RESEARCH IN FOCUS

Japan's cybersecurity policy: an introduction

Julia Schuetze
July 2020

EU CYBER DIRECT
Supporting EU Cyber Diplomacy

This project is funded by the European Union.

Contents

Disclaimer

This paper is an introductory summary of Japanese cybersecurity policy that aims to give a broad overview and increase the basic understanding about Japan's approach. The author leveraged the expertise and experience of cybersecurity researchers and other experts from/in Japan. All interviews were held under the Chatham House Rules. The author thanks all experts. The content of this publication does not reflect the official opinion of the European Union. Responsibility for the information and views expressed therein lies entirely with the authors.

Abstract

Japan's cybersecurity policy and international engagements on cybersecurity have been developing rapidly. This paper aims to give a current (2018–2019) state of affairs taking into account that the field of cybersecurity and Japan's approach towards solving cybersecurity challenges are changing fast. It therefore aims to provide a bigger picture in order to introduce scholars, policymakers and interested individuals to different aspects of how Japan approaches cybersecurity challenges. It is an easy first introduction to important issues in fostering international engagement with Japanese stakeholders. The paper starts with an overview of Japan's main policies—strategies implemented in 2018 and 2019—and analyses which issues drive cybersecurity policy development in Japan. This is followed by an overview of main stakeholders, focusing on the relationships between them. Finally, the paper touches on the extensive international activities of Japanese stakeholders, highlighting that Japan's international work on cybersecurity is vast and ownership is taken by domestic ministries as much as the Ministry of Foreign Affairs.

Key takeaways

- Japan's cybersecurity policies and architecture have been advancing since 2015, with the Tokyo 2020 Olympic and Paralympic Games (now rescheduled for 2021) and the vision for a Society 5.0 being the main catalysts for rapid actions addressing vulnerabilities and threats.
- The Japanese government relies on Public Private Partnerships and Public Civil Partnerships to tackle cybersecurity challenges such as a lack of cybersecurity workforce, information sharing and incident response.
- Japan is applying similar policy instruments to those of the EU and the US to address common challenges of Internet of Things (IoT) security and supply chain security, such as certifications, minimum standards and transparency requirements. In the development of policies, Japan already puts particular emphasis on building mutual recognition systems among the US and Europe, aiming to prevent the spread of unique rules that distort private entities' activities. This is done by allowing international comments on draft frameworks and developing correspondence tables to other standards.
- Domestically, Japan is piloting some new approaches to address cybersecurity challenges, for example its distinct use of cybersecurity workforce training programs and rotation of staffers among ministries and its information security agency to tackle the workforce shortage as well as testing preventative scanning of IoT devices more broadly to achieve password security.
- Japan's international cybersecurity policy and engagements are shaped by domestic and foreign priorities of different ministries that address cybersecurity vulnerabilities and threats in Japan and abroad.

1 Introduction

Japan's cybersecurity policy and international engagements on cybersecurity have been developing rapidly since 2015, driven by the administration of Prime Minister Shinzo Abe, the Olympic Games 2020 in Tokyo and the vision for an interconnected society. Authors[1] have focused on various aspects of Japan's cybersecurity policy describing its cybersecurity policy development and evaluating its cyber readiness and its approach specifically towards cyber diplomacy. This paper aims to give a current (2018–2019) state of affairs, taking into account that the field of cybersecurity and Japan's approach to solving cybersecurity challenges are changing fast. The paper therefore aims to provide a bigger picture in order to introduce scholars, policymakers and interested individuals to different aspects of how Japan approaches these challenges. It should be read as an explanatory summary highlighting some recent developments as well as some unique approaches Japanese stakeholders are taking. The paper briefly notes Japan's main vulnerabilities, threats and priorities in cyberspace, and gives an overview of its main policies, strategies and stakeholders. It touches on some unique policy instruments and explains the relationships among the different actors. There is a short overview of Japan's international activities, highlighting that its international engagements are vast and ownership depends on the individual ministry's responsibilities. As Japan's international work on cybersecurity is well developed, it may provide a starting point for international stakeholders to engage with Japan.

2 Legal and regulatory landscape

This paper highlights developments in the legal and regulatory landscape of 2018 and 2019. For a more historic overview please refer to Gady (2017).[2]

2.1 Japan's cybersecurity strategy 2018

Japan's 2018 cybersecurity strategy[3] focuses on the goals of achieving Society 5.0 while taking account of threats and vulnerabilities that these developments would bring.[4] In order to tackle the challenges, Japan domestically developed policies and adopted its cybersecurity architecture accordingly. It moreover seeks diplomatic over military solutions and makes use of international engagement as a means to prevent, detect and respond to malicious cyber activities. The 2018 Cybersecurity Strategy of Japan reflects the paradigm shift towards Society 5.0 and developments since 2015 such as increasing seriousness of threats in cyberspace and the necessity of securing the Games of the XXXII Olympiad and the Tokyo Paralympic Games. The Cybersecurity Strategy of 2018 also reflects supply chain security and the establishment, and international delivery of a model for addressing vulnerabilities of IoT devices which is to be developed.

The **visions and objectives** of the strategy are to ensure a 'free, fair and secure cyberspace', the free flow of information, the rule of law, openness, autonomy, and collaboration among stakeholders.

The **goals** of the 2018 strategy are cybersecurity for sustainable development and the promotion of a 'Cybersecurity Ecosystem'.

---

[1] Melissa Hathaway, 'Japan: Cyber Readiness At A Glance,' Potomac Institute for Policy Studies, 2016, http://www.potomacinstitute.org/images/CRI/CRI_Japan_Profile_PIPS.pdf.
Franz-Stefan Gady, 'Japan: The Reluctant Cyberpower,' *Asie.Visions*, No. 91, Ifri, March 2017, https://www.ifri.org/sites/default/files/atoms/files/gady_japan_reluctant_cyberpower_2017.pdf.
Wilhelm M. Vosse, 'Japan's Cyber Diplomacy,' Research Focus, EU Cyber Direct, 18 October 2019, https://eucyberdirect.eu/content_research/japans-cyber-diplomacy/.

[2] Franz-Stefan Gady (2017), 'Japan: The Reluctant Cyberpower.'

[3] The Government of Japan, 'Cybersecurity Strategy,' provisional translation, 27 July 2018, https://www.nisc.go.jp/eng/pdf/cs-senryaku2018-en.pdf.

[4] The Government of Japan, 'Cybersecurity Strategy.'

In order to these visions, objectives and goals the Japanese government takes three **approaches**: (1) Mission Assurance for Service Providers, meaning that it aims to ensure a free and open cyberspace; (2) risk management to ensure cybersecurity; (3) participation, cooperation, and collaboration.

