10 May 2023

Japan's Indo-Pacific strategy in cyberspace

Piotr Malachinski

Cybersecurity is a matter of rising concern in countries all across the globe. With the number of devices connected to the internet at 14.4 billion as of 2022[1] – almost twice the world's population – the number of security threats only continues to increase. From profit-driven ransomware attacks or wipers erasing data from a network to state-sponsored cyber espionage – malicious actors, private and public alike, have long taken advantage of the expanding digitization of our social, economic, and political environments, not followed by a rise in security consciousness until relatively recently.

It is thus no surprise that questions of cybersecurity are gaining on importance on the agendas of states' ministries of foreign affairs and diplomatic offices. On the one hand, less cyber-advanced states want to catch up to their peers in terms of capacities by entering cooperation programs; on the other, the regional pioneers of cybernetics spread their influence in the region through technology sharing and ensure that their allies dispose of necessary know-how.

Among the countries in the latter category is Japan. Situated strategically in East Asia, Japan has long been a strong ally of Western states, notably the United States, vis-à-vis China and North Korea. It forms the backbone of the notion of the Indo-Pacific, Shinzo Abe being at the origin of the term first in 2007 and later promoting the 'Free and Open Indo-Pacific' concept from 2016 onwards.

The concept of the Indo-Pacific and the related strategies have since been borrowed by numerous other states, from Australia to Canada and even Europe, every country having its own definition of the region. Japan's geographical vision is especially broad, encompassing regions such as the Middle East, Eastern Africa, and even parts of Latin America.[2] Among the many objectives of Japan's Indo-Pacific strategy is promoting a rule-of-law-based geopolitical order, countering the growing influence of China, and boosting connectivity between different allied parts of the world.[3]

Of course, connectivity can also be digital, and it requires proper securitization, too. Japan does have a framework of cyber cooperation with its Indo-Pacific partners and allies, scattered throughout different theoretical frameworks and practical government initiatives. The purpose of this paper is thus to analyze to what extent Japan's Indo-Pacific strategy (even if sometimes not explicitly named so) effectively covers the cyber dimension and mitigates the threats emanating from it. The answer will be provided all along the foreign security policy implementation cycle. First, a brief analysis of threats to Japan will be studied, leading to the implementation of written strategic frameworks. Second, various diplomatic initiatives with Japan's Indo-Pacific partners will be analyzed and juxtaposed with real impact made on the ground.

---

[1] IoT Analytics. State of IoT 2022: Number of connected IoT devices growing 18% to 14.4 billion globally. May 18, 2022.
[2] Free and Open Indo-Pacific Basic Thinking Material. Foreign Policy. Ministry of Foreign Affairs of Japan, April 24, 2023.
[3] Observatory Indo Pacific. CERI, Sciences Po.

I. From threats to solutions: Theoretical framework

A prosperous island nation facing no imminent military threat since the end of Second World War, Japan is nonetheless under continuous threat of cyberattacks and data breaches. Its political proximity to the US makes it a potential target of threat actors. This and other reasons are behind the inclusion of the cyber dimension in its Free and Open Indo-Pacific strategy.

A. Japan's cyber risk analysis

Japan has one of the most forward-looking and ambitious visions of creating a highly digitized, post-information society. According to its development plan Society 5.0, "high degree of convergence between cyberspace (virtual space) and physical space (real space)" is going to help respond to many of Japan's domestic issues, such as ageing of the population, rising energy demand, distribution of wealth, or climate change.[4] This includes the application of robotics in prevention and treatment of diseases, further automated industrial production, including agriculture, and diversification of the energy basket using high-tech. Naturally, such a high level of interconnectedness between people, infrastructure, and the state requires huge amounts of data collected and analyzed with the help of artificial intelligence.

