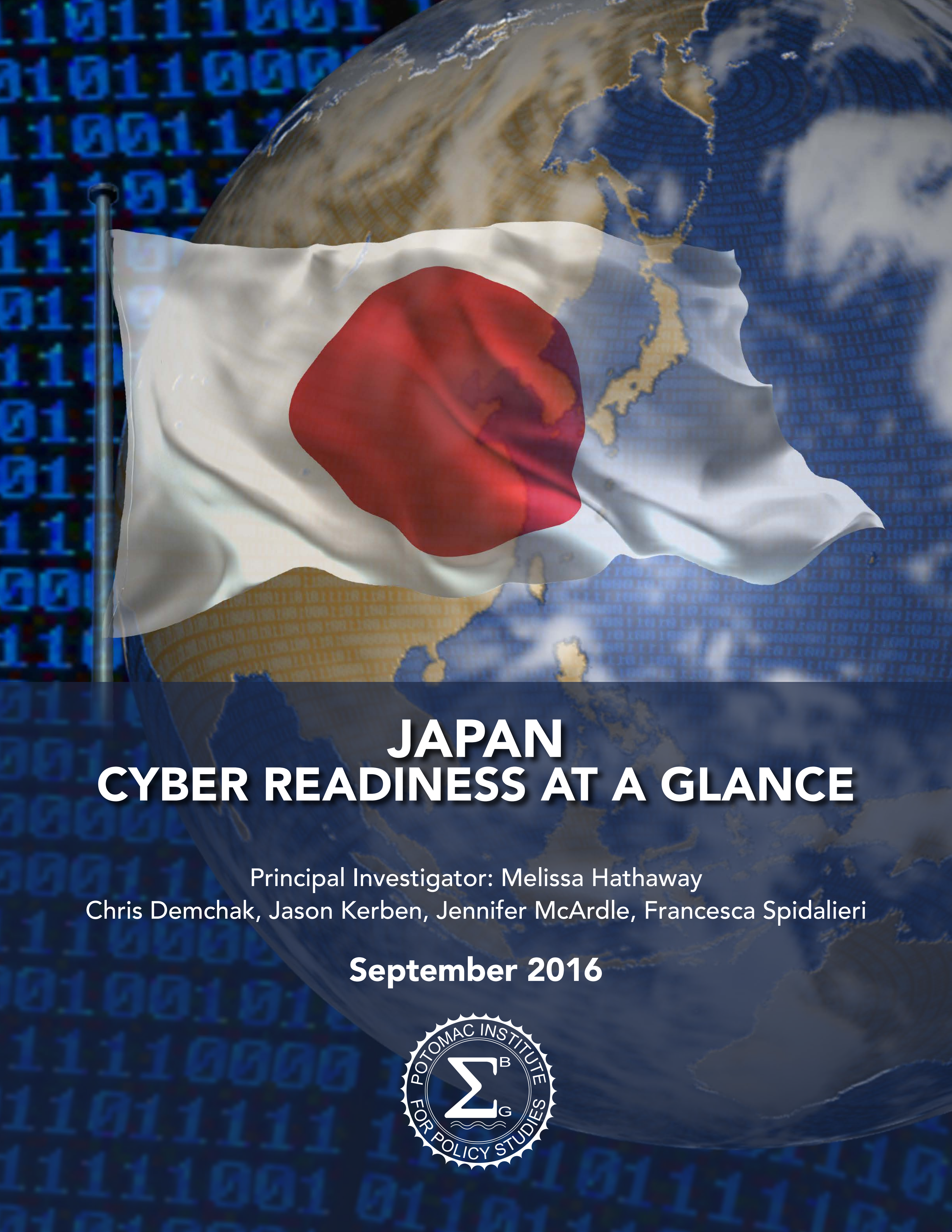


JAPAN
CYBER READINESS AT A GLANCE

Principal Investigator: Melissa Hathaway
Chris Demchak, Jason Kerben, Jennifer McArdle, Francesca Spidalieri

September 2016

POTOMAC INSTITUTE FOR POLICY STUDIES

Published by Potomac Institute for Policy Studies

Potomac Institute for Policy Studies
901 N. Stuart St, Suite 1200
Arlington, VA 22203
www.potomacinstitute.org
Telephone: 703.525.0770; Fax: 703.525.0299

Email: *CyberReadinessIndex2.0@potomacinstitute.org*

Follow us on Twitter:
@CyberReadyIndex

Cover Art by Alex Taliesen.

