological Defence Group, respectively, in the DDC. Lastly, the DOTC functions as a centre of excellence of digital expertise that would train experts to develop digital products and solutions to meet changing operational requirements.[32]

To institutionalise cyber-security collaboration between military and civilian agencies, the DIS and CSA signed a Joint Operations Agreement in November 2022. The agreement established a framework for collaboration in joint operations and capability development, reinforcing Singapore's collective approach for cyber incidents and emergencies.[33]

On the whole, Singapore has developed a robust cyber governance structure for civilian and military sectors, though command and control of cyber capabilities in the civilian sector is far more developed than in the military realm.

Core Cyber-intelligence Capability

Little is known in public about Singapore's cyber-intelligence capabilities. The Internal Security Department (ISD) in the MHA specialises in addressing threats to internal security and stability, including using all available means to monitor foreign subversive elements, spies as well as racial and religious extremists and terrorists.[34] The department leverages advanced technologies such as biometrics and AI to boost its cyber-intelligence capabilities. The job description of cyber and technology officers in the ISD indicates a range of opportunities in biometrics, cyber intelligence and security, data science, ICT security and software development, among others.[35] It is likely that the ISD relies heavily for its signals interception technologies on foreign cyber-intelligence firms.[36]

Established in 1966, the highly secretive Security and Intelligence Division (SID) is Singapore's dedicated external-intelligence unit. Its responsibilities include monitoring for various challenges including terrorism, cyber security, and geopolitical threats. One of the SID's few publicly acknowledged achievements was the disruption of a 2016 terror attack on the iconic Marina Bay Sands resort. The job descriptions of SID personnel provide some insights into their capabilities.[37] For instance, SID operations officers use technology to help them identify threats to provide early warning and situational updates. In the same vein, according to the SID website, its technology officers utilise 'diverse cutting-edge technologies to develop innovative solutions to help SID tackle challenges in its operating landscape'. In addition, public reports indicate that SID has procured tools from foreign and local cyber-intelligence firms to carry out communications interceptions.[38]

Established in 1975, the Military Security Department (MSD) is an independent body reporting directly to the permanent secretary of defence and tasked to counter espionage, subversion and sabotage against MINDEF/SAF. Like the ISD and SID, the MSD's roles also include counter-terrorism and cyber security. The job descriptions of MSD personnel provide an indication of the department's cyber-intelligence capabilities. For instance, cyber and infocomm technology security officers are responsible for roles including cyber-security monitoring, threat hunting and analysis.[39]

Within the armed forces, the DIS performs intelligence operations through the JIC. The latter is tasked to provide round-the-clock 'accurate, relevant and timely' intelligence, including during peacetime, to contribute to early warning and decision-making of SAF operations.[40] The JIC comprises two brigade-equivalent groups: the Imagery Support Group and the Counter-Terrorism Intelligence Group. The JIC works together with other intelligence entities in the armed services under the purview of the Military Intelligence Organisation.

Given the involvement of the ISD, SID, MSD and DIS in counter-terrorism, they are likely to cooperate closely for intelligence sharing. Public reports indicate SID and ISD share intelligence to deal with terrorism threats, such as the operation against the Jemaah Islamiah transnational terrorist network in the early 2000s.[41] Beyond domestic cooperation, Singapore also benefits from external cyber intelligence garnered from traditional military partnerships including the Five Power Defence Arrangements, as well as hosting multilateral initiatives like the Information Fusion Centre and Counter-Terrorism Information Facility.

While Singapore possesses some cyber-intelligence capabilities, the overall scale is small with a limited focus, and there is a heavy reliance on cooperation with international partners.

Cyber Empowerment and Dependence

Singapore is recognised globally as one of the most digitally competitive countries and a leading smart city.[42]

Its overall digital economy is expected to reach a compound annual growth rate of 19% and US$22 billion in gross merchandise value by 2025.[43] Underlying the city-state's robust digital economy is its strong connectivity foundations. For instance, smartphone penetration reached about 88% of the population in 2020,[44] and Singapore had the world's fastest median download speed for fixed broadband in early 2022.[45]

Likewise, Singapore's innovation ecosystem has placed high in global rankings. For instance, it ranked 7th in the 2022 Global Innovation Index.[46] The 2021 Bloomberg Innovation Index placed Singapore second after South Korea, citing its strengths in tertiary education and manufacturing categories.[47] In another study, Singapore was the eighth-most innovative nation globally for three consecutive years from 2019 to 2021.[48] In addition, the republic topped rankings in indicators of high-tech manufacturing and high-tech exports and attained the top position in terms of venture capital (VC) investors and recipients.[49] One of Singapore's strengths as a tech ecosystem is its ability to attract foreign tech companies to set up shop in the country. Indeed, VC and private-equity deals in Singapore reached US$16.5bn in 2021, more than three times the previous year's value.[50] By 2022, the market became quite depressed, though Singapore remained the leader in Southeast Asia.[51] The government, through the EDBI investment group, owns a global strategic investment vehicle to finance innovative tech companies.[52] Multinational companies such as Google are attracted to Singapore due to its unique geographic connectedness to developed and emerging economies.[53]

On the other hand, Singapore has performed weakly in some indicators of digital competitiveness. It scored poorly in education expenditure (117th) and software spending (50th) in the Global Innovation Index 2022.[54]

Nevertheless, Singapore's overall status as a leading digital economy can be attributed to its leaders' early recognition of technology as a key driver of economic development. Since the 1980s, Singapore has set up several technology-oriented projects, the most prominent of which being the 2014 Smart Nation initiative.[55] This endeavour seeks to harness Industry 4.0 technologies in key domains such as health, transport, urban solutions, finance and education not only to drive economic development and civic engagement, but also to address national challenges like climate change and an aging population.[56] For instance, the Smart Nation Sensor Platform launched in 2017 is a nationwide sensor network that collects and analyses data to support more efficient city planning, responsive maintenance and delivery of citizen-centric services such as transport management and public safety.[57] Other government-led digital projects include the National Digital Identity, which enables secure personal authentication for access to digital government services, and the Networked Trade Platform that acts as a one-stop trade and logistics system for the shipping sector.[58] While the use of common and open platforms in Singapore's smart-city projects creates added cyber-security risks, this could be alleviated by the city-state's security-by-design approach which accounts for security risks right from the software- or hardware-development stage.[59]

The country's main developmental challenge remains the small size of its indigenous technology resources, especially the workforce but also the scope of its industries. There are only a small number of home-grown cyber security companies, a situation driving the Singapore government to a heavy reliance on foreign corporations.

Singapore recognises artificial intelligence as one of the key new technology frontiers to drive its Smart Nation plan. In this regard, it launched the National Artificial Intelligence Strategy in 2019, underscoring its vision of becoming a global leader in AI development and deployment. The strategy identified five areas as key: transport and logistics; smart cities and estates; healthcare; education; as well as safety and security.[60] Before the AI strategy was launched, AI Singapore, a national programme in the field, was created in 2017 to bring together all locally based research institutions, start-ups, and companies to catalyse the country's AI capabilities.[61] Under the Research, Innovation and Enterprise 2020 plan, S$500 million (US$370.3m) was allocated for AI-related activities[62], and an additional S$180m (US$133.3m) was allocated in 2021 to support fundamental and translational AI research and to further support industry–research collaboration.[63] Singapore's AI research impact was evidenced in a 2022 research ranking of publications in the two most prestigious AI

research conferences, where the city-state ranked 11th, just behind Japan (10th) and Israel (9th).[64] Successful applications of AI in Singapore so far include tools to detect skin cancer, analyse chest x-rays or perform diabetes screens from a patient's retina scan.[65] Singapore's success in developing and adopting AI has been cited as a role model for US states to emulate.

