7. Japan

Japan has been among the global leaders in the commercial application of information and communications technologies since the early 1980s, but its readiness to deal with the security aspects of cyberspace is a much more recent phenomenon. Its first mature cyber-security strategy was issued in 2013, building on several earlier policies that were focused on rhetorical principles of classic information security of a narrow technical kind. Japan now has a well-developed approach to the governance of cyberspace, but this constitutes a looser set of arrangements than in countries such as the United States and the United Kingdom, particularly in terms of information-sharing by the private sector. Japan's defences in cyberspace are not especially strong, with many corporations unwilling to meet the costs of bolstering them. The country's resilience planning has been rather limited, though this intensified in the run-up to the 2020 Olympic and Paralympic Games (postponed due to COVID-19). Japan still does not have an official military cyber strategy or an official military doctrine pertaining to cyberspace, though it has made modest organisational changes in its armed forces, including the creation of some dedicated cyber units. Its offensive cyber capabilities remain underdeveloped because of the constitutional and political constraints on the country's use of force. By 2020, prompted in part by the US and Australia, Japan had shifted to a more robust cyber posture because of rising concerns about China and North Korea.

Strategy and doctrine

As its title suggests, Japan's 'First National Strategy on Information Security', in 2006, was the earliest document of its kind.[1] (At the time, many countries preferred the term 'information security' to 'cyber security'.) It did not lead to many changes in policy, however, and focused largely on narrow technical aspects of cyber security that had been topical since the mid-1990s. Several related policy documents followed.

The strategy published in 2013, the first under the title of 'Cybersecurity Strategy', was a watershed event that reflected organisational measures undertaken during the previous year.[2] In comparison with the earlier documents it had a stronger overall emphasis on national security and focused much more on cyberspace as an operational environment for politics, economics, diplomacy and global influence. It was the first Japanese government document to call for the Ministry of Defense

List of acronyms

ASEAN	Association of Southeast Asian Nations
CCDCOE	Cooperative Cyber Defence Centre of Excellence
CSSH	Cyber Security Strategic Headquarters
DIH	Defense Intelligence Headquarters
DSI	Directorate for Signals Intelligence
ICT	information and communications technology
IoT	Internet of Things
IPv6	Internet Protocol Version 6
JSDF	Japan Self-Defense Forces
MoD	Ministry of Defense
NISC	National Center of Incident Readiness and Strategy for Cybersecurity
NTT	Nippon Telegraph and Telephone

(MoD) to defend against strategic cyber attacks by other states. Referring to cyberspace as a new domain of warfare, it outlined the creation of the first cyber-defence unit within the Japan Self-Defense Forces (JSDF) and stronger coordination between civilian and military entities in cyber defence. Furthermore, it noted the importance of norms in cyberspace and the need for a multi-stakeholder approach towards internet governance. In 2013 Japan also released a new National Security Strategy, although cyber capabilities did not feature prominently within it; the principal emphasis was on developing norms for behaviour in cyberspace and closer cooperation with like-minded countries in cyber defence.[3]

A revised Cybersecurity Strategy was issued in 2015, calling for uniform cyber-security standards across government and for stronger reporting and coordination requirements in response to cyber threats.[4] It also underlined the need for a more comprehensive approach to cyber security in the light of Tokyo's anticipated hosting of the 2020 Olympic and Paralympic Games. It was the country's first strategy document to address the potential benefits and dangers posed by the Internet of Things (IoT), a topic on which the government issued a separate document in 2016.[5] It also reiterated the growing role of the MoD in defending against cyber attacks and stressed the importance of closer ties with the United States military under the updated 'Guidelines for U.S.–Japan Defense Cooperation'.[6] The 2015 strategy document was the first to be considered at cabinet level, reflecting a greater recognition of the importance of cyberspace security among the upper echelons of the Japanese government.

The Cybersecurity Strategy released in July 2018 – covering the period 2018–21, with a special emphasis on the Olympic and Paralympic Games – represented a further evolution in Japanese policy.[7] It clearly recognised the potential cyber threat from hostile states, referring on its first page to the growing danger of 'organised, sophisticated, and possibly state-sponsored' cyber attacks. It noted the gradual merging of 'cyberspace and real space' as a result of increasingly sophisticated cyber technologies including artificial intelligence (AI), the IoT, robotics and 3D printers – capabilities at the core of Japan's concept of an information society, or 'Society 5.0' as the government refers to it. The strategy called for improved incident readiness against massive cyber attacks, new initiatives for the protection of critical infrastructure, and enhanced collaboration between stakeholders. Another stated priority was to improve cyber security in the private sector, with a policy of 'Proactive Cyber Defence' including better sharing and utilisation of threat information and system vulnerabilities by businesses.