2.2 Regulations and guidelines for the protection of critical infrastructure 2018

To achieve security of critical infrastructure, Japan takes a voluntary approach. It encourages the sharing of threat information and incidents among private-sector actors and cooperation of critical infrastructures with relevant ministries in case of serious incidents, as described in the updated **Cybersecurity Policy for Critical Infrastructure Protection (4th edition)** (revised July 2018).[5] This policy focuses specifically on the promotion of activities for reducing critical infrastructure services' (CISs) outage risk that could be the result of cyberattacks or natural disasters. It also ensures resilience and that essential services for organising the Olympic and Paralympic games will be secured. The policy looks to create effective information-sharing mechanisms by diversifying the contact points (anonymisation, sharing via the Capabilities for Engineering of Protection, Technical Operation, Analysis, and Response (CEPTOR) Secretariat, cybersecurity-related agencies). Moreover, it defined the go-to ministries for critical infrastructure protection.[6]

Japan recently also updated the **Guideline for Establishing Safety Principles for Ensuring Information Security of Critical Infrastructure (5th edition)** (April 2018) and issued the **Risk Assessment Guide Based on the Concept of Mission Assurance in Critical Infrastructure** (April 2018)[7]. These documents assist the private sector in creating cybersecurity and adopting relevant mechanisms that support general information technology (IT) security.

Uniquely, a **Common Standard on Information Security Measures of Government Entities** is developed by each ministry that applies and reviews the policy.

Moreover, part of the developments is a **Cybersecurity Human Resources Development Plan** and a **Cybersecurity Research and Development Strategy**.

To protect critical infrastructure and assure the implementation of Society 5.0, the Ministry of Economy, Trade and Industry's (METI) **Framework on Cyber/Physical Security**[8] was put out for feedback in December 2018 and finalised in 2019. It focuses on a new Society 5.0 where cyberspace and physical spaces are highly integrated. METI calls this the value creation process. Because cyber threats are growing through this evolving supply chain, METI developed a framework for establishing security guidance to secure this value creation process. The guidelines are, however, flexible and voluntary, aimed at different levels of cybersecurity professionals and looking at aspects of cybersecurity from policies and methods to risk assessment. They focus on three layers (connection between organisations, mutual connection between cyberspace and physical space, and connection in cyberspace) and present policy and security measures for each risk source for six elements (organisation, people, components, data, procedure, and system).

[5] Cybersecurity Strategic Headquarters, Government of Japan (2017), 'The Cybersecurity Policy for Critical Infrastructure Protection (4th Edition),' tentative translation, http://www.nisc.go.jp/eng/pdf/cs_policy_cip_eng_v4_r1.pdf.

[6] The five ministrie responsible s for critical infrastructure are FSA (Financial), MIC (Info & Comm, Admin), MHLW (Medical, Water), METI (Electric power supply, Gas, Chemical, Credit card, Petroleum), MLIT (Aviation, Airport, Railway, Logistics).

[7] Find the newest documents here: http://www.nisc.go.jp/eng/.

[8] METI (2019), 'Cyber/Physical Security Framework (CPSF) Formulated,' 18 April 2019, https://www.meti.go.jp/english/press/2019/0418_001.html.

2.3 Cyber defence strategy 2018

A new defence strategy[9] was published in 2018, which creates more capabilities and establishes a cyber operation unit. A Cabinet Decision also established cyberspace as a new defence domain. In the realm of local threat actors such as China, North Korea, and Russia, which use cyber capabilities for espionage and in international conflicts against Japan, cyber defence becomes more important. Hideaki Watanabe, Former Commissioner of the Acquisition, Technology and Logistics Agency, Ministry of Defence, said at the Tokyo Cyber Initiative conference in December 2019 that government agencies receive attacks every day and that the level of sophistication is increasing. Further, he said that the Japanese government has therefore taken a multi-dimensional approach to its defence capability that includes cybersecurity in all traditional military domains. He said that cross-domain attacks are going to be rising and that this is what the Defence Ministry would be calling cyberwar. Watanabe further explains that since 2014 the Defence Ministry has started to develop a cyber defence team, the Japan Self Defence Force (JSDF), comprising roughly 150 people in December 2019. This team is organised under the Minister and has focused on cooperation with the private-sector defence industry. It has set up a US–Japan cyber working policy group to exchange information with the US. To tackle the workforce shortage, the Defence Ministry has set up a new programme for cybersecurity professionals called 'Capture the Flag'.[10]

In terms of offensive capabilities, Shinzo Abe repeatedly stated that the reinterpretation of Article 9 of Japan's pacifist constitution (the 2015 'Legislation for Peace and Security') does not apply to JSDF activities in cyberspace. Therefore, the Ministry of Defence 'will be confined to studying offensive cyberwar techniques as the Japanese government continues to debate whether the JSDF are allowed to conduct cyberattacks in defense of military networks'.[11]

2.4 Policy priorities: securing 'Society 5.0' and the Olympic Games

The main priorities for Japan are the successful realisation of Society 5.0, of which cybersecurity is a prerequisite, and the protection of Tokyo Olympic Games.

2.4.1 Society 5.0

Japan's main concern is any vulnerabilities and threats that could impact the successful realisation of its vision for the Society 5.0.[12]

The **goals of Society 5.0** are the systematic integration of digital technologies and the physical world to spur economic growth and provide solutions to social challenges. Society 5.0 is a roadmap concept that governs Japan's unique position and role in mastering the potentials of digitisation and connectivity.[13] The development of digital infrastructure is welcomed as a strategy to cope with labour shortages and a declining population. Japan already has an advanced digital economy IT industry,[14] which is expected to grow even more as part of Society 5.0. But due to the rising level of digitisation

[9] Ministry of Defence, Defense of Japan 2018, http://www.mod.go.jp/e/publ/w_paper/2018.html.

[10] Mark Pomerleau, 'A First in Cyber "Capture the Flag",' 22 August 2019, https://www.fifthdomain.com/show-reporter/technet-augusta/2019/08/22/a-first-in-cyber-capture-the-flag/.

[11] Franz-Stefan Gady, 'Japan's Defense Ministry Plans to Boost Number of Cyber Warriors,' *The Diplomat*, 17 July 2017, https://thediplomat.com/2017/07/japans-defense-ministry-plans-to-boost-number-of-cyber-warriors/.

[12] Cabinet Public Relations Office, Cabinet Secretariat, The Government of Japan (2018), 'Realizing Society 5.0,' https://www.japan.go.jp/abenomics/_userdata/abenomics/pdf/society_5.0.pdf; 'Facing Cyber Attacks, the Japanese Experience,' Institut Montaigne, 13 March 2019, https://www.institutmontaigne.org/en/events/facing-cyber-attacks-japanese-experience.

[13] Franz Waldenberger, 'Society 5.0,' International Reports of the Konrad-Adenauer-Stiftung, 2018, http://www.kas.de/wf/en/33.52119/.

[14] EU–Japan Centre for Industrial Cooperation, 'Digital Economy in Japan and the EU – An Assessment of the Common Challenges and the Collaboration Potential,' March 2015, https://www.eu-japan.eu/sites/default/files/publications/docs/digitaleconomy_final.pdf.

and dependencies on information and communications technology (ICT), the country is vulnerable to cyberattacks.

