Notes de l'Ifri
Asie.Visions 119

Japan's Cybersecurity Strategy

From the Olympics to the Indo-Pacific

Mihoko MATSUBARA
Dai MOCHINAGA

February 2021

ifri since 1979
Center for Asian Studies

The French Institute of International Relations (Ifri) is a research center and a forum for debate on major international political and economic issues. Headed by Thierry de Montbrial since its founding in 1979, Ifri is a non-governmental, non-profit organization.

As an independent think tank, Ifri sets its own research agenda, publishing its findings regularly for a global audience. Taking an interdisciplinary approach, Ifri brings together political and economic decision-makers, researchers and internationally renowned experts to animate its debate and research activities.

ISBN: 979-10-373-0302-8

How to cite this publication:
Mihoko Matsubara et Dai Mochinaga, "Japan's Cybersecurity Strategy: From the Olympics to the Indo-Pacific", *Asie.Visions*, No. 119, Ifri, February 2021.

Ifri

27 rue de la Procession 75740 Paris Cedex 15 – FRANCE

Tel.: +33 (0)1 40 61 60 00 – Fax: +33 (0)1 40 61 60 60

Email: accueil@ifri.org

Website: Ifri.org

Authors

Mihoko Matsubara is Chief Cybersecurity Strategist, NTT Corporation, Tokyo, being responsible for cybersecurity thought leadership. She worked at the Japanese Ministry of Defense before her MA at the Johns Hopkins School of Advanced International Studies on Fulbright. Her most recent experience includes VP and Public Sector Chief Security Officer for Asia-Pacific at Palo Alto Networks. She is Adjunct Fellow at the Pacific Forum, Honolulu, and Associate Fellow at the Henry Jackson Society, London. She published a book on cybersecurity, attackers, defenders, and cyber threat intelligence in Japanese from the Shinchosha Publishing Co., Ltd. in 2019.

Dai Mochinaga is a Senior Researcher at Keio Research Institute at SFC, Japan. As a consultant for Japanese government, he has contributed to its cyber security policy development including technology development, critical infrastructure protection, and government standards. He is a computer scientist and works on cyber security and international security research. His book: *Rulers of Cyberspace: Power across Borders* [in Japanese] describes the controlling factors of cyberspace and US-Europe-China power transition. He received a Ph.D. degree in computer science from Waseda University.

Foreword

Céline Pajon

Last September, the Ifri Center for Asian Studies held an online event on Japan's cybersecurity strategy.[1] The starting point was to look at the cybersecurity challenges posed by the organization of the Olympic Games, initially planned to be held in Tokyo in 2020. Indeed, in recent years, the use of cyber-attacks to derail the organization of mega sport events has been multiplying. Japan has therefore taken a variety of measures to reinforce cybersecurity both for government agencies and companies. Beyond these preparatory measures to reinforce Tokyo's own capabilities, the event also touched upon the various diplomatic initiatives taken by the Japanese government and industry to act as a leading nation in terms of cybersecurity and cyber governance on the international stage. Japan is indeed a proactive actor in this area, both at multilateral and bilateral levels.

Further elaborating on the discussions, the following two papers present perspectives on Japan's evolving cybersecurity strategy, at the domestic and international level.

First, **Mihoko Matsubara** presents Japan's efforts to enhance its national cybersecurity capabilities ahead of the 2020 Olympics.[2] In particular, Japan has been facing a shortage of cybersecurity professionals. In order to cope with this situation, a variety of industry and government-driven initiatives were taken to cultivate an adequate cybersecurity manpower. Secondly, the 2015 Cybersecurity Strategy stated, for the first time, the responsibility of business executives to include cybersecurity in their business strategy. As a result, business leaders are now playing a key role to improve the national level of cybersecurity and encourage others to have board-level discussions on cybersecurity. Finally, the 2019 Rugby World Cup helped Japan prepare for the Olympics by providing a dry-run opportunity to test cybersecurity readiness to host a mega sport event.

---

1. The recorded event is posted on Ifri's website: "Japan's Cyber-Security Strategy: From the Olympics to the World", September 15, 2020, available at: www.ifri.org.
2. Mihoko Matsubara also presents her perspective on Japan's cybersecurity and the COVID-19 in a short interview posted on Ifri's website: "Cybersecurity and COVID-19: Responses from Japan", September 18, 2020, available at: www.ifri.org.

In his paper, **Dai Mochinaga** presents his vision of Japan's diplomacy on cybersecurity and cyber governance.[3] More specifically, the author provides a first assessment of the dynamic between the Free and Open Indo-Pacific (FOIP) vision developed by the Japanese government since 2016 and Tokyo's approach in terms of cyber-diplomacy. The FOIP initiative has been helpful to integrate ongoing initiatives in terms of cyber-diplomacy, while pursuing Japan's national interests. Tokyo's cyber-diplomacy helps shaping collective action to influence international fora, through bilateral and multilateral discussions, particularly on the digital economy and data governance. The paper concludes on a reservation: Tokyo has still limited options to counter malicious cyber-activities. The imposition of sanctions is an option that Japan might want to consider for a better deterrence.

3. Dai Mochinaga also presents his analysis on Japan's cyber diplomacy in a short interview posted on Ifri's website: "Japan's cyber diplomacy: cooperation with the EU and challenges ahead", September 18, 2020, available at: www.ifri.org.

Table of Contents

Tokyo 2020 and Japan's ongoing cybersecurity efforts

Mihoko Matsubara

Introduction

After Tokyo was selected to host the 2020 Summer Olympic and Paralympic Games in September 2013, Japan has been accelerating its efforts to enhance its national cybersecurity capabilities. Both cyber and physical security are indispensable to ensure the success of the high-profile event, especially as the 2012 London Summer Olympic and Paralympic Games and 2014 Sochi Winter Games faced cyberattacks.[1]

Prime Minister Shinzo Abe recognizes the important role cybersecurity may play in the global event. He stated at a Cybersecurity Strategy Headquarters meeting in May 2015 that cybersecurity is the essential foundation for IT utilization, economic growth, national security and crisis management, and successful Tokyo 2020.[2]

In fact, Japan's Cybersecurity Strategy of September 2015, which is the first national strategy after Tokyo was selected to host the 2020 Games, reveals Japan's strong will to take advantage of the Tokyo 2020 momentum to improve its national cybersecurity capabilities. As growing international interest in Tokyo 2020 is expected to lead to increasing cyberattacks on Japan, the strategy lays out a few action items to achieve the set goal such as public-private cybersecurity partnerships, workforce development, and cyber exercises. It also urged business leaders to incorporate cybersecurity in their business strategy and invest pro-actively in cybersecurity for innovation and vigorous growth.[3]

---

1. G. Corera, "The 'Cyber-attack' Threat London's Olympic Ceremony," *BBC News*, July 8, 2013, available at: www.bbc.com, and *NBC News*, "Sochi Security: Warning of Cyber Attacks as Hackers Target Games," February 5, 2014, available at: www.nbcnews.com.
2. Prime Minister's Office of Japan, "Cybersecurity Strategy Headquarters," [In Japanese] May 25, 2015, available at: www.kantei.go.jp.
3. Cybersecurity Strategy Headquarters, "Cybersecurity Strategy," [In Japanese] September 4, 2015, available at: www.nisc.go.jp, pp. 11, 15 and 39.