This raises obvious questions with regards to information security and personal data protection. Japan is well aware of the newest trends in cyber threats, ranging from attacks on critical infrastructure such as water management systems or nuclear power plants, or political and electoral interference.[5] It is a common target of many APTs, or Advanced Persistent Threats – groups conducting cyber-espionage for the sponsoring state, often financing their spying activities through cybercrime. Among many Japanese organizations affected in the last two decades was Japan's most important defense contractor Mitsubishi, victim of a data breach in 2011.[6] In the following year, government networks were allegedly targeted 3,000 times a day on average.[7]

North Korea is one the most notorious cyber actors Japan worries about. North Korean APTs are one of the most notorious cyber-spies and criminals in the world, typically targeting US public and private institutions, but also Japan. The infamous Lazarus Group, believed to be behind a massive ransomware worm WannaCry, has targeted Japanese operators of crypto assets as recently as in 2021.[8] And beyond the Indo-Pacific *sensu stricto*, Russia is yet another source of concern for Japan. The latter's diplomatic position vis-à-vis Russia has turned considerably more assertive since Fumio Kishida took office as Prime Minister, partly out of fear for creating a precedent for China to invade Taiwan.[9] Now since elements of hybrid warfare have been employed by the Russian state, from propaganda warfare and mass disinformation to cyberattacks, Japan has expressed its concern over the use of cyber means against the Ukrainian state, seeing it as a threat for Japan itself.[10] Shortly after sending 100

---

[4] Society 5.0. Council for Science, Technology and Innovation, Cabinet Office.
[5] Iwasawa, Akinobu. "Cyberattacks on Japan soar as hackers target vulnerabilities". Nikkei Asia, January 28, 2023.
[6] Paul Kallender & Christopher W. Hughes. "Japan's Emerging Trajectory as a 'Cyber Power': From Securitization to Militarization of Cyberspace" Journal of Strategic Studies, 2017, 40:1-2, p.121-122.
[7] Yokko, Nita. "Japan's Approach Towards International Strategy on Cyber Security Cooperation", 2013.
[8] "Japan police warn of cyberattacks by North Korea's infamous Lazarus hackers". The Japan Times, October 16, 2022.
[9] Malachinski, Piotr. "Pulaski Commentary: Japan's Policy Towards Russia After the Invasion of Ukraine". Casimir Pulaski Foundation.
[10] National Security Strategy, December 2022, p.2.

million $ worth of aid to Ukraine in March 2022, an attack on Toyota's supply chain cost the car manufacturer 375 million $ in losses, though the perpetrator is not yet confirmed.[11]

However, the biggest threat emanates from the People's Republic of China. In 2016-17, a series of espionage attacks targeted the information systems of Japan Aerospace Exploration Agency and some 200 other Japanese research institutes and companies. The JAXA attacks were officially attributed to People's Liberation Army,[12] and it would not be a singular event. China is globally known for its cyber-espionage campaigns, and Japan is aware of that. Among the gravest security challenges, it lists "*cyber activities suspected of state involvement […] presumed to be conducted by China to steal information from companies related to the military industry and possessing advanced technology*".[13] Already ten years ago, the 2013 Defense of Japan White Paper mentioned Chinese cyber capabilities as a reason for concern and pointed to an attack on Japanese private firms immediately following Japanese acquisition of contested Senkaku Islands, known in China as Diaoyu Islands.[14]

The threat of China is not considered merely in cyber operational terms, but also on a strategic, geopolitical level. In fact, parallelly to the Belt and Road Initiative and investments in connectivity infrastructure, China is implementing its global digital development program from Asia all the way to Africa and Europe. The Digital Silk Road (DSR) involves China's heavy investment in third countries' information and communications technology (ICT), in terms of physical infrastructure such as fiber optic cables, hardware, and software.[15] Such a role is seen as giving the CCP strategic advantage over Japan and its Western allies, as control over the global technology supply-chain is currently the main area of competition between the US and China.[16]

In the eyes of many Western and Japanese observers, this may allow China to include backdoors in the technology introduced to other countries, allowing them to access terabytes of data of foreign assets and states with ease. Japan already banned government purchases of Huawei and ZTE in 2018 over concerns of espionage.[17] Moreover, the export of China's Great Firewall technology of Internet surveillance and mass content control, to countries such as Russia or Uganda under the banner of "cyber-sovereignty",[18] is in direct contradiction to Japan's principle of Free and Open Indo-Pacific – in this case free and open cyberspace.