The 2018 Cybersecurity Strategy also represented a landmark in being the first such document to refer to Japan's deterrence capabilities in cyberspace. It specified that these capabilities should be coordinated by the National Security Secretariat, which provides support to the National Security Council, an inter-agency body established in 2013 to coordinate national-security policies. As yet, however, there is neither an official national military cyber strategy nor an official JSDF military doctrine pertaining to cyberspace in the public domain.

Japan's military cyber journey began in earnest in 2012 with a plan to set up a 100-strong cyber-defence unit,[8] though in previous years the Japanese armed forces had already conducted various cyber-related activities. The most relevant document from which a doctrinal approach can be inferred is the 2019 National Defense Program Guidelines. This emphasised the need for jointness and inter-operability within the JSDF in order to create a multi-domain force that can seamlessly integrate itself into any US defence architecture in East Asia. It also referred to space, cyberspace and the electromagnetic spectrum as domains of warfare. Regarding military operations in cyberspace, its emphasis lay clearly on defence, in line with the JSDF's overall force posture, but it also noted the importance of achieving 'superiority' in the cyber domain and further hinted at the need for offensive cyber capabilities as part of defensive operations to 'disrupt' enemy cyber attacks.[9] Similarly, the 2018 Cybersecurity Strategy stated that acquiring 'capabilities to prevent malicious cyber actors from using cyberspace' should be considered.[10]

Japan's 2020 defence white paper emphasises that cyberspace 'could drastically change the conduct of warfare' and specifically calls for the strengthening of capabilities in order to enable cross-domain operations in space, cyberspace and the electromagnetic domain.[11] While it underlines the need to strengthen cyber-intelligence capabilities, the document also stresses the importance

of 'building the capability to disrupt C4I [command, control, communications, computers and intelligence] of opponents'.[12]

Another crucial document concerning the JSDF's role in cyberspace is the Medium Term Defense Program, which outlined defence priorities for 2019 to 2023.[13] It placed special emphasis on the need to create additional cyber units within the ground forces, which may indicate a particular capability deficit in that branch of the JSDF. The document also underlined the need for better protection of the JSDF's C4I capabilities; for the expansion of the existing cyber-defence unit and the creation of new ones by 2023; and for Japan to participate in bilateral and multilateral cyber exercises.

Governance, command and control

In 2014 the Japanese government began a process of rationalising and improving the civilian command-and-control structure that coordinates cyber activities at the national level. They now resemble those of allied states such as the US and the United Kingdom, although coordination between the public and private sectors remains comparatively weak. Japanese military cyber command and control is less advanced than in allied states.

The groundwork for establishing the current structures was laid in 2014 with the passing of the Basic Act on Cybersecurity (subsequently amended in 2016 and 2018). As a result of this new law, which came into effect in January 2015, the Cyber Security Strategic Headquarters (CSSH) was created, taking over the role of the institutionally weak Information Security Policy Council. Another important body is the National Center of Incident Readiness and Strategy for Cybersecurity (NISC), which acts as the executive organ within the Cabinet Secretariat. Both the CSSH and the NISC have legal authority to coordinate and implement Japan's national cyber-security strategy. The CSSH is officially 'the command and control body of national cybersecurity'.[14] Chaired by the Chief Cabinet Secretary, it also includes the chair of the National Public Safety Commission, the head of the National Police Agency, four ministers (internal affairs and communications; foreign affairs; economy, trade and industry; defense), and eight cyber specialists who chair expert panels.

The CSSH coordinates closely with the Japanese National Security Council and the IT Strategic Headquarters on questions of policy. The NISC in turn coordinates the implementation of policy with the relevant ministries, which share with the providers of critical national infrastructure a legal obligation to report back to the CSSH on cyber-relevant topics.[15] Specifically, the NISC is tasked with integrating and advancing the country's cyber-security strategy, a role which includes developing common standards, protecting infrastructure, developing human resources and implementing a research-and-development strategy.[16]

The second amendment to the Basic Act on Cybersecurity, passed in December 2018 with an eye on security for the Olympic and Paralympic Games, also established a Cybersecurity Council to exchange and collaborate on cyber-security-related information across government, the private sector and academia. Its role is to work in close coordination with the NISC, the national Computer Emergency Response Team (JPCERT) and other institutions such as the National Institute of Information and Communications Technology and the Information-Technology Promotion Agency, both of which aim to promote information-sharing between government and the private sector.[17]

In cyber affairs, Japan's military command-and-control structure remains less advanced than its civilian equivalent. In 2008 the MoD established the C4 Systems Command, reporting directly to the chief of staff of the Joint Staff Office, which was tasked with monitoring the defence of military networks and responding to cyber attacks. The C4 Systems Command reports to the MoD, which in turn cooperates with civilian authorities.