Acknowledgements

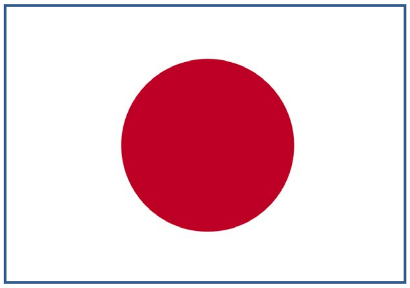
The Potomac Institute for Policy Studies and the authors would like to thank the following individuals for their contributions: Mr. Ikuo Takahashi of the Komazawa Legal Chambers; Mr. Ide Tatsuo of the National Defense Academy; Mr. Akira Saka of the Japan Cybercrime Control Center; Mr. Masumitsu Ito of KMPG; Admiral (ret.) Dennis Blair of the Sasakawa Peace Foundation, USA; Mr. Yasuhiko Taniwaki of the National Center for Incident Readiness and Strategy for Cybersecurity; and Major General Jiro Hiroe of the Japan Ministry of Defense. The authors would also like to thank Alex Taliesen for cover art and Sherry Loveless for editorial and design work.

JAPAN
CYBER READINESS AT A GLANCE

TABLE OF CONTENTS

JAPAN

CYBER READINESS AT A GLANCE



Country Population	127 million
Population Growth	-0.1%
GDP at market prices (current $US)	$4.123 trillion
GDP Growth	0.5%
Year Internet Introduced	1986
National Cyber Security Strategy	2013, updated in September 2015
Internet Domain	.jp
Fixed broadband subscriptions per 100 users	29.3
Mobile broadband subscriptions per 100 users	121.4
Mobile phone subscriptions per 100 users	120.2

Information and Communications Technology (ICT) Development and Connectivity Standing

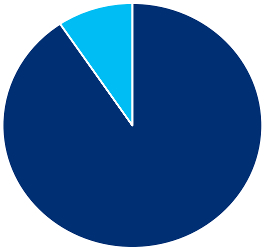
International Telecommunications Union (ITU) ICT Development Index (IDI)	11	World Economic Forum's Network Readiness Index (NRI)	10

Sources: World Bank (2015), ITU (2015), NRI (2015), and Internet Society.

INTRODUCTION

When the Internet was first introduced to Japan in the mid-1980s, it began as a scientific academic experiment. It took almost a decade for homes and offices around the country to have Internet connectivity. Today, Japan is a highly connected and digitally dependent country, and its population is among the most avid users of information communication technologies (ICTs) in the world with more than 90 percent Internet penetration. The key drivers of connectedness continue to be subscriptions to mobile communications and mobile broadband, while subscriptions to fixed line communications decline. To ease bottlenecks from increased mobile device usage, the Japanese government plans to share spectrum allocated to weather and amateur radio to double the bandwidth for wireless communications by 2017.

The Japanese government has been struggling for years to pull the world's 3rd largest economy out of a period of prolonged economic stagnation. At present, the ICT sector accounts for 9 percent of Japan's gross domestic product (GDP) – a lower figure than previous years as Japan's recession share of the global ICT market has fallen since 2014. Moreover, Japan has lost a significant share of its ICT exports, from 5 percent in 2012 to 3.3 percent in 2014, in contrast to the rest of the Asia-Pacific that has witnessed steady increases. The Japanese government views ICT as a mechanism to generate future growth. Japan expects the ICT sector to double by 2020, with the majority of that growth emerging from Internet of Things (IoT) opportunities. The Japanese government has also declared its goal of being the world's most advanced information technology (IT) nation by 2020 and is working to generate the right environment for ICT development through the promotion of open data, research and development (R&D), a world class ICT infrastructure, and a stronger cyber security posture.[1]