B. <u>"A free, fair and secure cyberspace". Japan's Indo-Pacific cybersecurity strategy</u>

We can thus see that the cyber dimension of Japan's security environment is far from stable, and Japan's position as a regional leader in digital affairs is being undermined. Thus,

---

[11] Jamie Tarabay et al. "Cybersecurity Nightmare in Japan Is Everyone Else's Problem Too". Bloomberg, April 18, 2023.
[12] Kashiwagi, Ryoma. "Japan aerospace cyberattacks show link to Chinese military: police". Nikkei Asia, December 29, 2021.
[13] Cybersecurity Strategy. The Government of Japan, September 28, 2021, p.9
[14] Defense of Japan, Annual White Paper 2013. Ministry of Defense, 2013.
[15] Mochinaga, Dai. "The Expansion of China's Digital Silk Road and Japan's Response". Asia Policy , January 2020, 15:1, p.42-441
[16] Mochinaga, Dai. "Policy Brief. China's Digital Silk Road and its influence in the Indo-Pacific". EUI Global Governance Programme, EU-Asia project, Issue 2022/47, September 2022.
[17] "Japan to ban Huawei, ZTE from govt contracts -Yomiuri". Reuters, December 7, 2018.
[18] Griffiths, James. "The Great Firewall of China: How to Build and Control an Alternative Version of the Internet". Zed Books, 2019

a cybersecurity plan of action, both domestic and outward-looking, is crucial, and cooperation between partner states in the field of cyber – of strategic importance.

On the domestic level, Japan has some of world's most (over)developed institutional frameworks for tackling cyber challenges. As early as in 2013, three different Ministries were tasked with tackling them: Ministry of Economy Trade and Industry, Ministry of Defense, and Ministry of Internal Affairs and Communications, joined by the National Police Agency responsible for combatting cybercrime.[19] The Personal Information Protection Commission (PIPC), created in 2016, is charged with protecting personal data of Japanese citizens and entities; and since 2015, the most important entity coordinating the efforts of different organs has been the National Center of Incident Readiness and Strategy for Cybersecurity (NISC).[20]

The year 2013 marks the release of 'j-initiative for Cybersecurity', or the International Strategy on Cybersecurity Cooperation – first such document in Japan's history. It identifies Asia Pacific as the most strategically important region for cyber policies – notably for capacity building for human resources development, or the transfer of know-how through training, sharing best practices, and cross-border collaboration. The US and Europe follow suit, and finally other regions such as Latin America or Africa. The strategy enumerates several principles and priorities for the international community, such as the need to identify evolving cyber risks and learn to tackle them collectively through a free flow of information. It stresses the need for rulemaking through technical security standards, however coming short of emphasizing a normative rule-based cyber order.[21]

More recently, the main document of reference in the field, developed and implemented by NISC, is the Cybersecurity Strategy, the most recent version released in 2021. Its primary goal is to realize "a free, fair and secure cyberspace", both in the private and public sectors, and both domestically and internationally. The strategy puts emphasis on ensuring the international "rule of law in cyberspace", including the fight against cybercrime and preventing terrorist organizations from exploiting the Internet. Japan wants to boost both its defense and deterrence capabilities and improve its non-operational measures, such as diplomatic condemnation and criminal prosecution of attackers.[22]

These and other goals would be achieved through strengthened cooperation and coordination of actions between partner states. Those "like-minded countries" include the US, Australia, India, and ASEAN – without mentioning the European Union – and cooperation with them would take different forms. First, policy coordination would take place on high-level bilateral meetings with the foreign counterparts. It would "enhance its international presence in the cyber community" through sharing of intelligence regarding vulnerabilities and threat actors, as well as lead joint exercises. These would be conducted first and foremost with the US army, notably to strengthen the defense of critical infrastructure, but Japan also considers leading some of these drills.[23]

Finally, the strategy puts much emphasis on "efforts to build the capabilities" of the cyber commands of developing countries to better respond to cyber incidents. Capacity building

[19] Yokko, Nita. "Japan's Approach Towards International Strategy on Cyber Security Cooperation", 2013.
[20] National Centre of Incident Readiness & Strategy for Cybersecurity (NISC) – Japan. Cyber Security Intelligence.
[21] Kondo, Reiko. "International Strategy on Cybersecurity Cooperation —j-initiative for Cybersecurity". Policy, New Breeze Winter 2014.
[22] Cybersecurity Strategy. The Government of Japan, September 28, 2021, p.36-37.
[23] Ibid, p.37.

would include human resources development, but also establishing technical standards and interpreting legal principles and their application in the cyber dimension.[24] Meanwhile, the second major strategic document mentioning cyber goals of Japan – the National Defense Strategy, modified in 2022 – puts further emphasis on the Japan-US partnership. It highlights the need to "ensure the Alliance's technological edge, interoperability, readiness, and persistent warfare capabilities."[25]

Although these aims constitute an effort "towards the realization of the Free and Open Indo-Pacific", these ambitions seem to eventually serve the Japanese national interests. "Today, as interdependence across borders has deepened, it is not possible for Japan to secure peace and stability only by itself."[26] Unlike in the 2013 'j-initiative', it is the nature of the cyberspace which knows no borders that seems to force Japan to take on an international role, rather than the country's own ambitions to be the global or regional leader in the field.