Buttressed by strong political will, the republic has maintained its edge in digital economy development through sustained investments in infrastructure, manpower development as well as R&D. Future priorities will include deeper digitalisation of existing industries, government support to local companies in that transition, and transformation of the infocomm media industry into a next-generation digital industry.

Cyber Security and Resilience

As digital connectivity permeates all sectors of Singapore, the republic's cyber-threat landscape has become more complex. From 2013 to 2019, Singapore experienced several significant cyber incidents,[66] the most prominent of which was the SingHealth hack in 2018 where the largest group of healthcare institutions in Singapore had 1.5m patient records stolen.[67]

The government has responded to these rising threats through various cyber-security policies and legislation. In 2018, the Cybersecurity Act was passed with an aim of strengthening CII.[68] The act also established a framework for sharing cyber-security information[69] and a licensing framework for cyber-security service providers.[70] Cybersecurity Codes of Practice (CCoP) for CII owners were subsequently published as legally enforceable according to the act.[71] Specific to the banking and finance sectors, the Monetary Authority of Singapore issued legally binding Cyber Hygiene notices[72] to all financial institutions in 2019 alongside the Notices on Technology Risk Management (TRM) and related guidelines issued in 2013.[73]

Beyond what is mandated by law, the CSA has in recent years issued various guidelines to enhance cyber resilience. The security-by-design framework was developed in 2017 to guide CII owners to incorporate security into their systems development lifecycle process, including in 5G networks development.[74] The CSA also introduced the 2019 Operational Technology (OT) Cybersecurity Masterplan to improve the cyber-security postures of CII owners and organisations that operate OT systems.[75] As mentioned above, an inter-agency Counter Ransomware Task Force was also created in 2022 to help companies and organisations more effectively counter that threat.[76]

Singapore is quick to adapt its cyber-security posture according to the rapidly changing threat environment. In September 2021, the republic announced its shift of position from emphasising prevention of threats to assuming its IT systems have already been breached, and this is a stance that requires constant vigilance and monitoring.[77] The Cybersecurity Act is also undergoing consultations for multistakeholder review, with considerations to expand the concept of CII beyond physical networks and systems to include key digital infrastructure and key digital services.[78] Plans are under way to update the CCoP. From October 2022, companies providing cyber-security services in Singapore have been required under the Cybersecurity Act to obtain a cyber-security provider's license. This license would certify complete implementation of up-to-date cyber-security standards.[79]

Underpinning the CSA's robust threat-intelligence and operational capabilities are its active partnerships with major industry players such as FireEye, Microsoft and Palo Alto Networks.[80] The agency has partnered with the Global Cyber Alliance and homegrown cyber-security specialist Ensign InfoSecurity on an Internet of Things (IoT) threat analytics platform to gain early warning and visibility into threats arising from IoT.[81] The CSA has established partnerships with private organisations to train indigenous cyber-security talent.[82] In April 2023, the Monetary Authority of Singapore and the US Treasury conducted a joint cyber-security exercise over three days to test protocols for data exchange and incident response coordination.[83]

To enhance operational readiness of CII sectors against sophisticated threats, the CSA has been conducting sector-specific exercises dubbed *CyberArk*[84] and national-level, multisectoral exercises dubbed *Cyber Star* to validate its cyber crisis-management system.[85] In addition, the CSA is reportedly developing the next-generation National Cyber Security Centre that will enable tighter integration with CII owners and sector leads.[86]

The government actively promotes local R&D through the triple-helix collaboration model between government, academia and industry. Launched in 2013, the National Cybersecurity R&D Programme was allocated S$190m until 2020 to promote research collaboration for deepening domestic cyber-security R&D expertise.[87] Moreover, the CSA has established the Cybersecurity Co-Innovation and Development Fund to stimulate local industry innovation.[88]

In terms of military cyber defence, MINDEF/SAF adopts a multilayered strategy where networks of different security classification are physically separated. Under the SAFC4COM/CSTF, the CDG provides round-the-clock defence of SAF networks,[89] while the Integrated MINDEF/SAF Security and Network Operations Centre conducts 24/7 monitoring of networks and systems across the defence sector.[90] Adopting a proactive cyber-security stance, MINDEF/SAF has implemented innovative solutions, such as the MINDEF Bug Bounty Programme, involving local and global 'white-hat' hackers to identify vulnerabilities.

Indigenous defence innovation capabilities boost MINDEF/SAF's cyber defence. The Defence Science and Technology Agency (DSTA) and Defence Science Organisation (DSO) develop cyber-security capabilities to defend MINDEF/SAF networks.[91] For instance, the DSTA and DSO, in collaboration with the MSD, have developed the Cyber Security Operations Centre 2.0 which integrates AI techniques for automated anomaly detection, alert prioritisation and recommendation for follow-up actions.[92]

MINDEF/SAF is prioritising investments in OT cyber-defence capabilities. It has jointly established the iTrust Centre for Research in Cyber Security with the Singapore University of Technology and Design. The centre's work includes development of OT testbeds for better threat profiling and co-organisation of the Critical Infrastructure Security Showdown (CISS), a global OT cyber exercise which enables the CSTF to validate its technical and operational skills.[93] In addition, the DIS organised the inaugural two-day Critical Infrastructure Defence Exercise in November 2022, the largest national OT critical infrastructure defence exercise involving over 100 participants from the DIS and 16 other national agencies across the CII sectors.[94]

To establish a steady flow of military cyber talent, MINDEF/SAF has established various initiatives since 2018. They include the Cyber NSF (full-time national servicemen) scheme for pre-enlistees,[95] establishment of the C4 Expert and Defence Cyber Expert vocations to recruit cyber professionals,[96] and inauguration of the C4I Wing in Officer Cadet School.[97] The Cyber NSF scheme develops so-called cyber specialists through partnering with two local universities under the Work-Learn Scheme (WLS) and providing on-the-job training with the CSTF.[98] From 2023, selected NSFs would also be able to train as digital specialists under the Digital WLS to develop AI applications and perform software engineering tasks in support of DIS operations and undergo academic training in related subjects.[99]

Given the government's well-planned cyber-security policies, effective legislation and solid financial commitment, Singapore has developed a strong cyber-security ecosystem and strengthened cyber resilience through tighter cooperation with CII owners. It attained fourth position in the United Nations International Telecommunication Union Global Cybersecurity Index (GCI) 2020, an improvement by two places from the previous GCI.[100]