This paper aims to analyze how Japan has been strengthening its cybersecurity capabilities ahead of and beyond 2020. First, the paper analyzes the unique aspect of Japanese cybersecurity career and talent development. A couple of examples will be provided to explain both industry and government-driven initiatives to cultivate cybersecurity professionals. The second section of the paper discusses why it is imperative to have business leaders involved in cybersecurity decision-making and how Japanese executives have been moving forward to reinforce their company's cybersecurity. Finally, it explores how the 2019 Rugby World Cup helped Japan prepare for Tokyo 2020 by providing a dry-run opportunity to test cybersecurity readiness to host a large-scale international sport event in the country.

Unique cybersecurity manpower situation in Japan

Although the shortage of cybersecurity professionals is not only an issue in Japan and although globally 3.5 million cybersecurity jobs are expected to remain unfilled by 2021,[4] Japan certainly faces a unique challenge to allocate technical professionals in general. Since Japanese end user companies outsource the majority of their IT and cybersecurity work, the size of their in-house cybersecurity team tends to be smaller than in other major countries. While 28.0 percent of IT professionals work in-house in Japan, the ratio is 65.4 percent in the United States, 61.4 percent in Germany, and 53.9 percent in the United Kingdom.[5]

Furthermore, Japan has a distinctive career development cycle, compared to other countries. In the 1950s during the period of rapid economic growth after the end of World War II, Japanese companies began offering lifetime employment and seniority-based promotion to keep loyal and long-term manpower and train employees based on the assumption that the economy would continue to grow.[6] This means that employees move from one position to another every two to three years within the same organization. This practice of job-rotation may help employees broaden their skills and become generalists on their company's business

4. S. Morgan, "Cybersecurity Talent Crunch to Create 3.5 Million Unfilled Jobs Globally By 2021," *Cybercrime Magazine*, October 24, 2019, available at: www.cybersecurityventures.com.
5. IPA, "White Paper 2017 on IT Professionals," [In Japanese] April 2g017, available at: www.ipa.go.jp, p. 13.
6. Ministry of Health, Labour and Welfare, "JFY 2013 White Paper on the Analysis of Labor Economics – How the Structural Change Has Changed the Way of Employment]," [In Japanese] August 2013, available at: www.mhlw.go.jp, p. 166.

but not necessarily useful to cultivate specialized skillsets including cybersecurity.[7]

If anyone wishes to choose a cybersecurity-focused career, he or she used to go to work for cybersecurity or IT vendors to focus on developing technical skills. Nonetheless, as companies are increasingly hit by cyberattacks, Japanese end user companies nowadays need to have larger in-house cybersecurity resources to protect themselves. Also, as the number of cyberattacks on Japanese industry were expected to rise further during Tokyo 2020, some companies started to realize that it is a collective responsibility for Japanese companies to work together to cultivate cybersecurity talents. Academia-government-industry collaboration is indispensable, because industry has the largest pool of cybersecurity professionals, academia builds next-generation talent pipelines, and government makes legislation and policy on cybersecurity.[8]

Cross-Sector Forum to cultivate cybersecurity talents

In June 2015, Hitachi, NEC Corporation, and Nippon Telegraph and Telephone Corporation (NTT) founded the Cross-Sector Forum to build an ecosystem to educate, recruit, retain, and train cybersecurity talent in collaboration with academia and government.[9] The original 30 member companies are from multiple critical infrastructure sectors including chemical, financial, manufacturing, media, and transportation. The Forum has 43 members as of January 2021.[10]

Their first task was to define cybersecurity professionals. The members used the National Institute of Standards and Technology (NIST) Cybersecurity Framework and National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework as global common languages. Because all of them have global business presence and one-fourth of them are Tokyo 2020 partners, they chose the NIST Frameworks to protect critical infrastructure, communicate between different industry

7. Cross-Sector Forum, "Interim report Version 1.0's Appendix 1 – Why Japanese Companies Suffer from Cybersecurity Manpower Shortage and Academic-government-industry Collaboration Is Needed," [In Japanese] January 2016, available at: www.cyber-risk.or.jp, p. 3.
8. *Ibid.*, pp. 4-5.
9. "Nippon" means Japan in Japanese.
10. Cyber Risk Intelligence Center – Cross Sectors Forum, [In Japanese], available at: www.cyber-risk.or.jp.

sectors in Japan and overseas, and map skills needed to fulfill each type of cybersecurity missions from C-suite executives to hands-on engineers.[11]

The Cross-Sector Forum has been sharing its findings with academia, government, and industry. They have published multiple documents regarding the definition of information and operational technology cybersecurity talents and skills, a calendar to execute cybersecurity missions by different types of cybersecurity talents, and guidelines to compare talents to insource or outsource. Some of the member companies started to donate funding to universities in Japan to launch a cybersecurity course and send their cybersecurity professionals as instructors to teach practical skills to tackle with cyberattacks.[12]

The Forum has presented its insights not only to the Japanese government but also to others including the US government. The National Center of Incident Readiness and Strategy for Cybersecurity (NISC) and Ministry of Economy, Trade and Industry (METI) have been inviting the Forum to their cybersecurity committee meetings to ask for their input in policy-making. For example, the Cybersecurity Talent Development Strategy in 2017 refers to the Cross-Sector Forum's definition of cybersecurity talents, which reflects how much weight the Forum's voice carries in policy-making.[13] Also, Forum members have given a talk at the NIST Cybersecurity Risk Management Conference in Baltimore, Maryland, in November 2018 to discuss their own way to use the NIST Frameworks to develop talents to deal with cyber risks.[14]