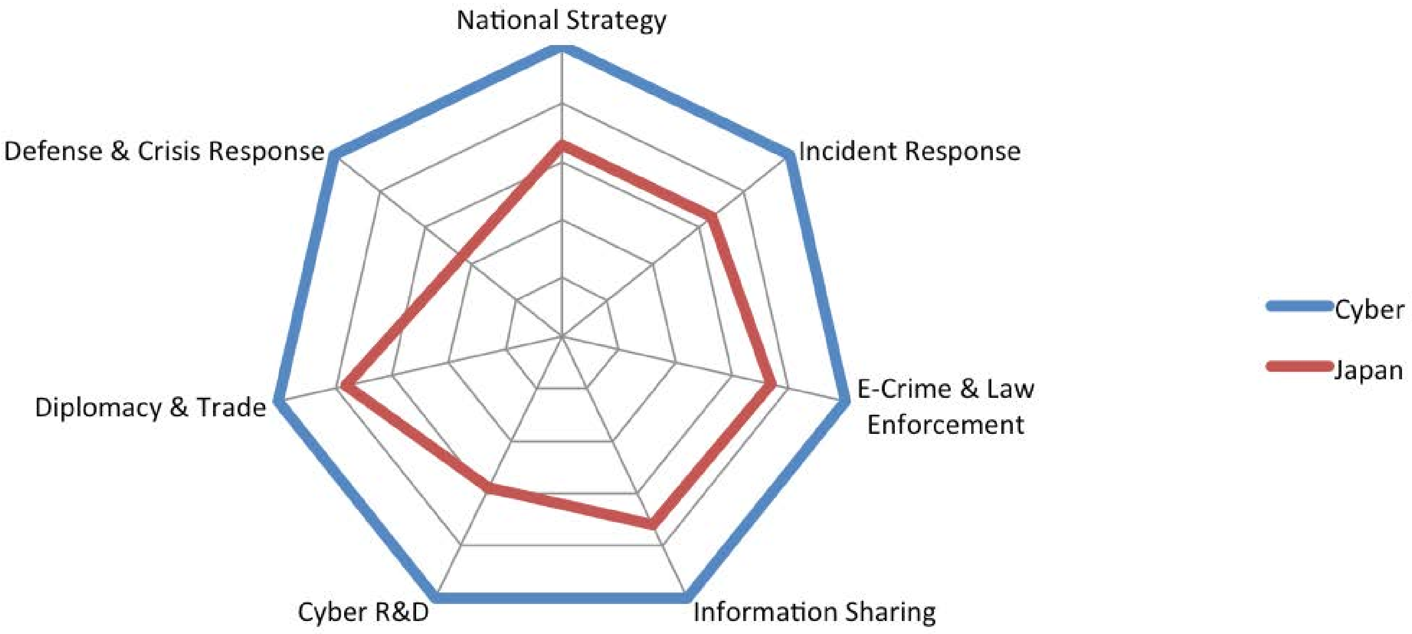

Japan Internet Penetration: 90.6%

While cyber security is not a new issue for Japan, Prime Minister Abe is now taking advantage of Japan's central role in hosting upcoming global events, such as the 2016 G-7 Ministerial meeting and the 2020 Tokyo Olympics and Paralympics Games, to transform cyber challenges into opportunities to drive Japan's security and resilience agendas. Indeed, Prime Minister Abe is using these events to establish cyber security as a national priority, placing renewed urgency on developing cyber security capacity and resilience. By dovetailing these efforts with the emerging IoT marketplace, Abe is also positioning Japan to secure a broader position of ICT economic marketplace dominance.

The Cyber Readiness Index (CRI) 2.0 has been employed to evaluate Japan's preparedness levels for cyber risks. This analysis provides an actionable blueprint for Japan to better understand its Internet-infrastructure dependencies and vulnerabilities and assess its commitment to and maturity in closing the gap between its current cyber security posture and the national cyber capabilities needed to support its digital future. A full assessment of the country's cyber security-related efforts and capabilities based on the seven essential elements of the CRI 2.0 (national strategy, incident response, e-crime and law enforcement, information sharing, investment in R&D, diplomacy and trade, and defense and crisis response) is depicted in the Figure "Japan Cyber Readiness Assessment (2016)," below.