Global Leadership in Cyberspace Affairs

As a small state, Singapore aims to expand its relationships, politically and economically, with regional states as well as major powers to protect and advance its national interests. However, in the context of great-power competition, balancing delicately between the US and China is challenging, and Singapore fastidiously avoids taking sides while promoting friendly relations.[101] This stance is also reflected in cyberspace, where the republic has signalled, through the two editions of its cyber-security strategy, its willingness to forge strong partnerships with the international community to combat cyber threats. Since the publication of the first strategy, Singapore has taken up a role as a global leader in the conduct of cyber diplomacy through its involvement in coordination and capacity-building in ASEAN. Internationally, the city-state participates and takes a leadership role in cyber matters at the UN Group of Governmental Experts (UNGGE) and the Open-Ended Working Group (OEWG). In its latest cyber-security strategy, Singapore pledged to step up

participation in international cyber-policy discussions in two specific areas: advocating a rules-based multilateral order in cyberspace and raising the global baseline level of cyber security.[102]

Singapore has been supportive of various cyber discussions at the UN. It voted in 2018 to advance the OEWG and UNGGE, as it viewed them as complementary,[103] and in 2020 for the creation of a new OEWG for 2021–2025.[104] Indeed, Singapore has played an outsized role in both groups. In 2019, the republic was selected for the first time to be one of the 25 members of the UNGGE on cyber security.[105] It has also participated actively in the OEWG through its advocacy of the development and implementation of voluntary and non-binding norms. For instance, Singapore proposed supranational CIIs to be a special category of critical infrastructure whose protection is the shared responsibility of all member states.[106] Singapore's prominence in global cyber diplomacy was further raised when Ambassador Burhan Gafoor, Permanent Representative of Singapore to the UN, was elected to chair the new OEWG in June 2021.[107]

Singapore espouses the importance of regional organisations in supporting frameworks for cyber norms.[108] Under its rotating chairmanship, the country led ASEAN in 2018 to be the first regional entity to subscribe in principle to the 11 UNGGE norms.[109] Singapore's leading role in regional cyber diplomacy is also seen in capacity-building initiatives such as the ASEAN Cyber Capacity Programme established in 2016 and the ASEAN–Singapore Cybersecurity Centre of Excellence set up in 2019.[110] Under the auspices of the UN–Singapore Cyber Programme launched in Singapore in 2018, the city-state co-organised in 2019 the Norm Awareness Workshop for senior ASEAN officials, and it is working with regional and global partners to develop a Norms Implementation Checklist.[111] In August 2022, Singapore collaborated with the UN Office of Disarmament Affairs to organise an inaugural cyber fellowship for cyber ambassadors and heads of agencies worldwide.[112] Such capacity-building efforts would help member states understand how international law applies to cyberspace, which can in turn help to advance discussions of such matters at the UN.[113] In July 2023, Singapore held the official opening of the ASEAN Cybersecurity and Information Centre of Excellence, which it established in partnership with the member states and several international partners, such as the Global Forum on Cyber Expertise.[114]

In October 2022, the US and Singapore conducted their inaugural cyber dialogue, discussing bilateral agreements, critical infrastructure protection, information sharing, supply chain security, regional capacity building and combating digital scams.[115]

Since 2016, Singapore has organised the region's most established annual cyber-security event – the Singapore International Cyber Week (SICW). The event convenes international thought leaders, industry experts and policymakers. At SICW 2022, the CSA partnered with the Global Forum on Cyber Expertise (GFCE) to organise the second GFCE Southeast Asia Regional Meeting that discussed ways to enhance cyber capacity building in the region.[116]

Singapore leads international cooperation with practical action

Singapore also leads international cooperation with practical action such as combating cyber crime. For instance, it hosts the INTERPOL Global Complex for Innovation (IGCI), a global hub in the fight against cyber crime. Moreover, the republic has led the IGCI Working Group and INTERPOL Operational Expert Group on Cybercrime as part of INTERPOL's cybercrime programme.[117] Collaborating with INTERPOL and partner countries, Singapore was involved in the ASEAN Cyber Capacity Development Project, the ASEAN+3 Cybercrime Workshop and the ASEAN Cyber Capability Desk. The republic's efforts to facilitate cooperation between ASEAN member states, INTERPOL and other partner nations have helped to spread best practices and improve operational links amongst them.

In view of promoting the development and adoption of objective technical standards in digital products and services, Singapore pioneered the Cybersecurity Labelling Scheme, the world's first multilevel labelling scheme providing ratings for consumer IoT, which is now extended to include medical devices. Finland and Germany have signed agreements with Singapore to mutually recognise cyber-security labels.[118] Along with

industry and government partners, Singapore is working on a proposal to develop an international standard (ISO 27404) that would serve as a guide for countries seeking to set up their own labelling schemes for consumer IoT. This aligns with Singapore's ambition to position itself as a global hub for security evaluation and testing.[119]

Singapore is in a leading position in international cyber diplomacy due to its diligent efforts in engaging with key global institutions, partner countries, ASEAN member states and industry through various platforms and partnerships to promote norms, support capacity building and enhance collaboration on cyber-security issues.

Offensive Cyber Capability

Singapore has indicated that its military use of cyber capabilities would be restricted to defensive use when it announced the restructuring of the Defence Cyber Organisation into the Digital and Intelligence Service. However, Singapore is aware of the need for and value of offensive cyber capability. In his Committee of Supply speech made in parliament in March 2022, the defence minister said the DIS is meant to deal with rising digital threats from external aggressors which are expected to grow in 'numbers, sophistication and organisation'.[120] One can find open discussion on the MINDEF website of the value of offensive cyber capability,[121] though such discourse is rare. It is highly likely that Singapore has some, albeit limited, offensive cyber capabilities. The country is, however, in an excellent position to acquire such capabilities directly through the open market or with the support of partner countries.

Notes

1 Infocomm Media Development Authority, 'Launch of the Infocomm Security Masterplan', 22 February 2005, https://www.imda.gov.sg/news-and-events/Media-Room/archived/ida/Speeches/2005/20050717163018.

2 Cyber Security Agency of Singapore, 'The Singapore Cybersecurity Strategy 2021', 2021, pp. 9–10, https://www.csa.gov.sg/Tips-Resource/publications/2021/singapore-cybersecurity-strategy-2021.

3 *Ibid*.

4 This refers to risks arising from cyber–physical systems. Such systems comprise hardware, such as sensors, and software elements embedded in physical objects and infrastructure. Cyber–physical systems typically connect the physical infrastructure or object to the internet and to each other to monitor and control the physical environment. See National Science Foundation, 'Cyber-Physical Systems: Enabling a Smart and Connected World', https://www.nsf.gov/news/special_reports/cyber-physical/.

5 Cyber Security Agency of Singapore, 'The Singapore Cybersecurity Strategy 2021', pp. 7–8.

6 See Cyber Security Agency of Singapore, 'Operational Technology Cybersecurity Competency Framework (OTCCF)', 8 October 2021, https://www.csa.gov.sg/Tips-Resource/publications/2021/operational-technology-cybersecurity-competency-framework-(otccf); Cyber Security Agency of Singapore, 'Guidelines for CII Owners to Enhance Cyber Security for 5G Use Cases', 29 April 2022, https://www.csa.gov.sg/Tips-Resource/publications/2022/guidelines-for-cii-owners-to-enhance-cyber-security-for-5g-use-cases; and Cyber Security Agency of Singapore, 'Critical Information Infrastructure Supply Chain Programme Paper', 27 July 2022, https://www.csa.gov.sg/Tips-Resource/publications/2022/cii-supply-chain-programme-paper.