Flagship projects[15] for the realisation of Society 5.0 are for example:

- Automated mobility systems
- Data-driven healthcare systems
- Smart energy management and finance
- Digital government
- Smart industry, community and small and medium enterprises (SMEs)

An example of a successful cyberattack that most Japanese citizens remember was when pension information was leaked in 2015.[16]

As Society 5.0 imagines a cyber–physical world, Japan is especially worried about **vulnerabilities of IoT devices**. In a 2019 presentation,[17] Reiko Kondo, Director-General for Cybersecurity, Ministry of Internal Affairs and Communications (MIC) highlighted that the National Institute of Information and Communication Technology (NICT), Japan's primary national research institute for information and communications, was observing cyberattacks globally by monitoring 3,000,000+ unused Internet Protocol (IP) addresses (in the darknet). Kondo showed that 'more than half were attacking IoT devices' and that 'attacks to IoT devices increased by 5.7 times from 2015–2017'. A Cybersecurity Task Force administered by MIC was therefore set up in October 2017 and introduced a comprehensive package of IoT security measures whose main goal is to measure IoT devices' vulnerabilities, covering the entire lifecycle (design, development, sales, installation, operation & maintenance and use).[18] Japan is also using a proactive approach to tackle specifically the threat of DDoDs attacks on IoT devices.

To tackle specifically the threat of DoDs attacks on IoT devices, the **Telecommunication Act** was revised in 2018. This amendment was to enable a program called NOTICE that would prevent IoT devices turning into a DDoS botnet and allow the discovery of vulnerable IoTs by login attempts. The amendment explicitly excludes this program from 'unauthorised computer access' for five years so that NICT can actively scan IoT devices over the Internet and identify IoT devices with improper password settings. The ICT Information Sharing and Analysis Center) (ICT-ISAC) Japan under recognition of MIC became, in accordance with the changes of the NICT Act, the third party, working as an information-gathering hub with firm security measures to manage sensitive information. It is therefore the recognised association for anti-DDoS: the new operations include SMPs (switched-mode power supply) that can share the log data including the source of information. The ICT Information Sharing and Analysis Center) (ICT-ISAC) will request other Internet service providers (ISPs) that are responsible for the source IPs, then conduct research to determine the source and command and control (C&C) server; then on request ISPs act for vulnerable IoT devices.[19] This program was reported in Europe as a 'hacking program' but, to be clear, the Japanese government will not monitor the substance of the communication or details of routers, webcams, and sensors with global IP version 4 (IPv4) addresses in Japan. It is a Public Private Collaboration among MIC, NICT and ISPs. NICT is responsible for research and sharing results with ISPs, ISP will notify owners, and MIC operates support centres. Also, a revision of IoT device regulation is

[15] 'OECD Economic Surveys: Japan,' April 2019, p. 36. https://www.oecd.org/economy/surveys/Japan-2019-OECD-economic-survey-overview.pdf.

[16] Tomoko Otake (2015), '1.25 million affected by Japan Pension Service hack,' *Japan Times*, 1 June 2015, https://www.japantimes.co.jp/news/2015/06/01/national/crime-legal/japan-pension-system-hacked-1-25-million-cases-personal-data-leaked/.

[17] Reiko Kondo, 'IoT Security Measures in Japan,' 24 January 2019, https://www.eunity-project.eu/m/filer_public/4d/ff/4dff1a1a-b95e-4afe-8d52-e79f88336fdf/ecso-eunitymic.pdf.

[18] Mihoko Matsubara, 'Assessing Japan's Internet of Things (IoT) Security Strategy for Tokyo 2020,' 19 September 2016, https://blog.paloaltonetworks.com/2016/09/cso-assessing-japans-internet-of-things-iot-security-strategy-for-tokyo-2020/.

[19] Reiko Kondo, 'IoT Security Measures in Japan,' p. 5.

planned: MIC plans a ministerial ordinance to revise IoT device regulation such as technical standards conformity certification, so-called GI-Teki.

2.4.2 The Olympic Games 2020

The upcoming Olympic Games 2020 (rescheduled for 2021) and the Paralympic Games in 2021 are seen as a major catalyst to Japan's cybersecurity architecture caused by major events' specific threats and vulnerabilities. Japanese cybersecurity experts prepare, for example, for targeted cyber operations on critical infrastructure by terrorists or states. In order to build resilient critical infrastructure, Japan focused on a national security exercise in 2018 to test its crisis communication process.

In terms of vulnerabilities and threats, special attention has been placed since 2015 on securing the 2020 Olympic Games.[20] Dion Schwartz et al. (2019)[21] analysed the threat landscape for the mega event. They identified four high-level threat categories:

- **Targeted attacks** aimed at high-profile Olympic assets, individuals, or organisations (e.g. broadcasting systems, Olympic commissioners, Japanese cybersecurity organisations), for either financial or political gain, could result in severe breaches or financial or reputational losses.
- **DDoS attacks** against Tokyo 2020 infrastructure or associated networks could disrupt the availability of services or distract from other ongoing attacks. DDoS attacks could be launched by advanced threat actors such as nation states, or less sophisticated groups such as hacktivists. Particular attention should be paid to developments in DDoS methods, including IoT–powered botnets.
- **Ransomware attacks** could affect a wide range of devices, services, and underlying infrastructure supporting the Olympics, including participant and visitor devices, transportation services, and point-of-sale systems.
- **Cyber propaganda or misinformation** could be deployed to cause reputational loss for individuals, sponsor organisations, or the host nation. It could also be deployed for political purposes or to disrupt the Olympic Games themselves.

‘

Japan has always put emphasis on international engagement even when its own 'whole of government approach' to cybersecurity is still under development.

Moreover, worst-case scenarios imagined by Japanese cybersecurity experts take account of **broader attacks that would aim to cause panic**. For example, 'hackers could use a cyberattack to show a fake emergency alert, for example, for a large earthquake or nuclear accident, on the electronic scoreboard during the opening ceremony and then fly dozens of drones capable of jamming mobile signals, causing a huge panic'.[22] Another scenario that Japan prepares for is **attacks against the building control system**, as such cyberattacks on critical infrastructures are increasing. 'Building control systems have seen cyber attacks on air conditioning systems in hospitals, ransomware infection of a

[20] Cabinet Public Relations Office, Cabinet Secretariat, Information Security Policy Council, 'The Prime Minister in Action,' 19 May 2014, https://japan.kantei.go.jp/96_abe/actions/201405/19jouhou.html.

[21] Cynthia Dion-Schwarz et al., 'Olympic-Caliber Cybersecurity: Lessons for Safeguarding the 2020 Games and Other Major Events,' Rand Corporation, 2018, https://www.rand.org/pubs/research_reports/RR2395.html.