Government-driven initiatives for manpower development

There have been multiple government-driven initiatives to develop cybersecurity human resources. The project aimed at training Tokyo 2020

11. NIST, "Success Story: Japanese Cross-Sector Forum," October 15, 2018, available at: www.nist.gov, and M. Matsubara, "Japanese Cross-Sector Industry Forum is Shaping Cybersecurity Talent Development Strategy," *New America*, June 27, 2019, available at: www.newamerica.org.
12. Cross-Sector Forum, "Updates on Cross-Sector Forum activities," [In Japanese] February 7, 2017, available at: www.nisc.go.jp, p. 8.
13. METI, "The third meeting of the Working Group 2 on Business, International, and Talent Issues under the Business Cybersecurity Committee," [In Japanese] November 9, 2018, available at: www.meti.go.jp; NISC, "The Third Meeting of the Working Group to Harmonize Cybersecurity Talent Development Policies under the Committee on Cybersecurity Awareness Raising and Talent Development of the Cybersecurity Strategy Headquarters," [In Japanese] December 27, 2017, available at: www.nisc.go.jp; and Cybersecurity Strategy Headquarters, "Cybersecurity Talent Development Strategy," [In Japanese] April 18, 2017, available at: www.nisc.go.jp, p. 13.
14. NIST, "NIST Cybersecurity Risk Management Conference 2019," November 7, 2018, available at: www.nist.gov, p. 21; C. Brumfield, "Why NIST Is So Popular in Japan," *CyberScoop*, November 8, 2018, available at: www.cyberscoop.com.

cybersecurity staff is called the Cyber Colosseo. The National Institute of Information and Communications Technology (NICT) under the Ministry of Internal Affairs and Communications started this program in February 2018, aiming to train some 520 CSIRT assistants and operators, and high-level cybersecurity analysts in total. Each cyber exercise session accommodates around 30 students to master forensics and incident response skills with virtual Tokyo 2020 IT infrastructure created by the NICT. The Cyber Colosseo also provides 20 courses such as penetration test, and log, malware, and traffic analysis. The coronavirus pandemic and postponement of the Summer Olympic and Paralympic Games to 2021, however, led the Japanese government to offer nine of the courses online in July 2020.[15]

Another government-led initiative is CYber Defense Exercise with Recurrence (CYDER). The Ministry of Internal Affairs and Communications originally launched it in 2013 to train incident response capabilities for central government officials and critical infrastructure companies.[16] Based on the 2015 Cybersecurity Strategy after the Japan Pension Service breach which affected 1.25 million Japanese citizens in June 2015, the government expanded the scope of trainees to include municipal government and government-affiliated agency officials from all over Japan.[17]

Since the NICT owns high-performance servers and analyzes cyberattacks on Japan, the institute uses those resources to host CYDER sessions and to create cyber exercise scenarios. While Course A targets cybersecurity beginners, Course B targets more experienced cybersecurity professionals – Course B-1 for municipal government officials, Course B-2 for central government officials, and Course B-3 for critical infrastructure companies. Both courses offer one-hour long e-learning sessions about the latest cyber threat landscape and cybersecurity technologies and the CYDER rules, as well as one-day in-person cyber exercise to learn what to do after an incident is detected.[18]

15. NICT, "Cyber Colosseo' Exercise to Prepare for the 2020 Tokyo Olympic and Paralympic Games]," [In Japanese] December 7, 2017, available at: www.nict.go.jp; Y. Nonoshita, "'Cyber Colosseo' Exercise Is Offered to Train Tokyo 2020 People," [In Japanese] CNET, December 28, 2017, available at: www.japan.cnet.com; National Cyber Training Center, "The Cyber Colosseo Program to Prepare for the Tokyo 2020 Olympic and Paralympic Games," [In Japanese] July 20, 2020, available at: www.colosseo.nict.go.jp, pp. 3-4, pp. 8-9.
16. NICT, "History of CYDER," [In Japanese], available at: www.cyder.nict.go.jp.
17. Cybersecurity Strategy Headquarters, "Cybersecurity Strategy," p. 17.
18. NICT, "CYDER," available at: www.cyder.nict.go.jp; "JFY 2018 CYDER," [In Japanese] available at: www.cyder.nict.go.jp.

The coronavirus pandemic has also had CYDER change the way it operates. The NICT began choosing larger venues for in-person sessions to keep social distancing, and all the trainees and trainers are required to wear a mask. Furthermore, the institute made CYDER materials downloadable for the public between May and June 2020 for the first time, because growing cyber threats take advantage of the pandemic and better cybersecurity has become more important than ever. As more organizations rely on remote work and information technology such as web conferencing tools, cyber attackers now target vulnerable remote workers and cloud service accounts to use their credential information for further attacks. The NICT hopes CYDER materials would be beneficial for cybersecurity practitioners to continue to learn about cybersecurity and improve their expertise.[19]

Leadership by business leaders and the NIST Cybersecurity Framework

Another focus of the 2015 Cybersecurity Strategy is the leadership to be taken by business executives to improve the national level of cybersecurity. In fact, it was the first time for the national strategy to refer to the inclusion of cybersecurity into business management strategy as a responsibility of business executives.[20] As IT plays an integral part of business operations, cybersecurity is essential to ensure business continuity and innovation. C-suites are ultimately responsible to incorporate cybersecurity into their business strategy.

Following the 2015 Cybersecurity Strategy, the METI and the Information-Technology Promotion Agency (IPA) published the Cybersecurity Guidelines for Business Leadership Version 1.0 in December 2015. It expressed a sense of urgency to raise business leaders' cybersecurity awareness, citing KPMG's findings that only 13 percent of Japanese board members strongly believe cybersecurity should be discussed at the board level. This low number stood in sharp contrast to 56 percent outside Japan.[21]

19. NICT, "NICT Started to Accept Request to Participate in JFY2020 CYDER," [In Japanese] July 1, 2020, available at: www.nict.go.jp, " CYDER Materials Will Be Available for the Public for a Limited Time Only," [In Japanese] May 12, 2020, available at: www.nict.go.jp; "CYDER," *op. it.*; D. Palmer, "Coronavirus and Home Working: Cyber Criminals Shift Focus to Target Remote Workers," *ZDNet*, March 27, 2020, available at: www.zdnet.com; McAfee, "McAfee Labs COVID-19 Threat Report," July 2020, available at: www.mcafee.com, p. 14.