7 Government of Singapore, 'Protection from Online Falsehoods and Manipulation Act 2019', 28 June 2019, https://sso.agc.gov.sg/Acts-Supp/18-2019/Published/20190625?DocDate=20190625.

8 Ministry of Home Affairs, 'HIC Provisions of the Foreign Interference (Countermeasures) Act to Take Effect from 7 July 2022', 6 July 2022, https://www.mha.gov.sg/mediaroom/press-releases/hic-provisions-of-the-foreign-interference-countermeasures-act-to-take-effect-from-7-july-2022/.

9 Aqil Haziq Mahmud, 'SAF to Restructure Intelligence and Cyber Defence Units, Acquire New Ships for Maritime Security Amid Evolving Threats', CNA, 2 March 2020, https://www.milipolasiapacific.com/news-post/saf-to-restructure-intelligence-and-cyber-defence-units-acquire-new-ships-for-maritime-security-amid-evolving-threats/.

10 Alfred Chua, 'Mindef Hit by Targeted Cyber Attack', TODAY, 1 March 2017, https://www.todayonline.com/singapore/mindef-internet-system-hacked-personal-data-850-personnel-stolen.

11 Singapore's defence edifice has six components: MINDEF; SAF; the Defence Science and Technology Agency; the Defence Science Organisation; the defence industry; and MINDEF-related organisations. Ministry of Defence Singapore, 'Defence Cyber Organisation', 27 November 2019, https://www.mindef.gov.sg/web/portal/mindef/about-us/organisation/organisation-profile/defence-cyber-organisation.

12 Ministry of Defence Singapore, 'Cyber Defence'. 10 March 2021, https://www.mindef.gov.sg/web/portal/mindef/defence-matters/defence-topic/defence-topic-detail/cyber-defence.

13 See Ministry of Defence Singapore, 'Speech by Minister for Defence Dr Ng Eng Hen, at the Ministry of Defence Committee of Supply Debate 2022', 2 March 2022, https://www.mindef.gov.sg/web/portal/mindef/news-and-events/latest-releases/article-detail/2022/March/02mar22_speech; and Eileen Yu, 'Singapore to Set Up Digital Intelligence Unit as Cyber Threats Intensify', ZDNet, 2 March 2022, https://www.zdnet.com/article/singapore-to-set-up-digital-intelligence-unit-as-cyber-threats-intensify/.

14 Digital and Intelligence Service, 'Our Mission', https://www.mindef.gov.sg/oms/dis/, Accessed 20 July 2023.

15 Ministry of Defence Singapore, 'Speech by Minister for Defence Dr Ng Eng Hen, at the Ministry of Defence Committee of Supply Debate 2022'.

16 Ministry of Defence Singapore, 'Speech by Minister for Defence Dr Ng Eng Hen at Second Reading of the Singapore Armed Forces and Other Matters Bill for the Parliament Sitting', 2 August 2022, https://www.mindef.gov.sg/web/portal/mindef/news-and-events/latest-releases/article-detail/2022/August/02aug22_speech.

17 As part of its evolution from the SAF C4I community, the DIS retains and continues previous functions of providing accurate, relevant and timely early warning and operational intelligence and advancing C4 connectivity to enable a networked and integrated force. See Ministry of Defence 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.

18 Cybersecurity Agency of Singapore, 'Singapore Cyber Landscape 2022', 2023, pp. 4–5, https://www.csa.gov.sg/docs/default-source/publications/2023/singapore-cyber-landscape-2022.pdf?sfvrsn=d64d1f26_1.

19 *Ibid.*, p. 5.

20 Home Team Science and Technology Agency, 'Data Science & AI', https://www.htx.gov.sg/expertise/our-expertise/data-science-ai; and Jill Tan, Shirlyn Ng, Jason Chen, Mirza Saad, Christi Lau and Ng Huey Liang, 'Transforming the Home Team', *Home Team Journal*, no. 7, issue 2018, p. 10, https://www.mha.gov.sg/docs/hta_libraries/publications/hta-journal-hr-issue-no-7.pdf.

21 Hariz Baharudin, 'New Police Watchgroup to Share Counter-terror and Cyber Crime Data with Tech Firms', *Straits Times*, 6 January 2021, https://www.straitstimes.com/singapore/politics/new-police-watchgroup-to-share-counter-terror-and-cyber-crime-data-with-tech; and CNA, 'Police Introduce New Guidelines on Online Safety to Counter Cybercrime', 7 April 2022, https://www.channelnewsasia.com/singapore/spf-aic-cybercrime-scam-prevention-new-guidelines-2613776.

22 The Total Defence concept refers to Singapore's whole-of-nation approach to respond to all challenges that threaten its sovereignty and national security. The other pillars are military defence; civil defence; economic defence; social defence; and psychological defence. See Total Defence, 'What is Total Defence?', https://www.mindef.gov.sg/oms/imindef/mindef_websites/topics/totaldefence/about.html.

23 Cyber Security Agency Singapore, 'Who We Are', https://www.csa.gov.sg/Explore/who-we-are.

24 Cyber Security Agency of Singapore, 'About SingCERT?', https://www.csa.gov.sg/Explore/who-we-are/our-identity/about-singcert.

25 Cyber Security Agency of Singapore, 'Singapore Cyber Landscape 2019', 26 June 2020, p. 26, https://www.csa.gov.sg/Tips-Resource/publications/2020/Singapore-Cyber-Landscape-2019.

26 Cyber Security Agency of Singapore, 'CSA Kicks Off Licensing Framework for Cybersecurity Service Providers', 11 April 2022, https://www.csa.gov.sg/News-Events/Press-Releases/2022/csa-kicks-off-licensing-framework-for-cybersecurity-service-providers#:~:text=The%20Cyber%20Security%20Agency%20of,effect%20from%2011%20April%202022.

27 Government of Singapore, 'Cybersecurity Act 2018', 12 March 2018, https://sso.agc.gov.sg/Acts-Supp/9-2018/Published/20180312?DocDate=20180312&ProvIds=P13-#pr7-.

28 The Chief Expert of DIS is responsible for planning and overseeing the development of DIS personnel, guiding the conduct of operations, as well as ensuring regimentation and operational discipline during round-the-clock intelligence operations.

29 Ministry of Defence Singapore, 'Fact Sheet: The Digital and Intelligence Service', 28 October 2022, https://www.mindef.gov.sg/web/portal/mindef/news-and-events/latest-releases/article-detail/2022/October/28oct22_fs.

30 The JID works with other military intelligence entities under the purview of the Military Intelligence Organisation.

31 The SAFC4COM/CSTF consists of two brigade-level groups, the C4 Operations Group and the Cyber Defence Group.

32 The DOTC is in charge of developing SAF digital experts such as those under the C4 expert vocation. C4 experts are proficient in software engineering, app development, data science, artificial intelligence and cloud architecting.

33 Ministry of Defence Singapore, 'National Agencies Tackle Cyber Threats at Inaugural Cyber Defence Exercise; DIS and CSA Sign Joint Operations Agreement for Cyber Cooperation', 16 November 2022, https://www.mindef.gov.sg/web/portal/mindef/news-and-events/latest-releases/article-detail/2022/November/16nov22_nr.