[22] Quoted from *Japan Times*, Cyberthreats bound to expand ahead of 2020 Games, experts warn,' 18 July 2019, https://www.japantimes.co.jp/news/2019/07/18/national/cyberthreats-bound-expand-ahead-2020-games-experts-warn/#.Xg3yIEdKjIU.

hotel's electronic key management system and DoS attacks on the stadium power control system at the London Olympic Games opening ceremony.'[23] On top of the technological threats, some experts are seeing Japan's risk assessment and crisis response as a vulnerability.

3 Institutional landscape and key stakeholders

Japan is on the path to becoming 'cyber ready'.[24] This is reflected in its cybersecurity architecture. Its cybersecurity policies and authorities are still somewhat fragmented and complex, with a governance structure that spreads the responsibility for cybersecurity among different, and often competing, ministries with a strategic body on top, similar to Germany's cybersecurity architecture.[25] Japan has always emphasised international engagement, while its own 'whole of government approach' to cybersecurity is still under development. Gady (2017)[26] judges the phase of international engagement to be ahead of Japan's domestic efforts.

Cyber diplomacy is one of Japan's strong suits.[27] An overview of the stakeholders in cybersecurity governance in Japan will show why certain policies take priority and by whom they are governed. The Japanese government relies on Public Private Partnerships and collaboration with non-governmental organisations (NGOs) and academia as a means to tackle some cybersecurity challenges, such as a lack of cybersecurity workforce, information sharing and incident response.

3.1 Government

Cybersecurity policy within the government is fragmented but coordinated at the cabinet level.

Coordination is oveseen by the **Cybersecurity Strategy Headquarters (CSHQ)**. The CSHQ has the authority and mandate under the cabinet and consists of ministers and notable experts on cybersecurity from the private sector as well as government. It is responsible for preparing the nation's cybersecurity strategy. The Deputy Chief Cabinet Secretary for Information Technology Policy is within the Cabinet's Secretariat, a command and control body of national cybersecurity. The Assistant Chief Cabinet Secretary is responsible for situation response and crisis management. Additionally, the Information Security Policy Council (ISCP) was established in the CSHQ to facilitate an advanced information and telecommunications network society for centralised/cross-cutting promotion of information security measures for the public and private sectors, and works towards improving the level of information security.

NISC borrows staff from other ministries on a rotating basis which aims to connect but also disperse cybersecurity knowledge across ministries over time.

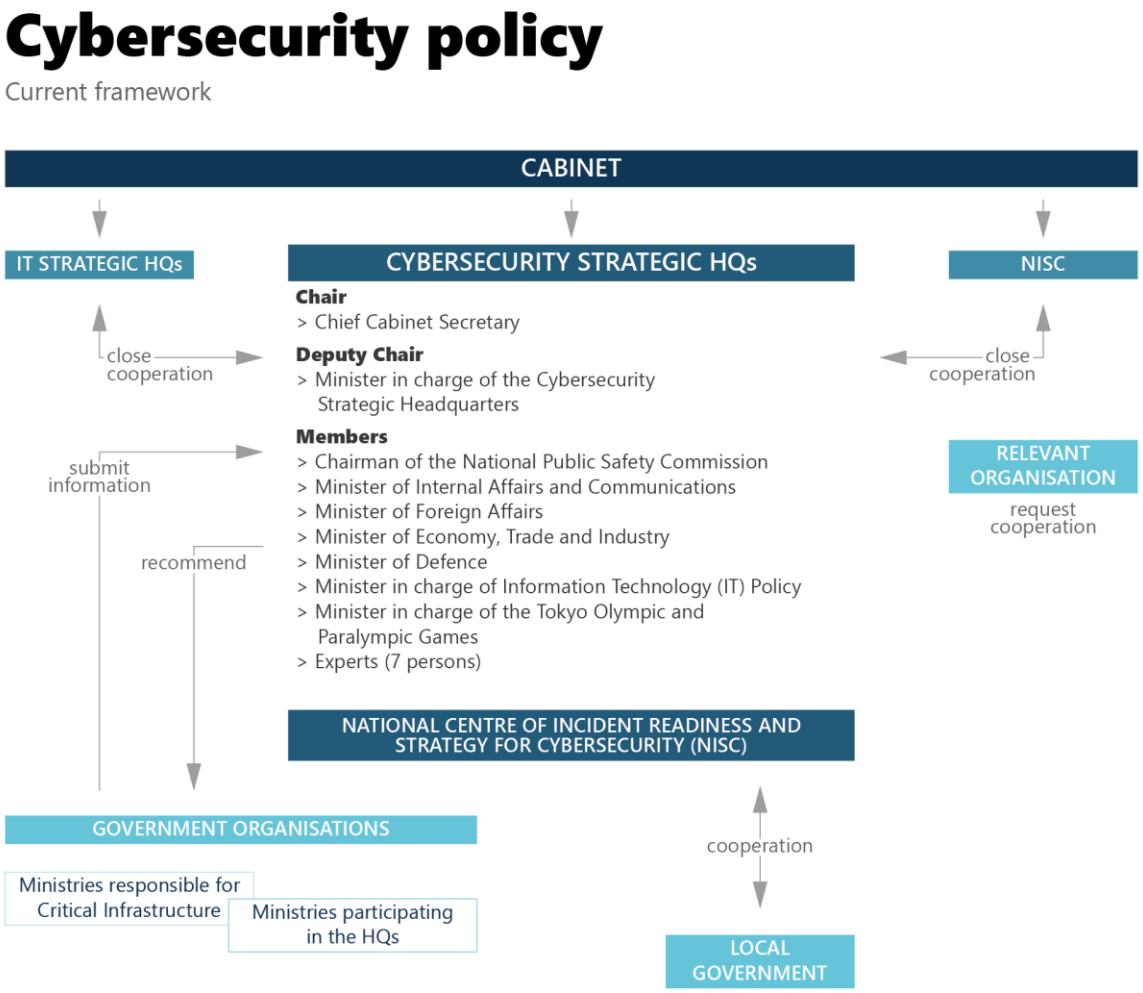
The **National Information Security Centre (NISC)** was established in April 2005 within the Cabinet Secretariat responsible for planning and general coordination related to the basic strategy and other centralised/cross-cutting promotion of information security measures for the public and private sectors. It serves as a secretariat for the CSHQ and integrates and advances cybersecurity policies across government, monitors cyberattacks

[23] Quoted from Steve Rogerson, 'NTT brings cyber security to building control systems,' IMC, 17 July 2018, https://www.iotm2mcouncil.org/nttfaci.
[24] Melissa Hathaway, 'Japan: Cyber Readiness at a Glance.'
[25] Rebecca Beigel and Sven Herpig, 'Zuständigkeiten und Aufgaben in der deutschen Cyber-Sicherheitspolitik,' März 2020, https://www.stiftung-nv.de/de/publikation/akteure-und-zustaendigkeiten-der-deutschen-cybersicherheitspolitik .
[26] Franz-Stefan Gady, 'Japan: The Reluctant Cyberpower.'
[27] Wilhelm M. Vosse, 'Japan's Cyber Diplomacy.'