20. Cybersecurity Strategy Headquarters, "Cybersecurity Strategy 2015", p. 11.

21 . KPMG, "Cybersecurity Survey 2013," [In Japanese] February 3, 2014, available at: www.assets.kpmg.com, p. 39; and METI, "Cybersecurity Guidelines for Business Leadership]," [In Japanese] December 28, 2015, available at: www.meti.go.jp, p. 2.

The METI and IPA emphasized the fact that cyberattacks are nowadays inevitable business risks, whose consequences include the leakage of personal information and national security-related intelligence and the suspension of critical infrastructure operations. The guidelines encouraged business executives not only to change their mindset to look at cybersecurity as an investment opportunity for innovation and business growth rather than as a cost center, but also to lead efforts to develop cybersecurity talents. It also presents ten action items that Chief Information Security Officers (CISOs) should pursue, such as identifying IT assets to protect and cybersecurity risks to address and participating in organizations to share cyber threat intelligence.[22]

Two years later, the METI and IPA released an updated version, Version 2.0, after they renewed their sense of concern. They found out that only 18.6 percent of Japanese companies believe cybersecurity is something worth investing in and 63.9% still think cybersecurity is merely a cost center. While 75.3 percent of companies which considerg cybersecurity as an investing opportunity have a sufficient cybersecurity budget, only 45.0 percent of companies which think cybersecurity is a cost center have a sufficient such budget.[23]

Thus, the Version 2.0 stressed the need to change the mindset of business executives and invest in cybersecurity, as IT is an indispensable tool to increase profitability and seek innovation in the competitive global market. The guidelines referred to the NIST Cybersecurity Framework for the first time in the check sheet of the ten action items, allowing Japanese companies to see how much cybersecurity measures they are able to take based on the global framework.[24]

Japanese Industry's initiative to move forward board level discussions

Yet, the Japanese industry has begun to take more cybersecurity actions over the last few years. In fact, the industry declared cybersecurity is a business management issue and needs C-suites' attention earlier than the Japanese government. In February 2015, the Japan Business Federation or Keidanren issued a "Proposal for Reinforcing Cybersecurity Measures," recognizing cyberattacks on critical infrastructure operations can lead to serious damages to people's daily lives and Japan's industrial

22. METI, "Cybersecurity Guidelines for Business Leadership Version 1.0," pp. I-II, pp. 5-6.
23. METI, "Cybersecurity Guidelines for Business Leadership Version 2.0," [In Japanese] November 16, 2017, available at: www.meti.go.jp, pp. 1-2; KPMG, "Cybersecurity Survey 2017," [In Japanese] June 28, 2017, available at: www.assets.kpmg.com, pp. 14-15.
24. METI, "Cybersecurity Guidelines for Business Leadership Version 2.0," pp. I, 3, pp. 17-20.

competitiveness. Keidanren emphasized the importance in positioning cybersecurity as an important managerial task and raise business executives' awareness, because IT and cybersecurity are an integral part of business continuity and trust.[25]

Three years later, Keidanren published a statement, "Declaration of Cyber Security Management," in March 2018. As Japan is pushing the concept of Society 5.0, cybersecurity plays a larger role to ensure its success, because cyberspace and physical space merge to take advantage of emerging technologies such as artificial intelligence and the internet of things to solve socioeconomic challenges including the aging society and manpower shortage. The declaration took a few steps further, compared to the 2015 statement: Keidanren urged Japanese business leaders not only to take the leadership to invest in cybersecurity and incorporate cybersecurity in their business strategy but also to establish a cybersecurity posture for internal defense, training, and supply chain risk management, and contribute to making an ecosystem of security and safety.[26]

This epoch-making statement has induced multiple companies to endorse the declaration and release their own document. Keidanren incentivized its member companies to do so by offering them to showcase their efforts on the Keidanren website and allowing them to use a special logo on their business cards and website so that those companies can show their strong commitment to cybersecurity. For example, Keidanren's website carries the link to such declarations made by ENEOS Holdings, Fujitsu, NEC, and Sumitomo Mitsui Financial Group.[27] In fact, all of the three Major Japanese banks including Mizuho Bank and MUFG Bank published a similar document between March and June 2018.[28]

Global trade associations' collaboration for more board level discussions

Furthermore, Keidanren worked with the Internet Security Alliance (ISA), a global multi-sector trade association based in the United States, and co-published a 43-page document, "Cyber Risk Handbook for Board of Directors," in Japanese to clarify the responsibility to be taken by the board

25. Keidanren, "Proposal for Reinforcing Cybersecurity Measures," February 17, 2015, available at: www.keidanren.or.jp.

26 . Keidanren, "Declaration of Cyber Security Management," March 2018, available at:www.keidanren.or.jp, and Cabinet Office, "Society 5.0," available at: www8.cao.go.jp.

27. Keidanren, "Examples of Cybersecurity Efforts by Member Companies," [In Japanese] available at: www.keidanren.or.jp; Y. Ishii, "Keidanren's Declaration of Cyber Security Management," [In Japanese] November 9, 2018, available at: www.newton-consulting.co.jp.

28. ZDNet Japan, "The Three Largest Japanese Financial Groups Issued a Declaration of Cybersecurity Management," [In Japanese] June 27, 2018, available at: www.japan.zdnet.com.

of directors and how to identify and manage risks and drive cybersecurity conversations and initiatives. The handbook in Japanese avoids using technical terminologies and offers five principles and ten check lists to facilitate cybersecurity discussions at the board level.[29]

The ISA has been working with various international partners to localize the US handbook in Germany, Latin America, and the United Kingdom. Even though each country or region has a different corporate governance model, board of directors are universally expected to play a leadership role to shape cybersecurity culture and strategy in order to tackle cyber threats as a business risk. The Japanese version is based on "the National Association of Corporate Directors Cyber Risk Oversight Director's Handbook" and "Managing Cyber Risk: A Handbook for UK Board of Directors."[30] In their interview by the *Sankei Shimbun* newspaper in December 2019, the Keidanren Cybersecurity Committee Chairpersons urged Japanese business leaders to take a look at this handy document and use it to strengthen their company's cybersecurity before Tokyo 2020.[31]