34 Ministry of Home Affairs, 'Internal Security Department', 30 March 2021, https://www.mha.gov.sg/isd/a-cause-greater-than-our-self.

35 Ministry of Home Affairs, 'Be Part of ISD', 30 March 2021, https://www.mha.gov.sg/isd/be-part-of-isd.

36 Christopher Bing and Raphael Satter, 'Exclusive: iPhone Flaw Exploited by Second Israeli Spy Firm – Sources', Reuters, 4 February 2022, https://www.reuters.com/technology/exclusive-iphone-flaw-exploited-by-second-israeli-spy-firm-sources-2022-02-03/.

37 Security and Intelligence Division Singapore, 'Our Mission, https://www.sid.gov.sg/about-us/our-mission/.

38 Intelligence Online, 'Singapore Turns to Israeli Cyber Spies Again', 3 April 2019, https://www.intelligenceonline.com/international-dealmaking/2019/04/03/singapore-turns-to-israeli-cyber-spies-again,108351899-art; and Intelligence Online, 'PCS Increasingly Essential to Israeli Cyber Specialists in the City-state', 21 April 2022, https://www.intelligenceonline.com/surveillance--interception/2022/04/21/pcs-increasingly-essential-to-israeli-cyber-specialists-in-the-city-state,109779575-eve.

39 Ministry of Defence Singapore, 'MSD Job Vacancies', 19 April 2022, https://www.mindef.gov.sg/web/portal/mindef/about-us/organisation/organisation-profile/military-security-department-2.

40 Aqil Hamzah, 'BG Lee Yi-Jin Appointed SAF's First Chief of Digital and Intelligence Service', *Straits Times*, 28 October 2022, https://www.straitstimes.com/singapore/bg-lee-yi-jin-appointed-saf-s-first-chief-of-digital-and-intelligence-service.

41 Ministry of Home Affairs, '20th Anniversary of ISD's Operations Against Jemaah Islamiyah in Singapore', 4 December 2021, https://www.mha.gov.sg/mediaroom/press-releases/20th-anniversary-of-isd-operations-against-jemaah-islamiyah-in-singapore/; and Ministry of Defence Singapore, 'Security and Intelligence Division Launches Official Website', 19 July 2021, https://www.mindef.gov.sg/web/portal/mindef/news-and-events/latest-releases/article-detail/2021/July/19jul21_nr.

42 Vincent Chang, 'S'pore Still 2nd Most Digitally Competitive in Global Ranking', 1 October 2020, Economic Development Board, https://www.edb.gov.sg/en/business-insights/insights/spore-still-2nd-most-digitally-competitive-in-global-ranking.html; and SmartCitiesWorld, 'Singapore Ranked Top of Smart City Index for Third Year', 2 November 2021, https://www.smartcitiesworld.net/news/news/singapore-ranked-top-of-smart-city-index-for-third-year-7086#:~:text=Singapore%20topped%20the%20index%20which,Smart%20City%20Index%20(SCI).

43 Gross merchandise value is a measure of online spending and one signal of the strength of the country's digital economy. See Olivia Poh, 'Singapore's Digital Economy Due to Bounce Back', *Business Times*, 7 December 2020, https://www.businesstimes.com.sg/hub/sff-x-switch-2020/singapores-digital-economy-due-to-bounce-back.

44 Statista, 'Share of Population Using the Mobile Internet in Singapore from 2010 to 2020 and a Forecast up to 2025', 2022, https://www.statista.com/statistics/974996/singapore-mobile-phone-internet-user-penetration/.

45 Dominic Low, 'Singapore Tops in Global Ranking of Median Fixed Broadband Speeds', *Straits Times*, 15 February 2022, https://www.straitstimes.com/tech/tech-news/singapore-tops-in-global-ranking-of-median-fixed-broadband-speeds.

46 World Intellectual Property Organisation, 'Global Innovation Index 2022', 2022, p. 17, https://www.wipo.int/edocs/pubdocs/en/wipo-pub-2000-2022-en-main-report-global-innovation-index-2022-15th-edition.pdf.

47 'South Korea, Singapore Lead World in Innovation; US Drops Out of Top 10', *Straits Times*, 3 February 2021, https://www.straitstimes.com/world/united-states/south-korea-singapore-lead-world-in-innovation-us-drops-out-of-top-10.

48 World Intellectual Property Organization, 'Global Innovation Index 2021: Singapore', 2021, p. 1, https://www.wipo.int/edocs/pubdocs/en/wipo_pub_gii_2021/sg.pdf.

49 *Ibid*., p. 8

50 Statista, 'Value of Private Equity (PE) and Venture Capital (VC) Deals in Singapore from 2013 to 2021', 2022, https://www.statista.com/statistics/1023247/singapore-pe-vc-deal-value/.

51 Ovais Subhani, 'As Private Equity Deals Plunge in Region, Singapore Grabs Lion's Share: Bain report', *Straits Times*, 20 April 2023, https://www.straitstimes.com/business/as-private-equity-deals-plunge-in-region-singapore-grabs-lion-s-share-bain-report.

52 Economic Development Board Singapore, 'How Singapore Brings Together the Best in Innovation and Investment to Drive Start-up Growth', 28 February 2022, https://www.investmentmonitor.ai/tech/how-singapore-brings-together-the-best-in-innovation-and-investment-to-drive-start-up-growth; and Nathaniel Fetalvero, 'Here's How Singapore is Building a Tech Ecosystem that Extends Beyond Its Shores', TechInAsia, 4 June 2021, https://www.techinasia.com/heres-singapore-building-tech-ecosystem-extends-shores.

53 *Ibid.*

54 World Intellectual Property Organization, 'Global Innovation Index 2022: Singapore', p. 6, https://www.wipo.int/edocs/pubdocs/en/wipo_pub_2000_2022/sg.pdf.

55 See Smart Nation and Digital Government Office, 'Smart Nation: The Way Forward', November 2018, https://www.smartnation.gov.sg/files/publications/smart-nation-strategy-nov2018.pdf; Ng Chee Khern, 'Digital Government, Smart Nation: Pursuing Singapore's Tech

Imperative', GovTech Singapore, 30 August 2019, https://www.tech.gov.sg/media/technews/digital-government-smart-nation-pursuing%20singapore-tech-imperative; and Infocomm Media Development Authority, 'Digital Economy Framework for Action', 1 June 2019, https://www.imda.gov.sg/About-IMDA/Research-and-Statistics/SGDigital/Digital-Economy-Framework-for-Action.

56 Yu-Min Joo, Teck-Boon Tan and Ming-Yee Foo, 'The Smart Nation: Unpacking Singapore's Latest Mega-digitalisation Push', in Yu-Min Joo and Teck-Boon Tan (eds.), *Smart Cities in Asia* (Cheltenham: Edward Elgar Publishing, 2020), p. 23, https://www.elgaronline.com/view/edcoll/9781788972871/9781788972871.00009.xml.

57 GovTech Singapore, 'Smart Nation Sensor Platform', May 2017, https://www.tech.gov.sg/files/media/speeches/2017/05/Factsheet%20Smart%20Nation%20Sensor%20Platform.pdf.