on government bodies, assists government bodies in case of an attack, and manages Mobile Incident Response Teams. It plays a leading role in cybersecurity policy, which is reflected in the cybersecurity strategy of 2018:

> Towards the realisation of this Strategy, under the Cybersecurity Strategy Headquarters, the related government bodies will keep working on improving their cybersecurity capabilities under the leadership of National Center of Incident Readiness and Strategy for Cybersecurity (NISC), and NISC will play its leading role as the focal point in coordinating intra-government collaboration and promoting partnerships between industry, academia, and the public and private sectors. The Headquarter will seek to secure and execute the budget necessary for the government so that the measures [are] executed.[28]

NISC borrows staff from other ministries on a rotating basis that aims to connect but also disperse cybersecurity knowledge across ministries over time. This allows a constant exchange of experts. NISC responds to and carries out audits, has the authority to conduct investigations, and sets common criteria. NISC also has staff that are paid by companies, and government employees from the police force. NISC is securing the Olympic Games as a whole and acts as an information sharing-platform for critical infrastructure.



Highlighted ministries that are relevant for cybersecurity policy are represented in the CSHQ through the ministers. Nevertheless, every ministry has its own responsibility for IT and cybersecurity within its

[28] NISC, Summary of the Japan's [*sic*] Cybersecurity Strategy, 2018, http://www.nisc.go.jp/eng/pdf/cs-senryaku2018-zentaigaiyou-en.pdf.

respective sector (health, transport, etc.). Also, each ministry has its own computer emergency response team (CERT).

METI is particularly important for cybersecurity as it has the **Information-technology Promotion Agency (IPA)** beneath it, which sets the standards.[29]

The **Ministry of Foreign Affairs' Cybersecurity Policy Division** is, according to the 2016 *Diplomatic Bluebook*, the entity with primary focus on cybersecurity foreign policy.

The **Ministry of Defence** since the 2018 cybersecurity strategy has had the task of defending against state-sponsored attacks.

The Information Security Policy Council Japan and the **Supreme Audit Institution (SAI)** also are active in shaping and implementing cybersecurity policies.

The **MIC** provides cybersecurity education courses and has responsibility over IoT security.

3.2 Private sector

Japan has companies with a global presence on cybersecurity-related services and issues, such as Trend Micro, Softbank, and NTT. Individuals from the private sector (e.g. Hitachi; NTT; members of Keidanren Association, Japan's largest business association; Microsoft Japan) **serve as technical advisers for the government (see Box 1) and may carry out research on cybersecurity policies but are also responsible for the implementation of cybersecurity measures**, such as standards, assisting in securing Tokyo 2020 or holding training and exercises. For example, for the Tokyo 2020 Olympic Committee, Nomura Research Institute and C-CERTJP experts work at NISC. Private companies are **involved in the development of standards and may even initiate them**; for example, the Japan Electrotechnical Standards and Codes Committee developed guidelines for a smart meter system and security guidelines for electric power control systems which were endorsed by METI and made mandatory through the Electricity Business Act 2016. Moreover, the private sector takes the lead in information-sharing efforts on cyber risks and threats. **The Public Private Partnership in information sharing is still fairly new and remains voluntary**. This is a different approach than the EU's NIS framework, which demands that critical infrastructure reports incidents to the government. In Japan, instead the government has assisted and provided budget to set up information-sharing platforms so that private-sector entities can share information among themselves: for example, the Japan Electricity Information Sharing and Analysis Centre shares information related to system vulnerabilities, best practices, and threats, and cooperates with counterparts overseas. The Japanese government supports these efforts but does not require that the information is shared with government agencies: instead, sharing is voluntary. For this, METI has a threat information scheme (J-CSIP) operated by the IPA: a voluntary sharing scheme that started in 2012. But industry actors may also use other platforms to share information.

Private companies are involved in the development of standards and may even initiate them; for example, the Japan Electrotechnical Standards and Codes Committee developed guidelines for a smart meter system and security guidelines for electric power control systems which were endorsed by METI and made mandatory through the Electricity Business Act 2016.

[29] METI, Cybersecurity Management Guidelines Revised, 2017, http://www.meti.go.jp/english/press/2017/1116_001.html.

Some companies are also actively involved in executing policy or advocating for policies: notably the NTT Corporation, a telecommunications company involved in the NOTICE programme (see Box 3) and in the cybersecurity exercises; TMI Law Firm,[30] which advises on cyber diplomacy; the Japan Information Industry Association; and the Japan Electronics and Information Technology Industries Association (JEITA)[31] (involving the suppliers), which has been investigating computer security and technology trends and preparing technical standards. Keidanren is the largest business association and has numerous working groups. They do advocacy in Japan and have for example proposed reinforcing cybersecurity measures, pushing for security by design, raising awareness among top management, spreading recognition that protection is possible, and sharing information across national borders. Keidanren is in favour of making information-sharing cross-border, expanding the ISAC framework, and creating mechanisms to share real-time information with the US and other countries.

Public Private Partnerships are used as a means to tackle some cybersecurity challenges, such as a lack of cybersecurity workforce and information sharing. One example is the Industrial Cybersecurity Centre of Excellence for Industrial Cybersecurity Leaders, a state-of-the-art one-year educational programme.

Box 1. Multi-stakeholder approach: private sector as technical advisers

The Japanese government is looking to include expertise and input from stakeholders outside of the government. One example is a study group on industrial cybersecurity that includes representatives from, for example, Mitsubishi, Japan User Association of Information Systems, and NTT, and is observed by government agencies The working group works on rules and standards but also forms international strategies and concentrates on human resources. Then sector-specific working groups (building, electric utility, defence, smart home) even have representatives outside of the cybersecurity field, such as construction companies and design offices. Together these actors will create guidelines to be followed.

3.3 Academia

Academic institutions are responsible for cybersecurity research and serve as educational foundations for civil servants who enter government jobs after university. Most academic institutions work closely with the government.

The National Institute for Defence Studies (NIDS) supports the Ministry of Defence and researches cyber defence. NIDS has 150 staff members; its main tasks are planning visions, supporting policy concepts, and planning policy research. Its main topics are North East Asia, global challenges, cross-domain challenges and the North Atlantic Treaty Organization (NATO). It has cybersecurity-related engagements and fellowship exchanges with the NATO Cooperative Cyber Defence Centre of Excellence.

The Cybersecurity Research Center at Keio University and the Keio University Global Research Institute (KGRI) also provide research on cybersecurity policy. The EU Cyber Direct project together with KGRI and Mitsubishi Institute held a workshop on joint responses to malicious cyber activities.

Other relevant organisations are **Nagaoka University of Technology, National Institute of Informatics, and National Defence University**. The Japan Network Information Centre is responsible for the Internet Registry and is an active participant in Internet governance, as well as facilitator of Japan's Internet Governance Forum (IGF).