1. NATIONAL STRATEGY

The Japanese government has been refining its national cyber security strategy in a series of iterations starting in 2006 with the release of "First National Strategy on Information Security."[2] In 2009, Japan published the "Second National Strategy on Information Security,"[3] and in 2013, the Information Security Policy Council (now the Cybersecurity Strategic Headquarters) released its first dedicated national "Cybersecurity Strategy." In September 2015, the Japanese Cabinet approved the second Japanese "Cybersecurity Strategy," which is indicative of the importance senior leaders now place on cyber security.[4] The development of the 2015 strategy was mandated by the November 2014 "Cybersecurity Basic Act," which states that cyber security policy in Japan must adhere to the following



Japan Cyber Readiness Assessment (2016)

The 1st Japanese National Cyber Security Strategy was published in 2013 and the 2nd iteration was released in 2015.

principles: free flow of information, respect of citizen rights, multi-stakeholder approach, and cooperation.

In contrast to the 2013 strategy, the new cyber security strategy highlights both the opportunities and risks associated with ICT uptake. The Japanese government recognizes ICT as a potential source of economic growth through innovation (particularly as the IoT expands), but also as a source of risks and insecurity. In many ways, the 2015 cyber security strategy's emphasis on business opportunities, innovation, and the IoT aligns with Japan's ICT strategic policy agenda – Japan's "digital agenda" – which is based on a series of ministerial-level policies, such as Japan's "ICT Growth Strategy," "Japan Revitalization Strategy," and the "Declaration to be the World's Most Advanced IT Nation."

In the 2015 strategy, the Japanese government highlights the importance of securing critical information infrastructure (CII) as a key priority area and affirms that a multi-stakeholder approach is required to ensure the security of CII. The main CII sectors include electrical power, water services, information and communications services, and financial services, among others.

The 2015 strategy also designates a competent authority for the strategy's implementation – the Cybersecurity Strategic Headquarters. Established in 2014 through a reorganization of the Information Security Policy Council, the Cybersecurity Strategic Headquarters acts as the command and control body for national cyber security with the authority to provide recommendations to other governmental agencies. The Headquarters, led by the Chief Cabinet Secretary, Yoshihide Suga, also includes the foreign minister, the defense minister, the trade and economy minister, the internal affairs minister, the chairman of the National Public Safety commission, and other members and experts appointed by the prime minister.

Finally, in August 2016, the Japanese National center of Incident readiness and Strategy for Cybersecurity (NISC) released a "General Framework for Secured IoT Systems" as a follow-up to the 2015 national cybersecurity strategy. While the national strategy had already acknowledged the importance of sustainable economic development through IoT innovation and security, the new framework suggests that Japan will start seeking security even in non-critical infrastructure, including manufacturers, and pursuing a global multi-stakeholder approach to security in IoT.[5]

2. INCIDENT RESPONSE

Since the mid 1990s, Japan has developed a series of organizations dedicated to incident response in the event of cyber emergencies and crises, beginning with the establishment of a national Computer Emergency Response Team Coordination Center (JPCERT/CC) in 1996.[6]

With the passage of the new 2014 "Cybersecurity Basic Act," the already established National Information Security Center was elevated and renamed the National center of Incident readiness and Strategy for Cybersecurity (NISC) and now serves as the secretariat for the new Cybersecurity Strategic Headquarters (formerly the Information Security Council), effective as of March 2016.[7] The Act codified NISC and gave it a range of responsibilities, including coordinating policies, monitoring government-related organizations that handle large volumes of personal information, and providing command and control in times of crisis including attacks on critical infrastructure.

The 2014 "Cybersecurity Basic Act" formalized the National center of Incident readiness and Strategy for Cybersecurity.