58 Prime Minister's Office Singapore, 'PM Lee Hsien Loong at the Smart Nation Summit Week', 26 June 2019, https://www.pmo.gov.sg/Newsroom/PM-Lee-Hsien-Loong-Smart-Nation-Summit-Week-Closing-Dialogue.

59 Eileen Yu, 'Singapore Touts Open Platforms in Smart Nation Drive, Acknowledges Need to Do Better in Security', ZDNet, 9 October 2018, https://www.zdnet.com/article/singapore-touts-open-platforms-in-smart-nation-drive-acknowledges-need-to-do-better-in-security/.

60 Eileen Yu, 'Singapore Wants Widespread AI Use in Smart Nation Drive', ZDNet, 13 November 2019, https://www.zdnet.com/article/singapore-wants-widespread-ai-use-in-smart-nation-drive/.

61 See the website of AI Singapore at: https://aisingapore.org/.

62 Heng Swee Keat, 'DPM Heng Swee Keat at the Singapore FinTech Festival X Singapore Week of Innovation and Technology 2019', Prime Minister's Office Singapore, 13 November 2019, https://www.pmo.gov.sg/Newsroom/DPM-Heng-Swee-Keat-at-SFF-X-SWITCH-2019.

63 Eileen Yu, 'Singapore Launches National AI Schemes, Adds $133M Investment to Research', ZDNet, 8 November 2021, https://www.zdnet.com/article/singapore-launches-national-ai-schemes-adds-133m-investment-to-research/.

64 Thundermark Capital, 'AI Research Rankings 2022: Sputnik Moment for China?', 20 May 2022, https://thundermark.medium.com/ai-research-rankings-2022-sputnik-moment-for-china-64b693386a4.

65 Charlotte Trueman and Christina Lago, 'How Singapore is Using Artificial Intelligence', CIO, 12 March 2019, https://www.cio.com/article/221994/how-singapore-is-using-artificial-intelligence.html.

66 See, for example, Ian Poh, 'Hacker "Messiah" James Raj Arokiasamy Pleads Guilty to Charges of Computer Misuse', *Straits Times*, 23 January 2015, https://www.straitstimes.com/singapore/courts-crime/hacker-messiah-james-raj-arokiasamy-pleads-guilty-to-charges-of-computer; Irene Tham, 'Hackers Broke Into NUS, NTU Networks in Search of Government, Research Data', *Straits Times*, 12 May 2017, https://www.straitstimes.com/singapore/hackers-broke-into-nus-ntu-networks-in-search-of-government-research-data; and Tan Tam Mei, '52 Staff Accounts at Four Singapore Universities Breached by Iranian Hackers', *Straits Times*, 3 April 2018, https://www.straitstimes.com/singapore/user-accounts-at-four-singapore-universities-breached-by-iranian-hackers.

67 Irene Tham, Rachel Au-Yong, Tin May Linn and Rodolfo Pazos, 'SingHealth Cyber Attack: How It Unfolded', *Straits Times*, 20 July 2018, https://graphics.straitstimes.com/STI/STIMEDIA/Interactives/2018/07/sg-cyber-breach/index.html.

68 Government of Singapore, 'Cybersecurity Act 2018', 16 March 2018, https://sso.agc.gov.sg/Acts-Supp/9-2018/Published/20180312?DocDate=20180312. The Cybersecurity Act provides a framework for the designation of critical information infrastructure, and it provides CII owners with clarity on their obligations to proactively protect the CII from cyber attacks.

69 The Cybersecurity Act facilitates information sharing, which is critical as timely information helps the government and owners of computer systems identify vulnerabilities and prevent cyber incidents more effectively. The act provides a framework for the CSA to request information, as well as for the protection and sharing of such information.

70 The CSA adopts a light-touch approach to license only two types of service providers currently, namely penetration testing and managed security operations centre monitoring. These two are prioritised because providers of such services have access to sensitive information from their clients. They are also relatively mainstream in the Singapore market and hence have a significant impact on the overall security landscape. The licensing framework seeks to strike a balance between security needs and the development of a vibrant cyber-security ecosystem.

71 Cyber Security Agency of Singapore, 'Codes of Practice/Standards of Performance', 6 Jul 2022, https://www.csa.gov.sg/Legislation/Codes-of-Practice.

72 The Notices on Cyber Hygiene include requirements to secure administrative accounts; apply security patching; establish baseline security standards; deploy network-perimeter defences; implement anti-malware measures; and strengthen multi-factor authentication. See Monetary Authority of Singapore, 'Regulations and Guidance', 2 September 2022, https://www.mas.gov.sg/regulation/regulations-and-guidance?content_type=Notices&topics=Risk%20Management%2FTechnology%20Risk&page=1&q=cyber%20hygiene.

73 The TRM Notices include requirements to put in place a framework and process to identify critical systems; make reasonable efforts to maintain a high availability of critical systems; establish a recovery-time objective for each critical system; notify the MAS of a system malfunction or IT-security incident; submit a root cause and impact analysis report to the MAS of the relevant incident within 14 days; and implement IT controls to protect customer information from unauthorised access or disclosure. See Monetary Authority of Singapore, 'Regulations and Guidance', 2 September 2022, https://www.mas.gov.sg/regulation/regulations-and-guidance?content_type=Notices&topics=Risk%20Management%2FTechnology%20Risk&q=Technology%20Risk%20Management&page=1; and Monetary Authority of Singapore, 'Guidelines on Risk Management Practices – Technology Risk', 18 January 2021, https://www.mas.gov.sg/regulation/guidelines/technology-risk-management-guidelines.

74 Cyber Security Agency of Singapore, "Cybersecurity Act: Supplementary References', 10 June 2022, https://www.csa.gov.sg/Legislation/Supplementary-References; and Cyber Security Agency of Singapore, 'Safer Cyberspace Masterplan 2020', p. 21, https://www.csa.gov.sg/docs/default-source/csa/documents/publications/safer-cyberspace-masterplan-2020.pdf?sfvrsn=d1834c15_0.

75 Cyber Security Agency of Singapore, 'Singapore's Operational Technology Cybersecurity Masterplan 2019', 1 October 2019, p. 33, https://www.csa.gov.sg/Tips-Resource/publications/2019/OT-Cybersecurity-Masterplan.

76 Cyber Security Agency of Singapore, 'Opening Address by Mr Teo Chee Hean, Senior Minister and Coordinating Minister on National Security, at SICW Opening Ceremony on 19 October 2022', 19 October 2022, https://www.pmo.gov.sg/Newsroom/SM-Teo-Chee-Hean-at-the-Singapore-International-Cyber-Week-2022.

77 Kenny Chee, 'S'pore has Moved from Preventing Cyber Threats to Assuming Breaches have Occurred: Josephine Teo', *Straits Times*, 8 September 2021, https://www.straitstimes.com/tech/tech-news/singapore-to-work-with-estonia-on-cyber-security-helping-firms-to-go-digital.

78 Cyber Security Agency of Singapore, 'Review of the Cybersecurity Act and Update to the Cybersecurity Code of Practice for CIIs', 4 March 2022, http://web.archive.org/web/20221104153705/https://www.csa.gov.sg/News/Press-Releases/review-of-the-cybersecurity-act-and-update-to-the-cybersecurity-code-of-practice-for-ciis; and Cyber Security Agency of Singapore, 'Opening Address by Mr Teo Chee Hean, Senior Minister and Coordinating Minster on National Security, at SICW Opening Ceremony on 19 October 2022'. Digital information infrastructure includes hardware and systems, internet service and cloud service providers, physical cables. Key digital services refer to those that form the soft national infrastructure such as the National Digital Identity system (Singpass) and the National Digital Payment System (PayNow).