[30] Masaya Hirano asnd Kazuyasu Shiraishi, 'Cybersecurity in Japan,' *Lexology*, 25 February 2019, https://www.lexology.com/library/detail.aspx?g=1e0a8e7a-5347-4b55-bcb5-0765d90f4419.
[31] Japan Electronics and Information Technology Industries Association, 2010, https://www.jeita.or.jp/english/about/what/index.htm.

3.4 Civil society

Civil society is growing slowly in Japan. A possible reason is that Japan's 'Law to Promote Specified Nonprofit Activities' was established only in 1998. Before its passage, the criteria for certification as a corporate aggregate or a foundation were very rigid and difficult for many voluntary organisations: the vertically organised permission and supervision processes were not suitable for most smaller organisations.[32]

As of 2015, the number of non-profit organisations (NPOs) has reached more than 50,000, and 2,977 NGOs are registered as science and technology NGOs. By comparison, in Germany roughly 600,000 NPOs were registered in 2019. The Chaos Computer Club, founded in 1981, is Europe's largest association of hackers, with 7,700 registered members[33]. Nothing comparable exists in Japan.

A large civil society organisation in cybersecurity is the JPCERT/CC, which has official functions for society and business, providing for example incident response (see Box 2).

Another notable NGO is the **Japan Cybersecurity Innovation Committee (JCIC)**,[34] which aims to bridge the gap between government and the private sector. It is looking to provide a neutral platform to solve the aforementioned confusing reporting lines of breach notification.

An important civil society organisation is the Japan Institute for Promotion of Digital Economy and Community (JIPDEC),[35] which works on privacy and security issues[36] and produces non-technical standards of all types (hardware/software etc.) affecting all computer users, with a view to advancing the uptake of IT in Japan. Also significant are the Japan Users Association of Information Systems, Japan Network Security Association, Information Science and Technology Association,[37] and Japan Security and Crisis Management Association.[38] Science and Technology in Society (STS)[39] is a forum that addresses technological change and how it affects society more broadly, cybersecurity challenges included.

[32] Robert Pekkanen (2000), 'Japan's New Politics: The Case of the NPO Law,' *Journal of Japanese Studies*, vol. 26, no. 1 (2000), pp. 111–48, https://www.jstor.org/stable/133393?seq=1.
[33] Elizabeth Grenier, 'Die Deutschen und ihre Vereine,' *DW*, 1 May 2019, https://www.dw.com/de/die-deutschen-und-ihre-vereine/a-48403682.
[34] JCIC, 'A Hub for every initiative to achieve a secure and safe digitalized society,' 2019, https://www.j-cic.com/en/vision.html.
[35] JIPDEC, 2019, https://english.jipdec.or.jp/
[36] Wikipedia, 'Japan Institute for Promotion of Digital Economy and Community,' https://en.wikipedia.org/wiki/Japan_Institute_for_Promotion_of_Digital_Economy_and_Community, retrieved 15 August 2019.
[37] INFOSTA (Information Science and Technology Association, Japan), http://www.infosta.or.jp/start_e.html.
[38] JSSC. http://www.jssc.gr.jp/pg102.html.
[39] STS Forum 2019, '16th Annual Meeting Program,' https://www.stsforum.org/kyoto2019/.

Box 2. JPCERT/CC's role in Japan's cybersecurity architecture

Japan has two national computer security incident response teams (CSIRTs). The government agency NISC, which is under the Cabinet Secretariat, is mainly in charge of prevention and response to cyber incidents affecting government agencies and shaping policies. The non-profit JPCERT/CC is focused on prevention, detection and response to cyber incidents that affect businesses and critical infrastructures more broadly. The budget for JPCERT/CC comes from METI. In this Public Civil Partnership, JPCERT/CC has key activities such as incident response (roughly 200,000 incidents per year), handling advanced persistent threat (APT) cases (80% of resources go to this task) and Internet monitoring via TSUBAME, a network traffic monitoring system. TSUBAME is used by many Asian countries and is helpful in seeing what attacks are affecting Asia and Japan.

JPCERT/CC is also the designated vulnerability information contact for Japanese researchers. This information is *not* shared with the government. JPCERT/CC and another designated organisation, the IPA, work as the middle entity between vendor and researcher.

In its international work, JPCERT/CC, for example, helps developing countries with their CSIRTs. Recently JPCERT/CC has been working with African nations to set up their CSIRTs. Its staff also collaborate with other agencies by sharing information on threats in fora such as the Council of Anti-Phishing Japan and Nippon CSIRT Association. JPCERT/CC is a member of the Forum of Incident Response and Security Teams (FIRST) and a founding member of Asia Pacific Computer Emergency Response Teams (APCERT), a community of CSIRTs from the Asia Pacific region. It collaborates with many EU member states' CSIRTs, such as CERT-FR.

4 Japan's international cybersecurity policy and engagements

4.1 Cyber diplomacy

Japan's International Strategy on Cybersecurity Cooperation[40] states that Japan will promote initiatives for international cooperation and mutual assistance in cybersecurity under the common understanding shared by all domestic stakeholders including those from industry, academia and the government.

Japan's cyber diplomacy is well developed.[41] The Ministry of Foreign Affairs (MOFA) is leading international discussions on how to ensure a free, fair, and secure cyberspace, strengthening coordination with other countries.[42]

MOFA cyber diplomacy priorities are the promotion of the rule of law in cyberspace, the development of confidence-building measures, and cooperation on capacity building.

‘

In a multi-stakeholder and cross-government approach, Japan actively contributes to the shaping of a free, safe, and secure cyberspace.

In a multi-stakeholder and cross-government approach, Japan actively contributes to the shaping of a free, safe, and secure cyberspace.

Japan takes active part in international rulemaking on the use of cyberspace, develops confidence-building measures through dialogues and information exchange bilaterally and multi-laterally including via regional frameworks such as the Association of Southeast Asian Nations (ASEAN) Regional Forum (ARF), and promotes cybersecurity capacity building. Capacity building is

[40] Information Security Policy Council Japan (2013), International Strategy on Cybersecurity Cooperation – j-initiative for Cybersecurity, http://www.nisc.go.jp/active/kihon/pdf/InternationalStrategyonCybersecurityCooperation_e.pdf
[41] Wilhelm M. Vosse, 'Japan's Cyber Diplomacy.'
[42] MOFA, Japan's Cyber Diplomacy, https://www.mofa.go.jp/files/000412327.pdf.

another important goal for Japan. It is specifically focused on critical infrastructure protection via Meridian and the International Watch and Warning Network (IWWN), which are for government agencies, FIRST, and APCERT.