II. From theory to practice: Japan's cyber footprint in the Indo-Pacific

We have seen Japan has plenty of reasons for its relatively developed cyber foreign strategy. However, these documents do not have impact by themselves – they are but guidelines, or a first step for a robust and effective policy. To not be void, the strategy must be followed by both diplomatic and operational initiatives – the focus of the second part of this paper.

A. Japan's robust cyber diplomacy

One thing is certain – the cyber strategy has translated into an impressive series of diplomatic initiatives as part of the FOIP. Among them, cooperation with the US naturally remains the backbone of Japan's cyber diplomacy. Numerous initiatives can be identified. Through the US-Japan Strategic Digital Economy Partnership (JUSDEP), the two countries agreed to help develop digital economy infrastructure in developing countries.[27] US-Japan Global Digital Connectivity Partnership (GDCP) is a strengthened continuation of JUSDEP to "promote secure connectivity" on top of digital economy.[28] Among other initiatives, US-Japan Policy Cooperation Dialogue on the Internet Economy, was held for the 13th time in March this year,[29] and the 8th edition of the US-Japan Cyber Dialogue – forum for discussion of various cyber-related topics – took place on the 1st of May 2023.[30]

Another state that Japan is investing into diplomatically is India – a key Indo-Pacific partner sharing a common Chinese threat.[31] On the occasion of the 14th Japan-India Annual Summit, a joint statement was released, in which the two states, they decided to strengthen their cooperation in emerging technologies such as 5G, open radio access network, and quantum communication, after having signed memoranda of cooperation in the cyber field.[32] Japan-

[24] Ibid, p.41.
[25] National Defense Strategy. Ministry of Defense, December 16, 2022, p.20.
[26] Cybersecurity strategy…, p.40
[27] Diplomatic Bluebook 2022. Ministry of Foreign Affairs, p.104.
[28] Joint Statement on the Launch of the U.S.-Japan Global Digital Connectivity Partnership. Media note, US Department of State, June 3, 2021.
[29] Ibid.
[30] The 8th Japan-US Cyber Dialogue. Press Release. Ministry of Foreign Affairs, May 1, 2023.
[31] Masahiro, Kurita. "Japan-India Security Cooperation: Progress Without Drama". Stimson, February 15, 2023.
[32] Japan-India Summit Joint Statement. Partnership for a Peaceful, Stable and Prosperous Post-COVID World. March 19, 2022.

India Cyber Dialogue has had its fourth edition in June last year, and it added supply-chain attacks to the topics of bilateral discussion.[33] Australia, too, has had its share, albeit limited, of inter-ministerial agreements with Japan, with Australian Minister for Home Affairs Clare O'Neil saying: "*Japan and Australia are united in our vision of a prosperous and secure Indo-Pacific. […] I look forward to working together, harnessing opportunities generated by critical and emerging technologies, bilaterally and through the Quad.*" And indeed, together as Quad, the four states acted together on a few occasions, most recently to raise cybersecurity awareness to protect its communities from phishing and other cyber threats.[34]

Among Japan's bilateral initiatives with European countries, cooperation with the UK seems the most fruitful. Since 2016, yearly "2+2" meetings with British Defense and Foreign Ministers have been held,[35] parallel to Japan-UK Bilateral Consultations on Cyber Issues.[36] EU member-states, too, strengthened their diplomatic relation in cyber – for example Slovenia, Finland, and Estonia. The EU institutions, too, have engaged in specific cyber-related fields, notably internet governance and private data protection, advocating for a "multi-stakeholder approach to internet governance" within groups such as the United Nations Group of Governmental Experts (UNGGE).[37] In 2019, Partnership on Sustainable Connectivity and Quality Infrastructure between Japan and the European Union was agreed on, promoting "openness, transparency, inclusiveness" in digital connectivity globally through investment in third countries.[38]

A more multilateral initiative that Japan has been pushing for is DFFT, or Data Free Flow with Trust. This buzzword signifies a global system of rules, strengthening both information sharing across countries and personal data protection, hence the "trust".[39] Proposed by Shinzo Abe in 2019, the program was discussed within the G7, resulting in the UK G7 Roadmap for Cooperation on DFFT in 2021 and in the following year, the Germany 2022 G7 Action Plan on DFFT.[40] To manage these and other cyber diplomacy initiatives within Japan, the Digital Agency was created in 2021.