Each branch of the armed forces has a separate cyber-defence unit tasked with network and information-systems defence, principally against internal threats.[18] In March 2019 the JSDF also established the first regional cyber-defence unit as part of the Western Army of the Japan Ground Self-Defense Force (JGSDF), with about 60 personnel. The first of a number of similar regional formations due to be created in the coming years, the unit is tasked with defending and protecting JSDF systems and networks.[19]

A Cyber Defense Group, responsible for coordinating cyber defence across the JSDF as a whole and for

defending its information infrastructure, was created in March 2014. In 2021 it is due to expand from approximately 220 personnel to 290.[20] According to media reports the total number of JSDF personnel deployed in cyber defence will reach 500 by around 2024.[21]

Core cyber-intelligence capability

For a variety of political reasons, including the constitutional arrangements put in place after the Second World War, Japan's intelligence organisations are small and underfunded in comparison to those of other states of similar size. For example, Article 21 of Japan's constitution severely limits the extent to which the government can collect signals intelligence and consequently conduct cyber reconnaissance. Nevertheless, Japan has a suite of relevant organisations, including the Defense Intelligence Headquarters (DIH)[22] and its largest subordinate organisation, the Directorate for Signals Intelligence (DSI). Additionally, Japan has long hosted US signals-intelligence facilities as part of a close intelligence partnership.

The DSI is the equivalent of the National Security Agency (NSA) in the US and Government Communications Headquarters in the UK, though considerably smaller than both. Previously focused on collecting information from communications satellites, the DSI commenced intelligence support to cyber operations in 2012, with assistance from the US through the NSA. At the time, it described these operations as experimental.[23] Budget requests for restructuring and further developing the DSI were submitted for the 2020 fiscal year,[24] but resource choices in favour of expensive weapons platforms, and the Article 21 legal barrier, have so far prevented the establishment of a stronger Japanese signals-intelligence agency.

The total number of JSDF personnel deployed in cyber defence will reach 500 by around 2024

The comparatively well-funded Cabinet Intelligence and Research Office is also likely to play an important role. Reporting directly to the prime minister, it also acts as the coordinating and assessment body for the Japanese intelligence community.

Overall, Japan's indigenous cyber-intelligence capabilities are embryonic, with the country largely reliant on key international partners, especially the US, for its cyber situational awareness and its development of intelligence capabilities.

Cyber empowerment and dependence

Japan remains a world leader in cyberspace technologies. A 2019 study by the International Monetary Fund concluded that the country's digital economy accounted for 49% of its GDP (the figure in the US was 60%, and in China 30%).[25] Of the 51 telecoms or tech companies in the 2020 *Fortune* 'Global 500', the US had 16 and Japan was in second place with ten (just ahead of China with eight, while the combined total for the countries of Western Europe was also eight).[26]

As the pre-eminent producer of industrial robotics[27] and a world leader in the development of digital infrastructure,[28] Japan's economy is both empowered by and increasingly dependent on the ICT sector. The country has an established sovereign microchip-manufacturing capability, with the companies Tokyo Ohka Kogyo Co., Ltd. (TOK), JSR Corporation and Shin-Etsu Chemical together dominating global production of the extreme ultraviolet (EUV) photoresists used in the manufacture of cutting-edge seven-nanometre chips.[29]

Japan is home to the fourth-largest telecommunications group in the world, Nippon Telegraph and Telephone (NTT), which comprises a series of subsidiary branches including NTT Communications (international communications), NTT Domoco (mobile-device communication) and NTT World Engineering Marine Corporation (ground-cable installation and maintenance).[30] According to open-source IPv6 2019 data, the top five internet service providers in Japan are all indigenous: Bbix, Biglobe, Jpne, Mf-native6 and Ocn.[31] NTT World Engineering Marine Corporation's small fleet of cable-laying vessels enables the country to maintain a sovereign and indigenous telecommunications backbone.[32]

Japan is currently lagging behind many other members of the Organisation for Economic Co-operation and Development (OECD) in terms of technological productivity, with an OECD survey suggesting the country needs greater investment in skills and digital

competence – 'particularly for middle-aged and older workers' – in order to close the gap.[33] There is widespread concern about the digital divide between the younger and older generations – a situation illustrated in particularly embarrassing fashion for the government in 2018, when the minister responsible for cyber security was forced to admit he had never used a computer.[34]

Japan has nevertheless formulated a thorough Cyber/Physical Security Framework,[35] and in April 2019 the Ministry of Economy, Trade and Industry launched 'Society 5.0', a national policy aimed at 'integrating cyberspace and physical space in a sophisticated manner'.[36] This initiative set out to implement standards and regulations for governmental and commercial entities operating in cyberspace, and to improve the resilience of the domestic supply chain, as well as to address concerns about Japan's ageing population and shrinking labour force.[37]