Japan's goal is to not leave any regions in the international community vulnerable to cybersecurity threats. It contributes actively to capacity-building activities at the global level, including support for human resources development and for establishing incident response and information-sharing mechanisms.[43]

On the topics of international norms and international law, led by MOFA, Japan has been involved in efforts to govern cyberspace via the United Nations (UN), where it took part in the discussions at the Group of Governmental Experts (GGE) and contributed to the drafting of the report. The government considers it more realistic to develop legally non-binding soft norms for the short term. MIC and MOFA signed the Paris Call in 2018. At the same time, the Japanese government rejects approaches promoting excessive state control in cyberspace. Japan is of the view that existing international law, including the UN Charter and international humanitarian law, applies to state acts in cyberspace. It was the first Asian country to sign and ratify the Budapest Convention and is promoting this instrument with Asian partners; it joined the Global Alliance against Sexual Abuse Online. It advocated for international rule setting at the G8, the ARF, the Organisation for Economic Co-operation and Developmen (OECD), the Asia-Pacific Economic Cooperation (APEC) and NATO.

Japan's main partner is the US, as reflected in the many US–Japan cybersecurity policy engagements:

- Japan–US Cyber Dialogue
- Japan–US Policy Cooperation Dialogue on the Internet Economy
- Information-sharing processes on threats
- Cyber-incident response mechanisms via the Japan–US Security Arrangements
- US–Japan Cyber Defense Policy Working Group
- US–Japan joint cyber defence exercise

In Southeast Asia Japan takes a leading role in terms of capacity building and technical expertise as well as contributing to information sharing in the region:

- ASEAN–Japan Information Security Policy Meeting
- ASEAN–Japan Cybersecurity Capacity Centre in Thailand[44]
- JASPER - Japan–ASEAN Security Partnership

[43] OECD, 'Japan's Information Security Initiatives,' 2019, http://www.oecd.org/japan/japansinformationsecurityinitiatives.htm.

[44] Priyankar Bhunia, 'ASEAN-Japan Cybersecurity Capacity Building Centreto be launched in Thailand in June 2018,' *Open Gov*, 3 March 2018, https://www.opengovasia.com/articles/asean-japan-cybersecurity-capacity-building-centre-to-be-launched-in-thailand-in-june-2018.

> TSUBAME project cooperating with CSIRTs in the Asia region and installing sensors in CSIRTs.

These are just a few examples of instruments Japan uses in its cyber diplomacy. More were studied by Vosse.[45]

4.2 International engagement of domestic ministries and agencies

METI fosters the development of mutual recognition systems by allowing international stakeholders to comment on the draft framework and creating correspondence tables between the framework and other standards.

In its policy development, Japan is prioritising international solutions alongside domestic solutions. Examples are solutions for cybersecurity challenges related to digital economy. Here Japan aims to take the approach of *'building mutual recognition systems among Japan, the US and Europe; preventing spread of unique rules which distort private entities' activities'*.[46] Therefore, Japan is looking to build a platform that would establish a comprehensive cybersecurity evaluation and verification process for encouraging market access of reliable security products. METI formulated the Cyber/Physical Security Framework (CPSF)[47] and is developing sector-specific security guidelines under this concept. METI fosters the development of mutual recognition systems by allowing international stakeholders to comment on the draft framework and creating correspondence tables between the framework and other standards. Entities can use this framework along with the standard risk management process adopted in ISO31000 and ISO/IEC27001 standards. Additionally, there are correspondence tables between the framework and other standards such as NIST by the US.[48] This is so that a foreign enterprise can show that its security treatment is sufficient based on the other standards. This approach is reflected in the international engagement of domestic agencies such as METI take (see Box 3). Therefore, cybersecurity cooperation goes way beyond the activities of the Ministry of Foreign Affairs (MOFA) and is reflected in the work of most agencies, METI being just one example. The international strategy is therefore translated into objectives of domestic agencies.

[45] Wilhelm M. Vosse, 'Japan's Cyber Diplomacy.'
[46] Hiroshi Yoshida (2019), 'Current Policy on Digital Economy,' METI, February 2019, http://www.cicc.or.jp/japanese/kouenkai/pdf_ppt/pastfile/h30/190221-0.pdf.
[47] METI, 'Cyber/Physical Security Framework (CPSF) Formulated,' 18 April 2019, https://www.meti.go.jp/english/press/2019/0418_001.html
[48] NIST, 'NIST Releases Version 1.1 of its Popular Cybersecurity Framework,' 16 April 2018, https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework

Box 3. METI's international partnership efforts

METI is very engaged in international cooperation on cybersecurity topics. Here are a few examples from 2018 and 2019.

METI and the US

> At *TecGlobal* in April 2018 in Washington, DC, METI shared basic ideas about the cybersecurity framework currently being studied in Japan with the Department of Homeland Security (DHS), the Department of Commerce and US private companies.

> At the Industrial Control Systems Joint Working Group in April 2018 in Albuquerque, METI introduced its cybersecurity policy to the framework National Cybersecurity and Communications Integration Center (NCCIC) under DHS in order to deepen collaboration between public and private stakeholders for the protection of critical infrastructure.

> At the 2nd Global Cyber Dialogue held by the Chamber of Commerce in October 2018 in Washington, DC, METI discussed cybersecurity policy with representatives of 37 countries.

> At CES 2019 in Las Vegas, METI introduced the cybersecurity framework and asked for public comment.

> Japan–US Joint Training for IPA's Industrial Cyber Security Center of Excellence (ICSCoE) and DHS, which conduct yearly joint training to improve capability of nearby countries to secure the global supply chain. This is a five-day event in Tokyo with participants from ASEAN countries, Australia, India, New Zealand, South Korea, and Taiwan.

> Japan and US cooperation for a free and open Indo-Pacific region, which includes joint training for industrial cybersecurity.

METI and APEC

> METI gave presentations on the cybersecurity framework at TEL 57 in June 2018 in New Guinea and an IoT workshop organised by the Computer Network Emergency Response Technical Team/Coordination Center of China (CNCERT/CC).

> METI also gave a presentation on the cybersecurity framework at APEC TEL28 in October 2018 in Taipei.

METI and ASEAN

> At the 2018 2nd ASEAN–Japan information security working group in Indonesia, METI gave a presentation about Japan's measures on supply chain security, aiming to enhance cooperation and awareness.

METI and the EU

> At the METI–EU ICT Dialogue in April 2018 in Tokyo, METI introduced the cybersecurity framework to DG Connect.

> At the 8th EU–Japan ICT strategies workshop in Vienna, 2018, METI introduced the cybersecurity framework to the Directorate-General for Communications Networks, Content and Technology (DG Connect), ETSI and Digital Europe.

METI–OECD

> OECD Committee on Digital Economy Policy (CDEP) in May 2018 in Paris,

> OECD Global Forum on Digital Security for Prosperity in November 2018 in Paris.

METI–Germany

> Securing Global Industrial Value Networks, May 2018, Berlin.

> VDE Tec Summit 2018 in Berlin.