Otherwise, Japan was, alongside Australia and Singapore, the initiator of the negotiations on e-commerce within the World Trade Organization. The purpose of the ongoing negotiations is to establish "high-standard rules for governing the digital economy" and legal provisions for the protection of data privacy, similarly to the Comprehensive and Progressive Agreement for Trans-Pacific Partnership, Japan leading the negotiations following America's withdrawal from the original TPP.[41] More recently, a two-day conference, Cyber Imitative Tokyo, was launched in 2022, bringing together both the private, the public sector, and academia to discuss emerging cyber threats, hybrid warfare, and the future of cybersecurity policy.[42] Around the

[33] Forth Japan-India Cyber Dialogue. Press Releases. Ministry of Foreign Affairs, June 30, 2022.
[34] Quad Joint Statement on Cooperation to Promote Responsible Cyber Habits. The White House, February 7, 2023.
[35] Japan's Defense Capacity Building Assistance. Ministry of Foreign Affairs, February 2016.
[36] The 7th Japan-UK Bilateral Consultations on Cyber Issues. Press Releases. Ministry of Foreign Affairs, February 7, 2023.
[37] Vosse, Wilhelm."A Conceptional Broadening of the Security Order in the Indo-Pacific: The Role of EU-Japan Cooperation in ICT and Cybersecurity", Asian Affairs, 2022, 53:3, p.561-582.
[38] Ibid.
[39] Aidan Arasasingham & Matthew P. Goodman. "Operationalizing Data Free Flow with Trust (DFFT)". CSIS, April 13, 2023.
[40] Overview of DFFT. Digital Agency.
[41] Joint Initiative on E-commerce. World Trade Organization.
[42] Cyber Initiative Tokyo 2022. Global Nikkei.

issues of "cyber-sovereignty" and "web freedom", the 2023 edition of the multistakeholder platform Internet Governance Forum will take place in Kyoto.[43]

Finally, as South-East Asia is the geographical core of the FOIP, Japan has put much emphasis on developing cyber relations with ASEAN. This cooperation is exceptionally broad. During the ASEAN-Japan Cybersecurity Policy Meetings, held annually since as early as 2009, the two sides discussed "collaborative activities" in multiple cyber sectors, including building societies' healthy cyber habits, cyber exercises, and workshops, multisectoral cooperation platforms, and capacity building – the latter a strategic priority for Japan.[44] Among the many other initiatives between the two were the ASEAN-Japan Ministerial Policy Meeting on Cybersecurity Cooperation[45] and ASEAN-Japan Cybercrime Dialogues.[46]

B. Mixed impact on the ground

To say that the list of Japan's diplomatic initiatives on cyberspace is exhaustive would be an understatement. However, as often is the case with diplomacy, it is not an easy task to operationalize it, even when motivation and joint agreement is present. With multilateral agreements especially, coordination of objective implementation can be challenging. In case of Japan cyber strategy, the successfulness of strategy implementation is rather difficult to evaluate, as it varies drastically between different partner regions and specific fields of cooperation, and there is little data open to the public on its specificities.

ASEAN may well be the region where Japan has achieved the most in terms of implementing its international cyber policy. Significant steps have been taken to step up capacity building of its South-East Asian peers. ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC) was funded by Japan in 2018 to train specialized cybersecurity professionals. Surprisingly a lot of those capacity-building assistance were conducted in Vietnam – an arena of competition between Japan and China.[47] However, these investments are criticized as modest compared to the Japanese ambitions and far from achieving the desired results, partly due to the "sensitive nature of cooperation and cyber sovereignty" and the difficult-to-bridge gap in capabilities between the two parties.[48]