The role of the 2019 Rugby World Cup in Japan

Since Japan hosted the Rugby World Cup, another huge international sports event, between September and November 2019, it worked as a dry run for Tokyo 2020. This was a golden opportunity for the country to set a milestone before Tokyo 2020 to test its readiness and incident response capabilities in advance. The 2015 Cybersecurity Strategy expresses Japan's interests in taking advantage of cybersecurity lessons to learn from the 2019 Rugby World Cup for Tokyo 2020.[32]

Based on the strategy, the Japanese government decided to launch the Tokyo 2020 Computer Security Incident Response Team (CSIRT) to prevent damages caused by cyberattacks, detect cyberattacks at an early stage, and share cyber threat intelligence between concerned parties such as the Tokyo 2020 Organizing Committee, municipal governments which have Tokyo 2020-related venues, sports organizations, venue owners, and critical infrastructure companies. The CSIRT, now called the Cybersecurity Incident Response and Coordination Center, gained its initial operational capabilities in April 2019, and provided support for the 2019 Rugby World

29. Keidanren and Internet Security Alliance, "Cyber Risk Handbook for Board of Directors," [In Japanese] October 2019, available at: www.cdn2.hubspot.net.
30. *Ibid*.
31. N. Endo and S. Kaneko, "Please Read the Handbook: Business Executives Must Be Involved in Cybersecurity Initiatives," [In Japanese] *SankeiBiz*, December 25, 2019, available at: www.sankeibiz.jp.
32. Cybersecurity Strategy Headquarters, "Cybersecurity Strategy 2015," p. 39.

Cup and the 2019 G20 Osaka Summit. The center also hosts cyber exercises to improve cybersecurity procedures and capabilities.[33]

After the 2019 Rugby World Cup, the IT Director of its Organizing Committee emphasized the importance of cybersecurity resilience, preparation, and training in his interview with Nippon Hoso Kyokai (NHK), Japan's national broadcaster. A nightmare scenario is a cyberattack disrupting the operations of the event. Because the Committee had expected this type of cyberattacks such as distributed denial-of-service (DDoS) attacks and phishing emails to steal credential information, they had hardened their IT infrastructure and conducted cybersecurity training for Committee members to spot malicious emails. The Japanese government held a meeting in November 2019 to discuss cybersecurity lessons learned from the Rugby World Cup and use them for Tokyo 2020.[34]

Yet, the coronavirus pandemic has certainly complicated how to prepare for Tokyo 2020. The global travel restrictions and vaccine availability pose unprecedented challenges to the host country to hold the event in a safe and secure manner.[35] Over 90 percent of Tokyo 2020 Organizing Committee members had to work from home to prevent coronavirus infection during the first state of emergency between April and May 2020. If the event is held in 2021 and the pandemic still requires most of operators to work remotely, it would be important to secure not only Tokyo 2020-related infrastructure such as electricity, transportation, and venues, but also their remote work IT environment.

Conclusion

Both the Japanese government and industry have been accelerating their efforts to strengthen national cybersecurity capabilities over the last several years toward Tokyo 2020 and beyond. The designation of the 2020 Summer Olympic and Paralympic Games in 2013 has set a clear deadline to enhance cybersecurity resilience. It also incentivized the government and industry to work together to develop cybersecurity talents via the Cross-

33. NISC, "Cybersecurity Measures to Take to Prepare for the 2020 Tokyo Olympic and Paralympic Games," [In Japanese] June 13, 2016, available at: www.nisc.go.jp, p. 3, "Cybersecurity Incident Response and Coordination Center," [In Japanese] April 18, 2019, available at: www.nisc.go.jp, pp. 1-3, "Cybersecurity Measures to Take to Prepare for Tokyo 2020]," [In Japanese] May 23, 2019, available at: www.nisc.go.jp, p. 1.

34. *NHK*, "Cyberattacks on the Rugby World Cup Organizing Committee," [In Japanese] November 23, 2019, available at: www.nhk.or.jp; "Unveiled Cybersecurity Battles During the Rugby World Cup," [In Japanese] January 6, 2020, available at: www.nhk.or.jp.

35. R. Takahashi, "Doubt and Uncertainty Remain One Year Before Postponed Tokyo Olympic Games," *The Japan Times*, July 22, 2020, available at: www.japantimes.co.jp.

Sector Forum and cyber exercises and bring business leaders into cybersecurity discussions.

The 2019 Rugby World Cup served as a dry run to test the readiness of Japan to host a large-scale international sport event and run a CSIRT for Tokyo 2020. The public-private partnership during the World Cup avoided any serious impact by cyberattacks on the operations of the event. This experience would help the country further prepare for Tokyo 2020.

Needless to say, the coronavirus pandemic casts a long shadow over the outlook of Tokyo 2020 and has certainly complicated the way to secure the event in both the cyber and physical domains. Cybersecurity and resilience would become indispensable for the success of the event.

Fortunately, Japan has a momentum to expand frank and open discussions on cybersecurity between the public and private sectors and at the board level. Both government and industry leaders are committing to improve their cybersecurity posture and incorporate cybersecurity in their business strategy. Although the challenges lying ahead are undeniably excruciating, they themselves will provide valuable insights to remain cybersecurity resilient in difficult times at many levels.

Japan's Free and Open Indo-Pacific and Challenges in Cyber-space

Dai Mochinaga

In August 2016, the Abe administration unveiled Japan's new Free and Open Indo-Pacific vision (FOIP). This initiative aims to better integrate the area spanning the Pacific and the Indian oceans, based on three pillars: the promotion and enforcement of fundamental values (the rule of law, freedom of navigation), the pursuit of economic prosperity through improving connectivity, and the commitment to peace and stability, through capacity-building.

This broad vision offers regional partners options regarding infrastructure development and connectivity, including alternatives to the Chinese Belt and Road Initiative (BRI).[39] Digital connectivity and cyber-security cooperation have therefore been integrated into FOIP. While Japan has been playing a strong role in building up the capacity of Asian countries in the IT sector since the early 2000s, the implementation of FOIP has been influencing Japan's cyber-diplomacy. This paper aims at providing a first assessment of the dynamic between the FOIP vision and Japan's approach in terms of cyber-diplomacy.