In the field of AI, Japan is competitive. It was placed ninth, for example, in a study that ranked the top 50 countries based on their contributions to the two most prestigious AI conferences in 2020.[38] Japanese companies are very active in AI research, with nine of them featuring in a list of the world's leading 100 companies in that regard, compared with six from South Korea and none from India. Nevertheless, the aggregate contribution that Japan's industrial sector makes to AI research still falls behind that of South Korea.[39]

Much of Japan's digital technology has the potential to be further integrated into military applications, although currently that remains little more than a policy aspiration. Japan's annual defence white papers have addressed in general terms the global trend towards digital dependence in military operations, acknowledging the need for the Japanese armed forces to increase the resilience of their command-and-control systems.[40]

In terms of Japan's indigenous satellite capability, the Cabinet Office approved plans to implement and expand the Quasi-Zenith Satellite System (QZSS/*Michibiki*) programme, headed by Japan's Aerospace Exploration Agency, in 2002.[41] The programme launched its first satellite in 2010, followed by three more between 2016 and 2018. Originally designed to augment the functionality of the US Global Positioning System (GPS), the QZSS gives Japan a degree of what the Cabinet Office describes as 'technological sovereignty', as well as bringing a public good to the Asia-Oceania region.[42] The QZSS is currently being reviewed for formal recognition by the Worldwide Radio Navigation System under the auspices of the International Maritime Organization, a process already completed for peers such as GPS, GLONASS (Russia) and *Beidou* (China).[43]

Japan has become very focused on national-security aspects of outer space. It is concerned about North Korea's missile capability and China's growing military power, while remaining keen to expand its own space capabilities. In 2020 it established a Strategic Headquarters for National Space Policy in the Cabinet Office, announced the creation within the Joint Staff of a military unit that would be 'responsible for planning pertaining to joint operations in the space domain',[44] and created a Space Operations Squadron to prepare for the introduction in 2022 of a Space Situational Awareness system.

Cyber security and resilience

Digital and cyber technologies are at the heart of Japan's economy and society, and the overall degree of digital connectedness suggests that a sustained cyber attack on the country's infrastructure would be highly compromising, especially since national cyber resilience is still at a developmental stage.[45]

Japan's efforts to raise its level of resilience in cyberspace were driven principally by security concerns surrounding the planned 2020 Tokyo Olympic and Paralympic Games. The guiding document in that respect was the Cybersecurity Policy for Critical Infrastructure Protection, adopted in April 2018, which focused on the importance of public–private partnerships in boosting resilience and recovering quickly from damage to critical infrastructure caused by cyber attacks.[46] This is unsurprising, as 90% of Japan's ICT assets are in the private sector.[47]

The national-level Computer Emergency Response Team, JPCERT, coordinates with equivalent bodies in other countries and with tactical incident-response teams across the Japanese public and private sectors. The governmental CERT, NISC, also houses the Government Security Operation Coordination Team, which is responsible for accurate and prompt information-sharing across the CERT structure.[48]

In the private sector, the major obstacle to improving cyber resilience is the lack of willingness among companies to share information regarding cyber incidents. This is partly the result of cultural and structural factors. These include a general lack of familiarity with cyber-security issues among senior business leaders, an overreliance on government regulators to establish cyber-security requirements and traditional Japanese business practices that hinder collaboration between companies. According to government statistics, Japanese companies have been slow to integrate cyber security into their corporate governance, especially their risk planning.[49]

The Ministry of Economy, Trade and Industry and one of its subsidiaries, the Information-Technology Promotion Agency, Japan, have published 'Cybersecurity Management Guidelines' for business leaders in an effort to promote cyber-security measures and standards in the private sector.[50] The fact that these guidelines are based on the Cybersecurity Framework of the US National Institute of Standards and Technology illustrates both a tendency towards the adoption of the US view on cyber security and an absence of significant domestic innovation on the issue. Within the Japanese government, a framework for raising cyber-security standards – the Common Standards on Information Security Measures for Government Agencies and Related Agencies – has been in place since 2016.[51] The government's engagement with certain aspects of cyber security since 2006, and the strong ICT sector, probably contributed to Japan being ranked 14th out of 175 countries in the 2018 Global Cybersecurity Index compiled by the International Telecommunication Union.[52]

The government has also been holding regular cyber exercises involving both the public and private sectors, some of which have been on quite a large scale – the one in November 2019, for example, had about 5,000 participants.[53] As an example of partnerships with the private sector, in July 2013 the MoD set up a Cyber Defense Council consisting of around ten defence contractors. Its aim is to coordinate exchanges of information between the defence industry and the government, and to organise joint cyber exercises.[54]

Global leadership in cyberspace affairs

Japan has set itself the goal of becoming a leader in cyber diplomacy. Tokyo aims to solidify international rules and norms of behaviour for states in cyberspace and, as part of that norms-based approach, actively promotes the multi-stakeholder model of internet governance. The government has a policy of leading international debate on how to ensure a 'free, fair, and secure cyberspace, strengthening coordination with other countries'.[55] This policy has three pillars: promoting the rule of law in cyberspace, developing confidence-building measures and enhancing international cooperation on capacity-building.