In the field of norm-setting and creating a "rule-based cyber order", there is even less proof of the Japanese initiatives bringing fruitful results on the ground. Despite its comprehensive strategy, Japan's approach sometimes criticized by those who think the government is focusing too much on the technical aspects without paying enough attention to international legal reforms and the implementation of rule-of-law-based norms. Moreover, an argument can be made about Japanese policy being excessively reactive and not enough proactive. [49]

---

[43] Internet Governance Forum 2023 to Take Place in Japan. Ministry of Internal Affairs and Communications, December 5, 2022.
[44] Outcomes of the 14th ASEAN-Japan Cybersecurity Policy Meeting. Ministry of Economy, Trade and Industry, October 22, 2021.
[45] Kondo, Reiko. International Strategy on Cybersecurity Cooperation —j-initiative for Cybersecurity…, p.13.
[46] Hiromu, Murakami. "A Study on Foreign Policy on Cybersecurity Issues with an Emphasis on Capacity Building". Thesis. March 2018, p.89.
[47] Tomohiko Satake & Ryo Sahashi. "The Rise of China and Japan's 'Vision' for Free and Open Indo-Pacific". Journal of Contemporary China, 2021, 30:127, p.29.
[48] Katagiri, Nori. "Shinzo Abe's Indo-Pacific Strategy: Japan's recent achievement and future direction" Asian Security, 2019, p.186.
[49] Hiromu, Murakami. A Study on Foreign Policy on Cybersecurity Issues…, p.100, 103.

Japan has also been relatively present in foreign cyber exercises. In 2021, Japan took part in the Locked Shields exercise with NATO member-states, organized by the NATO CCDCOE, as well as the US-hosted Cyber Storm exercise.[50] In 2020, it finally organized its first cyber drill of such scale, hosting South-East Asian, American, and European competitors – although arguably late for a state that calls itself the world's leader of information technology.[51]

One reason for this mixed implementation of strategic priorities may be the fragmentation of responsibilities between different governmental bodies within Japan. While the hierarchy of cyber diplomacy is clear, with the Ambassador in charge of Cyber Policy as leading most initiatives, it is less obvious whoever is responsible for its operationalization. This, combined with relatively poor information sharing – ironic considering Japan's very own DFFT initiative – makes for a system that is confusing and difficult to collaborate with for foreign partners.[52]

In implementing its cyber foreign strategy, Japan may be stumbling on the same difficulties its FOIP is – scarcity of allocated resources.[53] The Japanese budget allocations for Official Development Assistance specifically on cybersecurity projects are scarce, which stands in contrast to the robust investment plans of the Digital Silk Road.

Conclusion

"Given that the Indo-Pacific region is now home to leading IT hubs, the risk of cyber-crime, cyber-insecurity and cyber competition is high", says Daniel Fiott, former analyst of the European Union Institute for Security Studies [54] Indeed, the Indo-Pacific is home to countless cyber security threats, and as the further digitization of its societies progresses, so will the number of vulnerabilities that governments must be wary of. In this vulnerable environment, China is seen as the main winner, capitalizing on developing states in the region to ensure its own doctrine of information control is followed and its access to competitors or proxies' state secrets is secured.

Japan, one of the most cyber-conscious countries in the world, has done incredible diplomatic work, drawing on its novel cybersecurity framework to tackle this plethora of challenges. For now, however, the Indo-Pacific cyber strategy is far from being fully put into practice. The first few steps have already been taken, the partnerships have been established, and the institutional framework has been prepared – it is not unreasonable to believe soon we might see an operational breakthrough in Japan's approach in the years to come. But until that happens, certain policy changes may have to be implemented – from better resource allocation among different state agencies and projects, to the better distribution of responsibilities for foreign cooperation, if not a new, more centralized system of cyber governance.

---

[50] Ibid, p.96.
[51] Tajima, Yukio. "Japan to lead first cyber defense drill with ASEAN, US and Europe". Nikkei Asia, August 9, 2020.
[52] Hiromu, Murakami. A Study on Foreign Policy on Cybersecurity Issues…, p.104.
[53] Tomohiko Satake & Ryo Sahashi. The Rise of China…
[54] Luis Simón & Ulrich Speck. "Natural partners? Europe, Japan and security in the Indo-Pacific". Elcano Policy Paper, November 2018, p.44.