4.3 Relations with the European Union

Historically Japan has worked closely with EU member states in the form of official cyber dialogues.[49] Recently it has engaged more directly with EU institutions. The **EU–Japan Cyber Dialogue builds a cooperative relationship to promote various efforts with shared values**. This partnership builds on a successful trade partnership that manifested in a free flow of data deal in the summer of 2018. In the first Cyber Dialogue between the EU and Japan, both agreed on a free and open cyberspace based on a multi-stakeholder model and recognised the importance of using regional fora for discussing norms of behaviour and promoting confidence building through transparency. The EU invited Japan to cooperate on building capacity in developing countries to cope with cybercrime and promote the Budapest Convention. Soon after the first dialogue, cooperation on cybercrime was operationalised via the European Cybercrime Centre (EC3), and an official mutual legal assistance (MLA) agreement has existed since 2009.

Japan and the EU also **host the Japan–EU Internet Security Forum**, which led to funding joint research projects in 2012. The Convention on Cybercrime also emerged from the Forum and was adopted by the Council of Europe. As data protection standards have been recognised by both entities, the next step could be an exchange on cybersecurity standards and regulations on cyber-incident response. In this area, thus far, the EU Agency for Cybersecurity (ENISA) and Japanese delegations have been in touch for initial exchange of ideas and perspectives[50] in international conferences.

Moreover, the **EU–Japan ICT dialogue** is an important regular contact point. The MIC and the European Commission facialite this exchange. It is used as an umbrella to cover most bilateral cooperation in the ICT sector that takes place throughout the year. Additionally, every two years, a high-level meeting has been held in Tokyo on ICT matters. The Commission maintains an ICT expert at the EU delegation in Tokyo. Participants discuss various topics, such as ICT policy, Internet governance, regulatory framework, and maintaining a safer Internet environment for children. In the 21st EU–Japan ICT Dialogue in 2015, the participants welcomed the signature of the 5G Memorandum of Understanding between the EU and Japanese industry, and discussed the signing of the EU–Japan 5G Joint Declaration.[51]

Another flagship program is the **EUNITY project**. This is a two-year project that aims to develop and encourage the dialogue between Europe and Japan on cybersecurity funded via the Horizon 2020 programme.

In December 2018 Europol signed a working agreement with the National Policy Agency of Japan.[52] Commissioner General Shunichi Kuryu said:

> This arrangement will establish a solid framework between the National Police Agency of Japan and Europol that will enable us to cooperate to combat crimes timely and effectively, in addition to the cooperation through the existing Agreement between Japan and the European Union on Mutual Legal Assistance in Criminal Matters. We especially value the opportunity of sending a liaison officer to Europol and enhancing the cooperation, as Japan will host the Games of the XXXII Olympiad and the Tokyo 2020 Paralympic Games.

In December 2018 another milestone for the security partnership between Japan and the EU was set when both entities signed a **Strategic Partnership Agreement (SPA)** that also includes cyber-diplomacy topics. 'The Council identified key areas for deeper security engagement and cooperation: maritime security; cybersecurity; counter-terrorism; hybrid threats; conflict prevention; the proliferation

[49] Wilhelm M. Vosse, 'Japan's Cyber Diplomacy.'
[50] ENISA, *ENISA Quarterly Review*, vol. 4, no. 4, October–December 2008, https://www.enisa.europa.eu/publications/eqr-archive/issues/eqr-q4-2008-vol.-4-no.-4/at_download/issue.
[51] European Commission, '21st EU-Japan ICT dialogue: strengthening cooperation,' 24 March 2015, https://ec.europa.eu/digital-single-market/en/news/21st-eu-japan-ict-dialogue-strengthening-cooperation.
[52] Europol, 'Europol Signs Working Arrangement with the National Police Agency of Japan,' press release, 3 December 2018, https://www.europol.europa.eu/newsroom/news/europol-signs-working-arrangement-national-police-agency-of-japan.

of chemical, biological, radiological, and nuclear weapons; and the development of regional cooperation.

The SPA is a framework that enables new channels to strengthen the overall security partnership, by promoting political and sectoral cooperation and joint actions in more than 40 areas of common interest. This is particularly relevant given the series of defence cooperation agreements Japan signed with EU member states in 2017. The agreement will facilitate joint EU–Japan efforts to promote shared values such as human rights and the rule of law, a rules-based international system, and peace and stability across the world.

5 Conclusion

Japan's cybersecurity policies and architecture are constantly evolving. This paper gives an overview of 2018–2019 developments in Japan's cybersecurity policy as an introduction for international stakeholders. To summarise, the Tokyo 2020 Olympic and 2021 Paralympic Games and the vision for a Society 5.0 are the main catalysts for taking rapid actions addressing cybersecurity vulnerabilities and threats in Japan, and led to the development cybersecurity strategy and regulations in 2018 and 2019.

Japan is applying similar policy instruments to those of the EU and the US to address common challenges of IoT and supply chain security, such as certifications, minimum standards, and transparency requirements, but places particular emphasis on building mutual recognition systems during the drafting phase of a framework, with the aim of preventing the spread of unique rules that distort private entities' activities.

Domestically, Japan is piloting some new approaches to address cybersecurity challenges, for example its distinct use of cybersecurity workforce training programmes and rotation of staffers among ministries, and its information security agency to tackle the workforce shortage as well as testing preventative scanning of IoT devices more broadly to achieve password security.

The Japanese government relies on Public Private Partnerships as well as cooperation with NGOs as a means to tackle some cybersecurity challenges, such as a lack of cybersecurity workforce, information sharing, and incident response.

Japan's international cybersecurity policy and engagements are shaped by domestic and foreign priorities of various ministries that address cybersecurity vulnerabilities and threats in Japan and abroad.

About the author

Julia Schuetze is a project manager for international cybersecurity policy at Stiftung Neue Verantwortung and works on cyber diplomacy of the EU with the US and Japan as part of the EU Cyber Direct project. Her research focus is on cyber operations against electoral processes, comparative cybersecurity policy and governance. As part of her role at Stiftung Neue Verantwortung she has spoken at the Congressional Cybersecurity Caucus in the US, has facilitated workshops on Germany's cybersecurity architecture with the German foreign office, and has organised a cybersecurity conference with the Bundesakademie für Sicherheitspolitik as well as several other workshops and events with US,European and Japanese cybersecurity experts in Washington, DC, Tokyo and Berlin. Her work has been published or cited in Council on Foreign Relations Net Politics Blog, Politico Europe, WirtschaftsWoche, Der Tagesspiegel, F.A.Z and the BBC. She is a Cybersecurity Policy Fellow at New America Foundation and volunteers for the OGP Civil Society Working Group in Germany..

About EU CyberDirect

The **EU Cyber Direct** project supports EU cyber diplomacy efforts and consequently contributes to the development of a secure, stable and rules-based international order in cyberspace through extensive dialogues with strategic partner countries and regional/international organisations. The **EU Cyber Direct** is funded by the European Commission under the Partnership Instrument, International Digital Cooperation project: Trust and Security in Cyberspace.

RESEARCH IN FOCUS

is a series of research papers aimed at supporting the EU's cyber-related policies by providing a timely and policy-relevant analysis.

EU CYBER DIRECT

This project is funded by the European Union.