At the global level, Japan has participated in five sessions of the United Nations Group of Governmental Experts[56] and has been promoting the rule of law and confidence-building in cyberspace within the framework of the UN.[57] Tokyo participates in the G7 Cyber Expert Group and various dialogues with regional organisations, such as the ASEAN–Japan Information Security Policy Meeting and the ASEAN–Japan Cybercrime Dialogue.[58] Japan is also a party to the Convention on Cybercrime and actively aims to strengthen international law in that respect by promoting the convention in international forums.[59]

In regional diplomacy, Japan has been partnering with members of the Association of Southeast Asian Nations (ASEAN) on the protection of critical infrastructure and rapid incident response. Tokyo was a leading force in establishing the ASEAN–Japan Cybersecurity Capacity Building Centre, in Bangkok, which facilitates the development of a standardised incident-reporting framework across Southeast Asia,[60] and was also instrumental in setting up the ASEAN Computer Emergency Response Team (ASEAN-CERT).

As one of NATO's global partners and a member of the Partnership for Peace (PfP), Japan became a contributing member of NATO's Cooperative Cyber Defence Centre of Excellence (CCD COE) in March 2019.[61] The CCD COE's mission is to enhance cooperation and information-sharing on cyber defence among NATO members and partners.[62] Japan participated in the CCD COE-led exercise dubbed *Cyber Coalition* 2019 in December 2019; the aim, according to the Japanese MoD, was 'to deepen the knowledge of how to cooperate with NATO on cyber defence' and to improve the 'tactical skills' of the MoD and the JSDF.[63]

Japan's longest and closest international cyber partnership, however, is with the US. The current Japan–US

Cyber Dialogue and the Japan–US Policy Cooperation Dialogue on the Internet Economy are of particular importance to the Japanese government, given that the US is the ultimate guarantor of Japan's security. The Japanese MoD and the Pentagon have established the Cyber Defense Policy Working Group, aiming to deepen information-sharing, organise joint exercises, promote policy discussions and cooperate in training cyber-security experts.[64]

Japan has CERT cooperation agreements with other Asian countries, including India, and with Australia. Japanese CERT officials meet annually with Chinese and South Korean counterparts, and also cooperate with the Asia-Pacific Computer Emergency Response Team (APCERT) on the TSUBAME project, a traffic-monitoring system that shares data between 23 national CERTs.[65] Japanese CERTs cooperate effectively with their US counterparts, and with others in the Asia-Pacific region, but less so with those in Europe.

Japan has established bilateral cyber dialogues with 11 countries – Australia, Estonia, France, Germany, India, Israel, Russia, South Korea, Ukraine, the UK and the US – and also with the European Union (EU) and NATO. Besides participating in the ASEAN–Japan Cybersecurity Policy Meeting, where the focus is on capacity-building, Japan also holds trilateral cyber discussions with China and South Korea, focusing on North Korean operations.[66] The UK and the EU have dialogues with Japan at the ministerial and expert levels, as well as technical cooperation and joint capacity-building.[67] Japan and the EU have also been jointly promoting better data protection, with the European Commission having agreed with Japan on arrangements for data exchange without further reference to national authorities for approval – a move that facilitates the gradual streamlining of data-privacy standards.[68]

Japan's longest and closest international cyber partnership is with the US

Offensive cyber capability

The development of any offensive military capability is constrained by Japan's military history and by current views on the post-Second World War pacifist constitution. Article 9 of the constitution denies the country the right to military forces of any kind. Though this has been ignored since 1954, when the Self-Defense Forces Act was passed, every government has had to make complex legal and political arguments to massage public opinion each time the reach and mission of Japan's forces have been extended. Since 2015 the government has made additional reinterpretations to make it possible, under certain circumstances, to come to the aid of an ally even if Japan itself is not under attack.[69] This shift is now also seen as allowing collective self-defence and active defence in cyberspace.[70]

At the same time, there have been hints in official documents of a subtle shift in Japanese policy from focusing purely on defence to developing offensive capabilities, for which there has been a low-key push by the JSDF.[71] The 2020 defence white paper states that the armed forces would act to disrupt enemy cyber operations during an attack on Japan.[72] Some senior policymakers have also suggested that offensive cyber is being considered as a way of providing a 'deterrence by punishment' option for Japan, including as part of its missile-defence strategy. However, this would require Japan's Self-Defense Forces Law to be revised.[73]

The fact remains that, for the foreseeable future, Japan will probably remain reliant on its alliance with the US for any kind of offensive response to a cyber threat. It is notable that the 2015 guidelines for US–Japan defence cooperation[74] include an entire section dedicated to cyberspace, setting out the circumstances under which the US can lend cyber support in Japan's defence. The narrowest interpretation of the text would limit US assistance to the protection of Japanese critical information infrastructure used by US forces in Japan, but in the broadest interpretation the text is analogous to NATO's Article 5, with a serious cyber attack on Japan being treated like an attack on the US.