Bibliography

Academic sources

1. Hiromu, Murakami. “A Study on Foreign Policy on Cybersecurity Issues with an Emphasis on Capacity Building”. Thesis. March 2018. Available at:
2. Japan. Observatory Indo Pacific. CERI, Sciences Po. Available at: https://www.sciencespo.fr/ceri/observatory-indo-pacific/
3. Katagiri, Nori. “Shinzo Abe's Indo-Pacific Strategy: Japan's recent achievement and future direction” Asian Security, 2019.
4. Mochinaga, Dai. “The Expansion of China’s Digital Silk Road and Japan’s Response. Asia Policy”. January 2020, 15:1, p.41-60.
5. Paul Kallender & Christopher W. Hughes. “Japan’s Emerging Trajectory as a ‘Cyber Power’: From Securitization to Militarization of Cyberspace” Journal of Strategic Studies, 2017, 40:1-2, p.118-145.
6. Tomohiko Satake & Ryo Sahashi. “The Rise of China and Japan’s ‘Vision’ for Free and Open Indo-Pacific”. Journal of Contemporary China, 2021, 30:127.
7. Vosse, Wilhelm.“A Conceptional Broadening of the Security Order in the Indo-Pacific: The Role of EU-Japan Cooperation in ICT and Cybersecurity”, Asian Affairs, 2022, 53:3, p.561-582.
8. Yokko, Nita. “Japan’s Approach Towards International Strategy on Cyber Security Cooperation”, 2013 World Cyberspace Cooperation Summit IV (WCC4). Available at: https://cybersummit.info/sites/cybersummit.info/files/Japan_edited%20v2.pdf-FINAL.pdf

Government sources

1. Cybersecurity Strategy. The Government of Japan, September 28, 2021, p.9. Available at: https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021-en.pdf
2. Defense of Japan, Annual White Paper 2013. Ministry of Defense, 2013.
3. Diplomatic Bluebook 2022. Ministry of Foreign Affairs, p.104. Available at: https://www.mofa.go.jp/policy/other/bluebook/2022/pdf/pdfs/2022_all.pdf
4. Forth Japan-India Cyber Dialogue. Press Releases. Ministry of Foreign Affairs, June 30, 2022. Available at: https://www.mofa.go.jp/press/release/press1e_000303.html
5. Free and Open Indo-Pacific Basic Thinking Material. Foreign Policy. Ministry of Foreign Affairs of Japan, April 24, 2023. Available at: https://www.mofa.go.jp/files/000430632.pdf
6. Internet Governance Forum 2023 to Take Place in Japan. Ministry of Internal Affairs and Communications, December 5, 2022. Available at: https://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/pressrelease/2022/12/05_03.html
7. Japan-India Summit Joint Statement. Partnership for a Peaceful, Stable and Prosperous Post-COVID World. March 19, 2022. Available at: https://www.mofa.go.jp/mofaj/files/100319162.pdf
8. Japan’s Defense Capacity Building Assistance. Ministry of Foreign Affairs, February 2016. Available at: https://www.mofa.go.jp/files/000146830.pdf
9. Joint Initiative on E-commerce. World Trade Organization. Available at: https://www.wto.org/english/tratop_e/ecom_e/joint_statement_e.htm

10. Joint Statement on the Launch of the U.S.-Japan Global Digital Connectivity Partnership. Media note, US Department of State, June 3, 2021. Available at: https://www.state.gov/joint-statement-on-the-launch-of-the-u-s-japan-global-digital-connectivity-partnership/
11. National Defense Strategy. Ministry of Defense, December 16, 2022. Available at: https://www.mod.go.jp/j/policy/agenda/guideline/strategy/pdf/strategy_en.pdf
12. National Security Strategy, December 2022. Available at: https://www.cas.go.jp/jp/siryou/221216anzenhoshou/nss-e.pdf
13. Outcomes of the 14th ASEAN-Japan Cybersecurity Policy Meeting. Ministry of Economy, Trade and Industry, October 22, 2021. Available at: https://www.meti.go.jp/english/press/2021/1022_001.html
14. Overview of DFFT. Digital Agency. Available at: https://www.digital.go.jp/en/dfft-en/
15. Quad Joint Statement on Cooperation to Promote Responsible Cyber Habits. The White House, February 7, 2023. Available at: https://www.whitehouse.gov/briefing-room/statements-releases/2023/02/07/quad-joint-statement-on-cooperation-to-promote-responsible-cyber-habits/
16. Society 5.0. Council for Science, Technology and Innovation, Cabinet Office. Available at: https://www8.cao.go.jp/cstp/english/society5_0/index.html
17. The 7th Japan-UK Bilateral Consultations on Cyber Issues. Press Releases. Ministry of Foreign Affairs, February 7, 2023. Available at: https://www.mofa.go.jp/press/release/press3e_000542.html
18. The 8th Japan-US Cyber Dialogue. Press Release. Ministry of Foreign Affairs, May 1, 2023. Available at: https://www.mofa.go.jp/press/release/press4e_003253.html