FOIP strategically integrates ongoing initiatives being implemented by government agencies. The Japanese Ministry of Foreign Affairs (MOFA) is one of the leading players in the country's diplomacy on cyber-security. It has contributed to cyber-norm discussions at the multilateral level and capacity-building, along with FOIP. Other agencies such as the Cabinet Secretariat, the Ministry of Internal Affairs and Communications (MIC), and the Ministry of Economy, Trade and Industry (METI) have cooperated in FOIP's practical operation for cyber-security and infrastructure development. MOFA played a key role in coordinating the different agencies and initiatives, implemented under the schemes of the

39. Ministry of Foreign Affairs, "Free and Open Indo-Pacific", available at: www.mofa.go.jp.

International Strategy on Cyber-security and the Partnership for Quality Infrastructure (PQI).[40]

The FOIP security pillar promotes cyber-security capacity-building in order to bolster defense against cyber-threats. It aims not only at helping partners to enhance their own defense against cyber-attacks, but also to build up a safer cyber-environment for Japan and ultimately strengthen its own security. However, this effort may not be sufficient to change the calculus of malicious actors in cyber-space. The Japanese government has rarely taken decisive diplomatic action against cyber-attacks that were possibly state-sponsored. The imposition of sanctions is a possible option to change the calculus of actors regarding the risk of reprisal, and to eventually deter attacks.

Japan's cyber policy and diplomacy

Tokyo started its cyber-policy efforts by setting up the IT Strategic Headquarters (ITSH) within the Prime Minister's Cabinet Office in 2001. The headquarters established the e-Japan strategy that aims to leverage the IT revolution and transform the country into a "knowledge-emergent society". The ITSH has also promoted international cooperation by establishing its international policy, the "Basic Concept on IT International Policy Centered on Asia".[41] The policy focuses on capacity-building, bilateral and multilateral cooperation, and Official Development Assistance (ODA) for building the social application of IT and global technology standards in Asia. The concept was implemented through initiatives carried out by government agencies responsible for international cooperation and IT policies. For example, the Japan International Cooperation Agency (JICA), an affiliate of MOFA coordinating ODA, carried out ICT education projects, and MIC promoted the Asia Broadband Program aimed at constructing intra-regional broadband networks across Asia and establishing a global information hub.[42] The ITSH has regularly revised its Basic IT Strategies and continued to focus on international engagement. The latest strategy, published in July 2020, focuses on promoting dialogue on the digital economy, advancing the APEC Cross-

40. Ministry of Foreign Affairs, "Announcement of "Partnership for Quality Infrastructure: Investment for Asia's Future," May 21, 2015, available at: www.mofa.go.jp.
41. IT Strategic Headquarters, "Basic Concept on IT International Policy Centered on Asia," September 10, 2004, available at: www.japan.kantei.go.jp.
42. Ministry of Internal Affairs and Communications, "Asia Broadband Program," March 28, 2003, available at: www.soumu.go.jp.

Border Privacy Rules (CBPR) System, and developing international cooperation on infrastructure building.[43]

Meanwhile, after the Japanese government was the target of cyber-attacks that defaced its websites in 2000, policymakers started to discuss ways of better protecting government agencies and critical infrastructure. In 2004, the Information Security Policy Council (ISPC) was established (it later became the Cyber-security Strategic Headquarters), and the National Information Security Centre (NISC, currently the National Center of Incident Readiness and Strategy for Cyber-security) formulated the first basic cyber-security strategy.[44] In 2013, the government established the government-wide strategy for cyber-security,[45] defining the basic principles of Japan's cyber-security policy: ensuring the free flow of information, responding to increasingly serious risks, enhancing the risk-based approach, and acting in public-private sectors. The international strategy is structured along defined priority areas of collaboration such as incident response, information-sharing, cyber-crime, and international security.[46]

Concerning developing countries, it consists of bilateral capacity-building for incident response, multilateral support against cyber-crime, and development of common understanding on rule-making and confidence-building measures. These various measures in the cyber-domain were put in place to contribute to lowering the global cyber-risk, secure Japanese nationals' and companies' operations in recipient countries, demonstrate Japan's position on cyber-space, and expand Japan's communication infrastructure development business.

The 2013 strategy also touched on diplomacy in international rule-making toward constructing "world-leading" cyber-space. The focus was put on promoting cooperation within multilateral frameworks such as the OECD and the G8 summit, contributing to sharing best practices, and developing international standards. For example, METI has worked on multilateral dialogues within the OECD and on standardizing cyber-security at ISO/IEC.[47] METI has also promoted international collaboration in incident response through JPCERT/CC (Japan Computer Emergency Response Team Coordination Center), Japan's point of contact for incident

43. IT Strategic Headquarters, "Declaration to Be the World's Most Advanced IT Nation: Basic Plan for the Advancement of Public and Private Sector Data Utilization," July 17, 2020, available at: www.kantei.go.jp.
44. IT strategic headquarters, "Review of the Role and Functions of the Government in terms of Measures to Address Information Security Issues," December 7, 2004, available at: www.kantei.go.jp.
45. Information Policy Council, "Cybersecurity Strategy," June 10, 2013, available at: www.nisc.go.jp.
46. Information Security Policy Council, "International Strategy on Cybersecurity Cooperation – J-Initiative for Cybersecurity –," October 2, 2013, available at: www.nisc.go.jp.
47. OECD, "Roles and Responsibilities of Actors of Digital Security," July, 2019, available at: www.oecd-ilibrary.org.

coordination. JPCERT/CC has provided training to computer emergency response teams (CERTs) in the Asia-Pacific region, and led the Asia-Pacific CERT (APCERT) as a steering committee member.

The cyber-security strategies of 2015 and 2018 continued to focus on the role of diplomacy for cyber-security and its close relation with Japan's national security.[48] However, these strategies were called 'stapled' strategies as they consisted of juxtaposed agencies' policies.[49] Therefore, it was difficult to realize cross-agency initiatives or integrate these policies within a more comprehensive approach.

FOIP's implementation in the cyber-domain

The Free and Open Indo-Pacific vision (FOIP), introduced by Prime Minister Shinzo Abe in 2016, has shaped Japan's international strategy, including its cyber-diplomacy.[50] There are three keywords in FOIP representing its fundamental values and geographical scope. "Free" refers to independence as well as liberal values in the economic and political domains. "Open" represents the openness of international public goods, including cyber-space. "Indo-Pacific" defines the broad geographical scope where the connectivity effort should be made.[51]

Japan's diplomacy on cyber-security, which includes promoting the rule of law in cyber-space, developing confidence-building measures, and cooperation in capacity-building, follows the FOIP pillars. Japan has thus reaffirmed the commitment to an open, free, fair and secure cyber-space in bilateral dialogues with 14 countries and regions, including France, the United States, the United Kingdom, and the European Union. It has contributed to the cyber-norms discussion in the United Nations Group of Governmental Experts (GGE) and Open-Ended Working Group (OEWG). Japan also proposed in 2017, along with Malaysia and Singapore, the establishment of the ASEAN Regional Forum (ARF) Inter-Sessional Meeting on Security and the Use of Information and Communication Technologies.[52] This platform discusses confidence-building measures and implements the ARF work plan on ICT security. At its fifth open-ended study group on confidence-building measures, the participants affirmed

48 . The Government of Japan, "Cybersecurity Strategy," September 4, 2015, available at: www.nisc.go.jp; The Government of Japan, "Cybersecurity Strategy," July 27, 2018, available at: www.nisc.go.jp.