The 2015 Japanese national "Cybersecurity Strategy" emphasizes the multi-stakeholder approach. This is also reflected in the organizational structure of the JPCERT/CC – a registered, independent, non-profit organization serving government ministries and the private sector since 2003. In addition to coordinating incident response with other CSIRTs, relevant government agencies, network service providers, security vendors, and industry associations, JPCERT/CC collects information about cyber incidents through a complex reporting process, and regularly publishes incident threat monitoring reports; incident handling reports, including daily updates on cases coordinated per business category; additional studies; technical notes; and press releases.[8]

Moreover, JPCERT/CC helped establish, and is the secretariat of, the Asia Pacific Computer Emergency Response Team (APCERT) that is instrumental in organizing an annual international cyber drill with other CERTs in the larger Asia-Pacific region.[9] Additionally, JPCERT/CC is part of a trilateral annual CERTs meeting among the countries of Japan, China, and Korea to discuss cyber incident response mechanisms. The meetings have helped instill confidence and trust among these three countries, which have historically experienced tensions, and have resulted in the development of a "cyber hotline" to communicate on significant cyber incidents.[10] Japan also conducts various cyber drills and exercises involving all relevant ministries and the National Police Agency in preparation for the 2020 Tokyo Olympic Games.[11]

Japan is standing up an Industrial Cybersecurity Promotion Agency (ICPA) – a new operational agency under the Ministry of Economy, Trade, and Industry (METI) – to protect Japan's critical infrastructures from cyber attacks. The new agency will focus on using "white hat hackers" to increase the resilience of key sectors including: electricity, gas, petroleum, chemical, and nuclear facilities. The ICPA opens in 2017, and the government wants it to be fully operational and ready to defend the country in time for the 2020 Olympics. In addition, the Japanese government recently announced the creation of a "cyber attack institute" to train its employees to prevent, mitigate, and respond to cyber attacks to critical infrastructures.[12] The institute, which is also expected to be operational by early 2017, will be the first center for training in Japan to focus specifically on preventing cyber incidents on electrical systems and stopping leaks of sensitive power plant designs. The training institute will operate as part of Japan's Information-Technology Promotion Agency (IPA), with the goal of preventing potential large-scale blackouts during the 2020 Tokyo Olympics and Paralympics.

Japan's overall efforts show a dedicated campaign to resolve challenges in intergovernmental coordination, while working to unify government operations impacting incident response capabilities.

3. E-CRIME AND LAW ENFORCEMENT

Japan signed and ratified the Council of Europe Convention on Cybercrime (commonly known as the Budapest Convention) in 2001 and since then has been developing a series of cyber crime legislation, efforts for international cooperation, and processes to combat criminal offenses in cyberspace. Apart from acceding to international cyber crime law, Japan has also revised its penal code to include relevant cyber offenses and passed several other laws, including: the Unauthorized Computer Access Law, the Telecommunications Law, the Copyright Law, the Child Pornography Law, the Classified Information Law, and the Law on Electronic Signatures.[13] Japan is also currently reviewing its Personal Data Protection Law to ensure its suitability with personal big data usage. In recent years, Japanese law enforcement has been successful in identifying, arresting, and prosecuting local cyber criminals illegally exfiltrating customers' personal data and trade secrets from Japanese companies.

Japan established its first independent data protection authority – the Personal Information Protection Commission (PIPC) – in 2014, and revised it in 2015, making it responsible for the protection of all personally identifiable information of Japanese citizens. Prior to the establishment of this authority, sixteen different ministries enforced privacy in various sectors overseen by government. This effort has become increasingly important, as Japan has launched a large-scale program to establish a national digital identity for all citizens to ensure accurate and rapid identification and verification. In the wake of the 2011 earthquake and tsunami, the Tokyo energy company Tepco has accelerated plans for the deployment of smart metering. The company plans to have smart meters deployed to 80 percent of customers by 2018. In addition, near field communication technology, such as Japan's *Suica* metro smart card, is being utilized and expanded for contactless payments, with banks introducing the wireless technology to credit and debit cards.

Moreover, Japan's Cyber Clean Center was created in 2006 to provide malware remediation and anti-botnet solutions.[14] This Center was the result of a cross-disciplinary collaboration among JPCERT/CC, various security vendors, and Internet service providers (ISPs), and created an automated "guardian network" against botnet malware infection and exploitation. It also provided tailor made solutions to address specific malware on individual computers. The Center was dismantled in 2011 and its functions moved to Telecom Information Sharing and Analysis Center Japan (T-ISAC Japan). In 2013, Japan suffered a breach that affected over 20,000 unique IP addresses, indicating a need to further strengthen botnet remediation capabilities.