79 Digital Ship, 'Port-IT receives Singapore CSP License', 2 May 2023, https://www.thedigitalship.com/news/maritime-satellite-communications/item/8392-port-it-receives-singapore-csp-license.

80 See, for example, Cyber Security Agency of Singapore, 'FireEye and CSA Look to Expand Strategic Partnership', 3 October 2019, https://www.csa.gov.sg/News-Events/Press-Releases/2019/FireEye-and-CSA-Look-to-Expand-Strategic-Partnership; and Cyber Security Agency of Singapore, 'Industry Leaders Join Hands with CSA in Cybersecurity Push', 11 October 2016, https://www.csa.gov.sg/News-Events/Press-Releases/2016/Industry-leaders-join-hands-with-CSA-in-cybersecurity-push.

81 Global Cyber Alliance, 'Singapore to Leverage the Global Cyber Alliance's IoT Threat Analytics Platform', 6 October 2021, https://www.globalcyberalliance.org/singapore-to-leverage-the-global-cyber-alliances-iot-threat-analytics-platform/; and Cyber Security Agency of Singapore, 'CSA Pushes Ahead with Efforts to Improve IOT Security', 6 October 2021, https://www.csa.gov.sg/News-Events/Press-Releases/2021/csa-pushes-ahead-with-efforts-to-improve-iot-security.

82 For instance, the Cybersecurity Development Programme and the Cyber Security Associates and Technologists Programme train and upskill fresh ICT and mid-career professionals for

cyber-security roles. See Cyber Security Agency of Singapore, 'Cyber Security Associates and Technologists Programme', 8 November 2021, https://www.csa.gov.sg/our-programmes/talents-skills-development/csat-programme; and Cyber Security Agency of Singapore, 'Cybersecurity Development Programme', 8 November 2021, https://www.csa.gov.sg/Explore/careers/cybersecurity-development-programme-(csdp).

83 Bryan Kow, 'MAS, US Treasury Conduct Cross-border Cybersecurity Exercise', Business Times, 2 May 2023, https://www.businesstimes.com.sg/singapore/mas-us-treasury-conduct-cross-border-cybersecurity-exercise.

84 Cyber Security Agency of Singapore, 'CSA Conducts First Cyber Security Table-top Exercise', 26 May 2015, https://www.csa.gov.sg/News-Events/News-Articles/2015/Cyber-Security-Table-Top-Exercise.

85 Cyber Security Agency of Singapore, '11 CII Sectors Tested on More Complex Cyber Attack Scenarios', 4 September 2019, https://www.csa.gov.sg/News-Events/Press-Releases/2019/Exercise-Cyber-Star-2019.

86 Cyber Security Agency of Singapore, 'Opening Address by Mr Teo Chee Hean, Senior Minister and Coordinating Minster on National Security, at SICW Opening Ceremony on 19 October 2022'.

87 Cyber Security Agency of Singapore, 'CSA Launches the CSA-National Cybersecurity R&D Lab Scholarship (NCLS) to Drive and Support the Development of Professionals in Singapore's Cybersecurity Sector', 20 October 2022, https://www.csa.gov.sg/News-Events/Press-Releases/2022/csa-launches-the-csa-national-cybersecurity-rnd-lab-scholarship.

88 Cyber Security Agency of Singapore, 'CSA Cybersecurity Co-Innovation and Development Fund (CCDF)', https://www.csa.gov.sg/our-programmes/innovation-schemes/csa-cybersecurity-co-innovation-and-development-fund.

89 Ministry of Defence Singapore, 'Cyber Defence', 10 May 2021, https://www.mindef.gov.sg/web/portal/mindef/defence-matters/defence-topic/defence-topic-detail/cyber-defence.

90 Ministry of Defence Singapore, 'Fact Sheet: Strengthening MINDEF/SAF's Cyber Defence Capabilities', https://www.mindef.gov.sg/web/portal/mindef/news-and-events/latest-releases/article-detail/2021/June/30jun21_fs7.

91 See Defence Science and Technology Agency, 'Digital', 2022, https://www.dsta.gov.sg/what-we-do?category=d; and Defence Science Organisation, 'Information', 2022, https://www.dso.org.sg/research/information.

92 Ministry of Defence Singapore, 'Fact Sheet: Defence Technology Prize 2020 Team (Engineering) Award Winner', 30 October 2020, https://www.mindef.gov.sg/web/portal/mindef/news-and-events/latest-releases/article-detail/2020/October/30oct20_fs7.

93 In the 2021 CISS, SAF trained with specialists from public-utility agencies and international military cyber teams against attacks on simulated water treatment and distribution plants. See the 2021 CISS website at: Singapore University of Technology and Design and iTrust Centre for Research in Cyber Security, 'The Fifth International Critical Infrastructure Security Showdown (Online) 2021', 2021, https://itrust.sutd.edu.sg/ciss/ciss-2021-ol.

94 Ministry of Defence Singapore, 'National Agencies Tackle Cyber Threats at Inaugural Cyber Defence Exercise; DIS and CSA Sign Joint Operations Agreement for Cyber Cooperation', 16 November 2022, https://bit.ly/3EvAWKw.

95 Ministry of Defence Singapore, 'Cyber Work-Learn Scheme', 23 March 2022, https://www.mindef.gov.sg/web/portal/mindef/news-and-events/latest-releases/article-detail/2018/cybernsf.

96 Ministry of Defence Singapore, 'Fact Sheet: Command, Control, Communications and Computers Expert (C4X) Vocation and Defence Cyber Expert (DCX) Job Specialisation', 20 February 2019, https://www.mindef.gov.sg/web/portal/mindef/news-and-events/latest-releases/article-detail/2019/february/20feb19_fs. C4 experts are under the SAF Military Domain Experts Scheme, while defence cyber expert is a non-uniformed profession under the Defence Executive Office Scheme. C4 experts specialise in military cyber operations and develop deep understanding of SAF systems and networks. Both C4 experts and defence cyber experts are trained in operational roles such as cyber incident response, network monitoring, vulnerability assessment and penetration testing. They can also be involved in cyber policy planning and long-term capability development.

97 Lim Min Zhang, 'Budget Debate: SAF to Set Up Fourth Service as Digital Threats Mount, Says Ng Eng Hen', 2 March 2022, *Straits Times*, https://www.straitstimes.com/singapore/politics/budget-debate-saf-to-set-up-fourth-service-as-digital-threats-mount-says-ng-eng-hen; and Ministry of Defence Singapore, 'Fact Sheet: Strengthening MINDEF/SAF's Cyber Defence Capabilities'.

98 Ministry of Defence Singapore, 'Fact Sheet: Strengthening MINDEF/SAF's Cyber Defence Capabilities'.

99 Ministry of Defence Singapore, 'MINDEF and NTU Singapore Launch New Work-Learn Scheme for Digital

Specialists', 9 March 2022, https://www.mindef.gov.sg/web/portal/mindef/news-and-events/latest-releases/article-detail/2022/March/09mar22_nr.