Notes

1 Information Security Council, *The First National Strategy on Information Security: Toward the Realisation of a Trustworthy Society*, 2 February 2006, http://www.nisc.go.jp/eng/pdf/national_strategy_001_eng.pdf.

2 Information Security Council, *Cybersecurity Strategy: Towards a World-Leading, Resilient and Vigorous Cyberspace*, 10 June 2013, http://www.nisc.go.jp/active/kihon/pdf/cybersecuritystrategy-en.pdf.

3 Japan Ministry of Foreign Affairs, *National Security Strategy*, 17 December 2013, http://japan.kantei.go.jp/96_abe/documents/2013/__icsFiles/afieldfile/2013/12/17/NSS.pdf.

4 Government of Japan, *Cybersecurity Strategy*, 4 September 2015, http://www.nisc.go.jp/eng/pdf/cs-strategy-en.pdf.

5 National Center of Incident Readiness and Strategy for Cybersecurity, *General Framework for Secure IoT Systems*, 26 August 2016, http://www.nisc.go.jp/eng/pdf/iot_framework2016_eng.pdf.

6 US Department of Defense, 'The Guidelines for U.S.–Japan Defense Cooperation', 27 April 2015, https://archive.defense.gov/pubs/20150427_--_GUIDELINES_FOR_US-JAPAN_DEFENSE_COOPERATION.pdf. The 'guidelines' framework has been used since 1979 to set the parameters of defence cooperation between the two countries.

7 National Center of Incident Readiness and Strategy for Cybersecurity, *Cybersecurity Strategy*, 27 July 2018, https://www.nisc.go.jp/eng/pdf/cs-senryaku2018-en.pdf.

8 Richard J. Samuels, *Special Duty: A History of the Japanese Intelligence Community* (Ithaca, NY: Cornell University Press, 2019), pp. 228–9.

9 Ministry of Defense, *National Defense Program Guidelines for FY 2019 and beyond*, 18 December 2018, https://www.mod.go.jp/j/approach/agenda/guideline/2019/pdf/20181218_e.pdf.

10 National Center of Incident Readiness and Strategy for Cybersecurity, *Cybersecurity Strategy*, 27 July 2018.

11 Ministry of Defense, *Defense of Japan 2020*, 2020, p. 41, https://www.mod.go.jp/e/publ/w_paper/wp2020/DOJ2020_EN_Full.pdf.

12 *Ibid*., pp. 218, 267.

13 Ministry of Defense, *Medium Term Defense Program (FY 2019 – FY 2023)*, 18 December 2018, https://www.mod.go.jp/j/approach/agenda/guideline/2019/pdf/chuki_seibi31-35_e.pdf.

14 Government of Japan, *Cybersecurity Strategy*, 4 September 2015.

15 These include: 'the network-based vigilance and monitoring of malicious activities against information systems of administrative organs; fact-finding on the cause of incidents and audit of relevant governmental bodies; information gathering and analysis on domestic and foreign cybersecurity; the promotion of international cooperation and collaboration; and cybersecurity workforce development for and by the governmental bodies'. National Center of Incident Readiness and Strategy for Cybersecurity, *Organisational Structure*, http://www.nisc.go.jp/about/organize.html.

16 National Center of Incident Readiness and Strategy for Cybersecurity, *Cybersecurity Framework in the Government of Japan* (handout), September 2019.

17 *Cyber Security Strategy in Japan: Present Situation and Challenges*, presentation delivered by Tomoo Yamauchi, Deputy Director-General, NISC, to the Foreign Press Center of Japan, 4 July 2019, https://fpcj.jp/wp/wp-content/uploads/2019/07/190704-Cybersecurity-StrategyForeign-Press-Center-1.pdf.

18 Ministry of Defense, 'Regarding Response to Cyber Attack', undated, https://www.mod.go.jp/e/publ/answers/cyber/index.html.

19 Franz-Stefan Gady and Yuka Koshino, 'Japan and Cyber Capabilities: How Much Is Enough?', Military Balance blog, International Institute for Strategic Studies, 28 August 2020, https://www.iiss.org/blogs/military-balance/2020/08/japan-cyber-capabilities.

20 'Japan Embraces AI Tools to Fight Cyberattacks with US$237 Million Investment', *CISO Magazine*, 6 April 2020, https://cisomag.eccouncil.org/japan-embraces-ai-tools-to-fight-cyberattacks-with-us237-mn-investment.

21 Daishi Abe, 'Lagging China and the US, Japan to beef up cyberdefense', Nikkei Asia, 20 June 2020, https://asia.nikkei.com/Politics/Lagging-China-and-the-US-Japan-to-beef-up-cyberdefense.