Press articles

1. Iwasawa, Akinobu. “Cyberattacks on Japan soar as hackers target vulnerabilities”. Nikkei Asia, January 28, 2023. Available at: https://asia.nikkei.com/Spotlight/Datawatch/Cyberattacks-on-Japan-soar-as-hackers-target-vulnerabilities
2. “Japan police warn of cyberattacks by North Korea's infamous Lazarus hackers”. The Japan Times, October 16, 2022. Available at: https://www.japantimes.co.jp/news/2022/10/16/national/japan-police-warn-cyberattacks-north-koreas-infamous-lazarus-hackers/
3. Jamie Tarabay et al. “Cybersecurity Nightmare in Japan Is Everyone Else’s Problem Too”. Bloomberg, April 18, 2023. Available at: https://www.bloomberg.com/news/features/2023-04-17/rising-cyberattacks-in-japan-show-how-us-europe-are-also-vulnerable#xj4y7vzkg
4. “Japan to ban Huawei, ZTE from govt contracts -Yomiuri”. Reuters, December 7, 2018. Available at: https://www.reuters.com/article/japan-china-huawei-idUSL4N1YB6JJ
5. Kashiwagi, Ryoma. “Japan aerospace cyberattacks show link to Chinese military: police”. Nikkei Asia, December 29, 2021. Available at: https://asia.nikkei.com/Business/Technology/Japan-aerospace-cyberattacks-show-link-to-Chinese-military-police
6. Tajima, Yukio. “Japan to lead first cyber defense drill with ASEAN, US and Europe”. Nikkei Asia, August 9, 2020. Available at: https://asia.nikkei.com/Business/Technology/Japan-to-lead-first-cyber-defense-drill-with-ASEAN-US-and-Europe

Other sources

1. Aidan Arasasingham & Matthew P. Goodman. “Operationalizing Data Free Flow with Trust (DFFT)”. CSIS, April 13, 2023. Available at: https://www.csis.org/analysis/operationalizing-data-free-flow-trust-dfft
2. Céline Pajon. Japan’s Indo-Pacific Strategy: Shaping a Hybrid Regional Order. IFRI, 19 December 2019.
3. Griffiths, James. “The Great Firewall of China: How to Build and Control an Alternative Version of the Internet”. Zed Books, 2019.
4. IoT Analytics. State of IoT 2022: Number of connected IoT devices growing 18% to 14.4 billion globally. May 18, 2022. Available at: https://iot-analytics.com/number-connected-iot-devices/
5. Luis Simón & Ulrich Speck. “Natural partners? Europe, Japan and security in the Indo-Pacific”. Elcano Policy Paper, November 2018.
6. Malachinski, Piotr. “Pulaski Commentary: Japan’s Policy Towards Russia After the Invasion of Ukraine”. Casimir Pulaski Foundation. Available at: https://pulaski.pl/pulaski-commentary-japans-policy-towards-russia-after-the-invasion-of-ukraine-piotr-malachinski-2/
7. Masahiro, Kurita. “Japan-India Security Cooperation: Progress Without Drama”. Stimson, February 15, 2023. Available at: https://www.stimson.org/2023/japan-india-security-cooperation-progress-without-drama/
8. Mochinaga, Dai. “Policy Brief. China’s Digital Silk Road and its influence in the Indo-Pacific”. EUI Global Governance Programme, EU-Asia project, Issue 2022/47, September 2022. Available at: https://cadmus.eui.eu/bitstream/handle/1814/74873/QM-AX-22-047-EN-N.pdf?sequence=1&isAllowed=y
9. National Centre of Incident Readiness & Strategy for Cybersecurity (NISC) – Japan. Cyber Security Intelligence. Available at: https://www.cybersecurityintelligence.com/national-centre-of-incident-readiness-and-strategy-for-cybersecurity-nisc-japan-1972.html