100 International Telecommunications Union, 'Global Cybersecurity Index 2020', 2021, p. 25, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf.

101 Vivian Balakrishnan, 'Full Speech: Five Core Principles of Singapore's Foreign Policy', *Straits Times*, 17 July 2017, https://www.straitstimes.com/singapore/five-core-principles-of-singapores-foreign-policy.

102 Cyber Security Agency of Singapore, 'The Singapore Cybersecurity Strategy 2021', p. 33.

103 United Nations, 'First Committee Approves 27 Texts, Including 2 Proposing New Groups to Develop Rules for States on Responsible Cyberspace Conduct', 8 November 2018, https://www.un.org/press/en/2018/gadis3619.doc.htm.

104 United Nations General Assembly, 'Developments in the Field of Information and Telecommunications in the Context of International Security: Resolution Adopted by the General Assembly on 31 December 2020', 2020, https://digitallibrary.un.org/record/3896458/files/A_RES_75_240-EN.pdf?ln=en.

105 Teo Chee Hean, 'SM Teo Chee Hean at the 4th Singapore International Cyber Week', Prime Minister's Office Singapore, 1 October 2019, https://www.pmo.gov.sg/Newsroom/SM-Teo-Chee-Hean-at-4th-Singapore-International-Cyber-Week.

106 Republic of Singapore Government, 'Singapore's Written Comment on the Chair's Pre-Draft of the OEWG Report', April 2020, https://front.un-arm.org/wp-content/uploads/2020/04/singapore-written-comment-on-pre-draft-oewg-report.pdf; Republic of Singapore Government, 'Singapore's Views on Developments in the Field of Information and Telecommunications in the Context of International Security, Pursuant to General Assembly Resolution 74/28', March 2022, https://front.un-arm.org/wp-content/uploads/2022/03/singapore-ict-security-2020.pdf, p. 1; and Republic of Singapore Government, ' Singapore's Views on Developments in the Field of Information and Telecommunications in the Context of International Security, Pursuant to General Assembly Resolution 75/32', March 2022, https://front.un-arm.org/wp-content/uploads/2022/03/singapore-ict-security-2021.pdf, p. 2.

107 Digital Watch, 'OEWG 2021-2025 Holds Organisational Session', 2 June 2021, https://dig.watch/updates/oewg-2021-2025-holds-organisational-session.

108 Keerthi, 'Statement by Mr Gaurav Keerthi, Deputy Chief Executive (Development), Cyber Security Agency of Singapore at the Virtual Consultations of the United Nations Open-Ended Working Group'.

109 ASEAN, 'ASEAN Leaders' Statement on Cybersecurity Cooperation', 2018, https://asean.org/wp-content/uploads/2018/04/ASEAN-Leaders-Statement-on-Cybersecurity-Cooperation.pdf; and Cyber Security Agency of Singapore, 'ASEAN Member States Agree to Strengthen Cyber Coordination and Capacity-Building Efforts', 19 September 2018, https://www.csa.gov.sg/News-Events/Press-Releases/2018/AMCC-2018.

110 Leon Spencer, 'How ASEAN is Driving Global Cyber Security Efforts', CNA, 7 October 2021, https://www.channelasia.tech/article/691880/how-asean-driving-global-cybersecurity-efforts/; and Republic of Singapore Government, 'Singapore's Views on Developments in the Field of Information and Telecommunications in the Context of International Security, Pursuant to General Assembly Resolution 75/32', March 2022.

111 Tham Yuen-C, 'Singapore, UN to Cooperate on Checklist for Countries to Implement Cyber-security Norms', *Straits Times,* 9 October 2020, https://www.straitstimes.com/singapore/politics/singapore-un-to-cooperate-on-checklist-for-countries-to-implement-cybersecurity; and Cyber Security Agency of Singapore, 'The Singapore Cybersecurity Strategy 2021', p. 35, https://www.csa.gov.sg/Tips-Resource/publications/2021/singapore-cybersecurity-strategy-2021.

112 Cyber Security Agency of Singapore, 'Opening Address by Mr Teo Chee Hean, Senior Minister and Coordinating Minster on National Security, at SICW Opening Ceremony on 19 October 2022'.

113 Republic of Singapore Government, 'Singapore's Written Comment on the Chair's Pre-Draft of the OEWG Report'.

114 Ministry of Defence, 'Fact Sheet: ASEAN Defence Ministers' Meeting (ADMM) Cybersecurity and Information Centre of Excellence (ACICE)', 18 July 2023, https://www.mindef.gov.sg/web/portal/mindef/news-and-events/latest-releases/article-detail/2023/July/18jul23_fs.

115 CSA, 'Conduct of Inaugural United States-Singapore Cyber Dialogue 20 October 2022', 4 November 2022, https://www.csa.gov.sg/News-Events/Press-Releases/2022/conduct-of-inaugural-united-states-singapore-cyber-dialogue-20-oct-2022.

116 Rachel Teng, 'Singapore to Build Cyber Capacity and More at the Singapore International Cyber Week', GovInsider, 19 October 2022, https://govinsider.asia/govware/singapore-to-build-cyber-capacity-and-more-at-the-singapore-international-cyber-week/.

117 Ministry of Home Affairs, 'National Cybercrime Action Plan', 2016, p. 15, https://www.mha.gov.sg/docs/default-source/media-room-doc/ncap-document.pdf.

118 Cyber Security Agency of Singapore, 'CSA Pushes Ahead with Efforts to Improve IOT Security', 6 October 2021, https://www.csa.gov.sg/News-Events/Press-Releases/2021/csa-pushes-ahead-with-efforts-to-improve-iot-security; and Cyber Security Agency of Singapore, 'Opening Address by Senior Minister of State, Ministry of Communications and Information, Dr Janil Puthucheary at International IOT Security Roundtable 2022', 20 October 2022, https://www.csa.gov.sg/News-Events/speeches/2022/opening-address-by-sms-mci-dr-janil-puthucheary-at-iiot-security-roundtable-2022.

119 Vanessa Lim, 'Singapore to Take a More Proactive Stance on Cyber Threats under Updated National Strategy', CNA 5 October 2021, https://www.channelnewsasia.com/singapore/singapore-proactive-stance-cyber-threats-updated-national-strategy-2223536#:~:text=SINGAPORE%3A%20Singapore%20unveiled%20an%20updated,threats%20and%20technological%20shifts%20emerge.

120 Ministry of Defence Singapore, 'Speech by Minister for Defence, Dr Ng Eng Hen, at the Committee of Supply Debates 2022', 2 March 2022, https://www.mindef.gov.sg/web/portal/mindef/news-and-events/latest-releases/article-detail/2022/March/02mar22_speech.

121 See, for example, Lim Guang He, 'Cyberspace: What are the Prospects for the SAF?', *Pointer: Journal of the Singapore Armed Forces*, vol. 41, no. 1., 2015, pp. 58–70, https://www.mindef.gov.sg/oms/content/dam/imindef_media_library/graphics/pointer/PDF/2015/Vol.41%20No.1/7)%20V41N1_Cyberspace%20What%20are%20the%20Prospects%20for%20the%20SAF.pdf.