22 DIH is Japan's largest intelligence organisation, with around 2,000 personnel in 2020.

23 Samuels, *Special Duty: A History of the Japanese Intelligence Community*, p. 232.

24 Ministry of Defense, *Defense Programs and Budget of Japan: Overview of FY2020 Budget Request*, 2019, https://www.mod.go.jp/e/d_act/d_budget/pdf/200225a.pdf.

25 Longmei Zhang and Sally Chen, 'China's Digital Economy: Opportunities and risks', International Monetary Fund Working Paper, no. WP/19/16, 17 January 2019, p. 4, https://www.imf.org/en/Publications/WP/Issues/2019/01/17/Chinas-Digital-Economy-Opportunities-and-Risks-46459.

26 For technology companies in 2020, see https://fortune.com/global500/2020/search/?sector=Technology. For telecoms

companies in 2020, see https://fortune.com/global500/2020/search/?sector=Telecommunications.

27 Hiroshi Fujiwara, 'Why Japan leads industrial robot production', International Federation of Robotics (IFR), 17 December 2018, https://ifr.org/post/why-japan-leads-industrial-robot-production.

28 OECD, *Japan*, OECD Economic Surveys, April 2019, p. 44, https://www.oecd-ilibrary.org/economics/oecd-economic-surveys-japan-2019_fd63f374-en.

29 Osamu Tsukimori, 'Japanese manufacturers use decades of experience to dominate key chemical market for cutting edge chips', *Japan Times*, 9 October 2019, https://www.japantimes.co.jp/news/2019/10/09/business/japanese-manufacturers-use-decades-experience-dominate-key-chemical-market-cutting-edge-chips/#.Xc7ePS10eHo.

30 Nippon Telegraph Telephone (NTT) Group, https://www.ntt.co.jp/index_e.html.

31 Ipv6 Test, 'IPv6 in Japan', October 2019, https://ipv6-test.com/stats/country/JP.

32 NTT WE Marine, 'Cable-Laying Vessels', https://www.nttwem.co.jp/english/ship.

33 OECD, *Japan*, OECD Economic Surveys, April 2019, p. 44.

34 BBC News, 'Japan's cyber-security minister has "never used a computer"', 15 November 2018, https://www.bbc.co.uk/news/technology-46222026.

35 Ministry of Economy, Trade and Industry, *The Cyber/Physical Security Framework: To ensure trusthworthiness of a new type of supply chain in 'Society 5.0', so-called 'value creation process'*, 18 April 2019, https://www.meti.go.jp/english/press/2019/pdf/0418_001b.pdf.

36 Ministry of Economy, Trade and Industry, *Cyber/Physical Security Framework (CPSF) Formulated*, 18 April 2019, https://www.meti.go.jp/english/press/2019/0418_001.html.

37 *Ibid.*

38 Gleb Chuvpilo, 'AI Research Rankings 2020: Can the United States Stay Ahead of China?', 21 December 2020, https://chuvpilo.medium.com/ai-research-rankings-2020-can-the-united-states-stay-ahead-of-china-61cf14b1216.

39 *Ibid.*

40 Ministry of Defense, *Defense of Japan 2019*, 2019, p. 229, https://www.mod.go.jp/e/publ/w_paper/wp2019/pdf.

41 Cabinet Office, 'Juntenchōeisei shisutemu ni tsuite', undated, https://www8.cao.go.jp/space/qzs/qzs.html.

42 Quasi-Zenith Satellite System (QZSS), 'Overview of the Quasi-Zenith Satellite System (QZSS)', https://qzss.go.jp/en/overview/services/sv01_what.html.

43 Quasi-Zenith Satellite System (QZSS), '[Report] Deliberations on QZSS at the 7th Session of the IMO's NCSR', 5 March 2020, https://qzss.go.jp/en/events/imo_200305.html.

44 Ministry of Defense, *Defense of Japan 2020*, pp. 266–7.

45 National Center of Incident Readiness and Strategy for Cybersecurity, *Cybersecurity Strategy*, 27 July 2018.

46 National Center of Incident Readiness and Strategy for Cybersecurity, 'Summary of Cybersecurity Policy for CIP (4th Edition)', 25 July 2018, https://www.nisc.go.jp/eng/pdf/cs_policy_cip_eng_v4_summary.pdf.

47 Mihoko Matsubara, 'A Glimpse into Private Sector Security in Japan', Lawfare, 26 June 2018, https://www.lawfareblog.com/glimpse-private-sector-cybersecurity-japan.

48 National Center of Incident Readiness and Strategy for Cybersecurity, 'The Guidance on Operations of Information Security Measures of Government Agencies and Related Agencies', 31 August 2016, Revised 25 July 2018, https://www.nisc.go.jp/eng/pdf/shishin30-en.pdf.