49. Taira Masaaki's Log, April 16, 2018, available at: www.taira-m.jp.

50. Ministry of Foreign Affairs, Foreign Policy – Free Open Indo-Pacific, available at: www.mofa.go.jp.

51. Ministry of Foreign Affairs, Diplomatic Bluebook 2018, chap. 1, available at: www.mofa.go.jp.

52. Ministry of Foreign Affairs, "The 24th ASEAN Regional Forum (ARF) Ministerial Meeting", August 7, 2017, available at: www.mofa.go.jp.

that ARF members must actively contribute to the international discussion on cyber-security, including the UN GGE and the OEWG.[53]

Building up the Indo-Pacific digital infrastructure

In the cyber-domain, FOIP initiatives related to the digital economy, infrastructure development and capacity-building steadily have expanded in the region. The Japanese government has released the factsheet listing its FOIP initiatives in digital infrastructure development.[54] Their financing schemes involve not only the ODA but also private-sector investment and public-private investment. For example, the Fund Corporation for the Overseas Development of Japan's ICT and Postal Services Inc. (JICT), the specialized public-private fund for ICT development, has supported funding for infrastructure development. JICT has invested in infrastructure development projects such as the Myanmar/Malaysia India Singapore Transit (MIST) cable system through a public-private partnership financing scheme with Japanese financial institutions.[55] JICCT also funded the Japan-Guam-Australia (JGA) fiber-optic submarine cable system project, connecting institutions in key countries throughout the region and promoting their collaboration.[56] Its engagement will expand to the Eastern Pacific and South America as Chile's government chose a submarine telecommunication cable route proposed by NEC. [57] The Japanese government has promoted these submarine cable systems that connect countries across the Indo-Pacific region by exporting telecommunication infrastructure with the support of JICT.

Japan has also been active in Southeast Asia, which is a core focus of FOIP, to provide alternatives to BRI, including in the ICT sector. For example, the Japanese government has focused on Vietnam, which decided to build its 5G network without using Huawei equipment. The Vietnamese carriers selected Ericsson, Nokia and Samsung to build the country's 5G infrastructure. Following the announcement, Japan strengthened its ties

53. Ministry of Foreign Affairs, ARF-ISM on ICTs Security 5th SG, January 16, 2020, available at: www.mofa.go.jp.
54. Ministry of Foreign Affairs, "Japan's Efforts for a Free and Open Indo-Pacific," May 2020, available at: www.mofa.go.jp.
55. Fund Corporation for the Overseas Development of Japan's ICT and Postal Services, "Start of Construction of Singapore-Myanmar-India Submarine Cable," December 13, 2019, available at: www.jictfund.co.jp.
56. "Japan-Guam-Australia North Cable System Begins Installation," Submarine Telecoms Forum, Press Release, September 12, 2019, available at: www.subtelforum.com.
57. Y. Hirose and N. Toyama, "Chile Picks Japan's Trans-Pacific Cable Route in Snub to China," *Nikkei Asian Review*, July 29, 2020, available at: www.asia.nikkei.com.

with Vietnam and held a bilateral policy dialogue focusing on cyber-security and 5G in December 2019.[58]

Japan not only acts on its own; it also promotes cooperation with like-minded partners in the Indo-Pacific area. Cooperation with the US is already under way regarding support for cyber-security and infrastructure in third countries. In the Japan-US 2019 Digital Economy Partnership (JUSDEP), the United States and Japan agreed to cooperate in developing smart cities, network infrastructure, and cyber-security in line with FOIP.[59] Their collaboration in the development of smart cities started as the Smart Sisters Program, which creates partnerships between Indo-Pacific cities.[60]

Digital capacity-building initiatives

Capacity-building is another tool of diplomacy on cyber-security. Japan has contributed to regional capacity development for over 20 years. Its engagement in capacity-building stems from one of the FOIP's pillars of pursuing economic prosperity and securing peace and stability. It has shared best practices and threat information within national CERT communities such as Meridian and FIRST. Its community-based approach led to collective power through sharing threat information and best practices. Japan has conducted cyber-security capacity-building by deepening understanding and training. For instance, Japan and ASEAN have held director-general and director-level meetings on cyber-security since 2009. The Cabinet secretariat, METI, and MIC joined meetings and agreed to the practical and operational-level collaboration. JICA has carried out projects for human resource development in cyber-security,[61] and it also supported the establishment of the ASEAN-Japan Cyber-security Capacity Building Centre in Bangkok in 2019, providing training in malware analysis and forensics with the support of Japanese companies such as NEC and LAC. Moreover, JICA conducted a technical cooperation

58. Ministry of Internal Affairs and Communications (Japan), "Results of the Third Meeting of the Japan-Vietnam Joint Working Group" [In Japanese], December 3, 2019, available at: www.soumu.go.jp.

59. US Department of State, Joint Statement on the 10th US-Japan Policy Cooperation Dialogue on the Internet Economy, October 11, 2019, available at: www.state.gov.

60. Ministry of Internal Affairs and Communications, "Joint Statement by the United States and Japan on Furthering the Development of Smart Cities in the Indo-Pacific," November 4, 2019, available at: www.soumu.go.jp.

61. Japan International Cooperation Agency, "ICT for Human Development and Human Security Project," available at: www.jica.go.jp.

project focused on cyber-security under the Japan-ASEAN Technical Cooperation Agreement.[62]

Shaping data governance in the Indo-Pacific and beyond

Japan's cyber-diplomacy also encompasses data governance, Society 5.0 and Data Free Flow with Trust (DFFT). Society 5.0 is Japan's science and technology policy aimed at integrating the cyber-space and physical space with information technologies.[63] It is a basic policy of innovation and digitalization, and its key technologies are artificial intelligence (AI) and data analysis. Japan has been promoting this approach within the FOIP framework, but also beyond the Indo-Pacific, at the global level. Indeed, Japan's approach inspired the 2019 G20 AI Principles that the G20 Trade Ministers and Digital Economy Ministers adopted, and followed the OECD Council Recommendation on AI.[64] The principles underline the importance of inclusive growth, sustainable development and well-being, human-centered values and fairness, transparency and relevance, robustness, security and safety, and accountability.