49 Information Technology Promotion Agency, 'Fact-finding survey on corporate CISOs and promotion of security measures', 25 March 2020, https://www.ipa.go.jp/security/fy2019/reports/2019DL_index.html.

50 Ministry of Economy, Trade and Industry, 'Cybersecurity Management Guidelines Revised', press release, 16 November 2017, https://www.meti.go.jp/english/press/2017/1116_001.html.

51 National Center of Incident Readiness and Strategy for Cybersecurity, 'The Guidance on Operations of Information Security Measures of Government Agencies and Related Agencies'.

52 International Telecommunication Union, 'Global Cybersecurity Index 2018', p. 62, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

53 'Jūyō infura 14 bun'ya ni yoru bun'ya ōdan-teki enshū o kaisai, yaku 5, 000-mei ga sanka (NISC)', ScanNetSecurity, 12 November 2019, https://scan.netsecurity.ne.jp/article/2019/11/12/43217.html.

54 'Inauguration and Initiatives of the Cyber Defense Council', *Japan Defense Focus*, no. 44, September 2013, https://www.mod.go.jp/e/jdf/sp/no44/sp_activities.html#article03.

55 Ministry of Foreign Affairs, Cybersecurity presentation, undated, https://www.mofa.go.jp/files/000412327.pdf.

56 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.

57 United Nations, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 22 July 2015, https://www.un.org/ga/search/view_doc.asp?symbol=A/70/174.

58 Ministry of Defense, *Defense of Japan 2019*.

59 Council of Europe, 'Japan joins Budapest Convention', press release, 3 July 2012, https://www.coe.int/en/web/cybercrime/news/-/asset_publisher/S73WWxscOuZ5/content/japan-joins-budapest-convention?inheritRedirect=false.

60 'Asean cybersecurity centre opens in Bangkok', *Bangkok Post*, 14 September 2018, https://www.bangkokpost.com/world/1540082/southeast-asian-cyber-security-centre-opens-in-thailand.

61 NATO Cooperative Cyber Defence Centre of Excellence (CCD COE), 'Japan to Join the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn', press release, 12 January 2018, https://ccdcoe.org/news/2018/japan-to-join-the-nato-cooperative-cyber-defence-centre-of-excellence-in-tallinn.

62 NATO Cooperative Cyber Defence Centre of Excellence, 'About Us', https://ccdcoe.org/about-us.

63 Ministry of Defense, 'Participation in NATO Cyber Defence Exercise "Cyber Coordination 2019"', press release, 27 November 2019, https://www.mod.go.jp/j/press/news/2019/11/27a.html.

64 Ministry of Defense, *Defense of Japan 2019*.

65 Asia Pacific Computer Emergency Response Team, 'TSUBAME Working Group', https://www.apcert.org/about/structure/tsubame-wg/index.html.

66 The latest trilateral dialogue was held in December 2020. See Ministry of Foreign Affairs of Japan, 'The 5th Trilateral Cyber Policy Consultation', 10 December 2020, https://www.mofa.go.jp/press/release/press24e_000019.html.

67 Wilhelm M. Vosse, 'Japan's Cyber Diplomacy', Research in Focus, EU Cyber Direct, October 2019, https://eucyberdirect.eu/wp-content/uploads/2019/10/vosse_rif_topublish.pdf.

68 European Commission, 'European Commission adopts adequacy decision on Japan, creating the largest area of safe data flows', press release, 22 January 2019, https://ec.europa.eu/commission/presscorner/detail/en/IP_19_421.

69 Franz-Stefan Gady, 'Toothless tiger: Japan Self-Defence Forces', BBC News, 14 October 2015, https://www.bbc.com/news/world-asia-34485966.

70 See Daisuke Akimoto, 'Cybersecurity and Japan's Right to Self-Defense', Institute for Security and Development Policy, undated, https://isdp.eu/cybersecurity-japans-right-to-self-defense.

71 Also, in 2019, according to a media report, the Ministry of Defense contracted private-sector companies to develop offensive cyber capabilities for defensive purposes. See 'Japan to develop 1st defense use computer virus against cyberattacks', *Kyodo News*, 30 April 2019, https://english.kyodonews.net/news/2019/04/e9e4df950d3d-japan-to-develop-1st-defense-use-computer-virus-against-cyberattacks.html.

72 Ministry of Defense, *Defense of Japan 2020*, p. 218.

73 See Franz-Stefan Gady and Yuka Koshino, 'Japan and Cyber Capabilities: How Much Is Enough?', Military Balance blog, International Institute for Strategic Studies, 28 August 2020, https://www.iiss.org/blogs/military-balance/2020/08/japan-cyber-capabilities.

74 US Department of Defense, 'The Guidelines for U.S.–Japan Defense Cooperation'.