DFFT represents Japan's concept of cross-border non-personal data flows. It promotes free data flows in securing consumers' and businesses' trust in cross-border transfers. Prime Minister Abe proposed DFFT at the Davos Meeting in 2019 and reiterated it at the G20 and G7 summits.[65] It focuses not only on data protection and transfer but also on the economy. The G20 Osaka leaders' declaration emphasized that DFFT would harness the opportunities of the digital economy while addressing challenges in privacy, data protection, intellectual property and security.[66] By promoting DFFT, Japan seeks to lead the rule-making in the digital economy. During the G20 Osaka summit, Prime Minister Abe hosted a special event on the digital economy and issued the "Osaka Declaration on Digital Economy," which proclaimed the launch of the "Osaka Track," a process for rule-

62. Japan International Cooperation Agency, "The first technical cooperation project implemented under the Japan-ASEAN Technical Cooperation Agreement: Making contribution to building up capacity to formulate policy to ensure cybersecurity in the ASEAN region," February 7, 2020, available at: www.jica.go.jp.
63. Cabinet Office, Society 5.0, available at: www8.cao.go.jp.
64. Ministry of Foreign Affairs, G20 Ministerial Statements on Trade and Digital Economy – Annex G20 AI Principles, June 9, 2019, available at: www.mofa.go.jp; OECD Legal Instruments, Recommendation of the Council on Artificial Intelligence, May 22, 2019, available at: www.legalinstruments.oecd.org.
65. Ministry of Foreign Affairs, Speech by Prime Minister Abe at the World Economic Forum Annual Meeting, January 23, 2019, available at: www.mofa.go.jp.
66. G20, G20 Osaka Leaders' Declaration, June, 2019, available at: www.g20.org.

making on the digital economy that boosted negotiations at the World Trade Organization (WTO).[67]

Japan's challenges in articulating cyber-diplomacy and cyber-defense

The missing piece of Japan's diplomacy on cyber-security is a policy implementing the FOIP pillar regarding security. Japan's contribution was mainly to foster defensive capabilities in the region. However, the growing number of malicious behaviors in cyber-space shows that good defense alone is not enough to deter attacks. Therefore, Japan's cyber-diplomacy should also promote coordinated actions with partners against cyber-attacks.

Japan has limited options to deter a cyber-attack. Attackers consider the odds of success and the consequences of the attack. In this process, they check whether their targets have the capability of detection and identification, the will to conduct counterattacks, and the capability to decide that an attack exceeds the threshold. If attackers do not have to consider the victim's reprisal, their calculus of consequences is favorable for attacks.

Deploying punishment capability is an option for Japan to deter cyber-attacks. The imposition of sanctions would be a powerful tool for realizing its punishment capabilities by not only inflicting economic damage but also disclosing the actors responsible for the attacks. The United States and the European Union have maintained programs to impose sanctions for malicious activity in cyber-space. While Japan has already imposed sanctions on individuals and organizations threatening international peace, these threats were not related to cyber-attacks. To fulfill its international obligations and achieve international peace, imposing sanctions on actors responsible for serious cyber-attacks is a possible option. It is also critical for Japan to join internationally coordinated action to counter cyber-attacks. Japan has already released public statements as a reaction to cyber-attacks threatening its national security environment. It also cautiously selects different narratives depending on the consequences of releasing a particular statement. It blamed North Korea for cyber-attacks targeting Japan in 2017 in a statement that directly pointed to the government of North Korea as being responsible for the attack.[68] However, the Japanese government did not

67. G20, Osaka Declaration on Digital Economy, June 28, 2019, available at: www.g20.utoronto.ca.
68. Ministry of Foreign Affairs, The U.S. Statement on North Korea's Cyberattacks (Statement by Press Secretary Norio Maruyama), December 20, 2017, available at: www.mofa.go.jp.

mention the connection between the cyber-attacks and the Chinese government, while the United States and the United Kingdom released statements that Beijing had been responsible for the attack, and led an internationally coordinated action criticizing the attack.[69]

In another instance, the United States, the European Union, the United Kingdom and other countries publicly attributed the cyber-attack on Georgia to the Russian government.[70] Internationally coordinated statements effectively imposed political costs on adversaries without disclosing details.

Conclusion

FOIP undergirds Japan's principles and views in the cyber-domain, and integrates ongoing initiatives in accordance with geopolitical and technological changes. It has been successful in strengthening ties between partners. Despite the great-power competition between the United States and China, or India's disapproval of DFFT, the Japanese government has continued its efforts to establish its basic approach and expand its influence in international communities.

Japan's cyber-diplomacy shaped collective action to influence international fora. Tokyo has conducted bilateral and multilateral cyber discussions and cooperates with international partners to ensure a free, fair and secure cyber-space. Moreover, FOIP provides a comprehensive direction of international engagement for relevant policies contributing to the rule-making on the digital economy and data governance.

Despite its successful engagement in the cyber-domain, the FOIP security pillar is not fully implemented in its diplomacy. Tokyo has limited options to counter malicious cyber-activities. It has never imposed sanctions for cyber-attacks and has seldom blamed any sponsoring states or organizations. The imposition of sanctions is an option that Japan might take to change the calculus of actors, contributing to coordinated action in the cyber-domain.

69. Ministry of Foreign Affairs, "Cyberattacks by a group based in China known as APT10 (Statement by Press Secretary Takeshi Osuga)," December 21, 2018, available at: www.mofa.go.jp; US Department of State, "Joint Statement by Secretary of State Michael R. Pompeo and Secretary of Homeland Security Kirstjen Nielsen: Chinese Actors Compromise Global Managed Service Providers," December 20, 2018, available at: www.state.gov.

70. Council of the EU, "Declaration by the High Representative on behalf of the European Union – Call to Promote and Conduct Responsible Behavior in Cyberspace," February 21, 2020, available at: www.consilium.europa.eu.

ifri
since 1979
French Institute
of International
Relations