4. INFORMATION SHARING

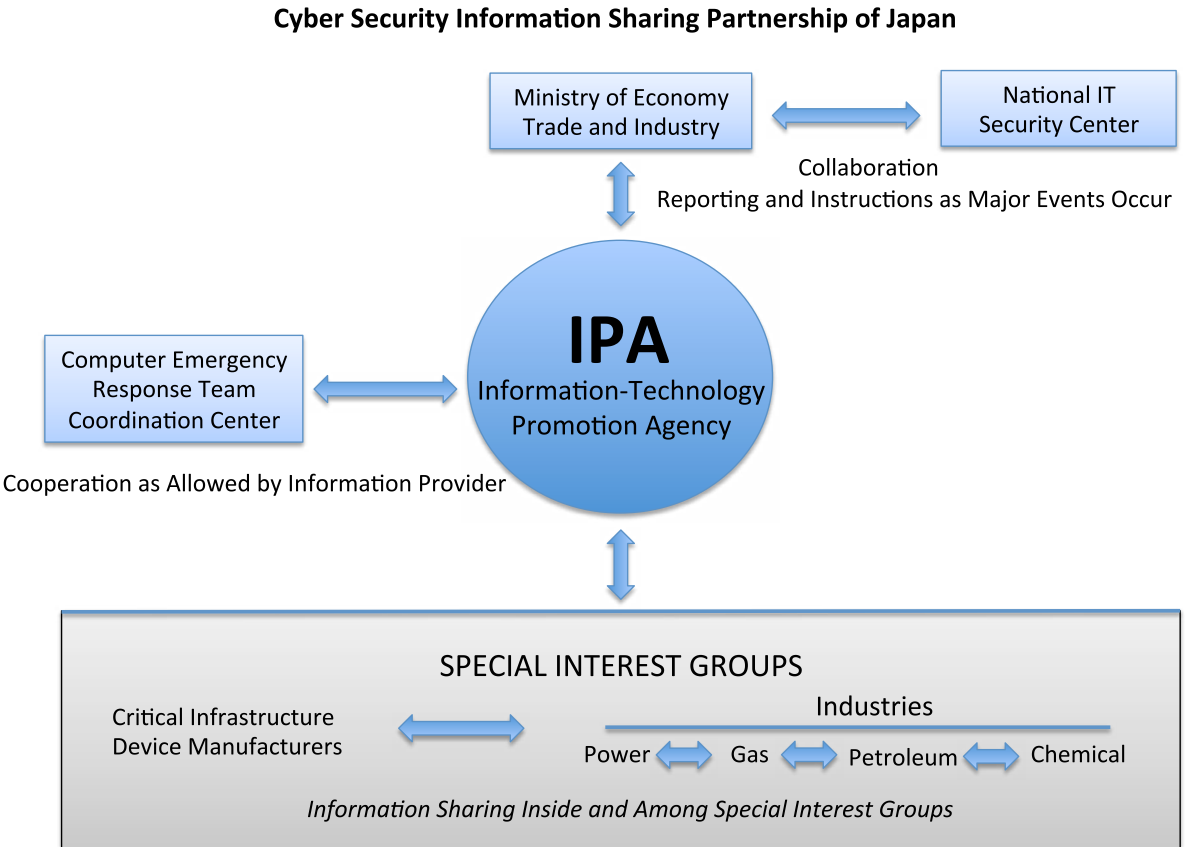
In order to build coordinated relationships and enhance information sharing arrangements, Japan is supporting the advancement and expansion of information sharing networks among public and private sectors. These measures include increasing the cyber-related knowledge and experience of administrative agencies and other organizational entities with information sharing and analysis functions, such as the various ISACs. Each governmental body is now required to work in close coordination and collaboration with the National Center for Incident Readiness and Strategy for Cybersecurity to share information with and provide essential advice to organizations and business operators under their respective jurisdictions. This is consistent with both the new 2015 national cyber security strategy and the third edition of the "Basic Policy of Critical Information Infrastructure Protection," which re-

The Information-Technology Promotion Agency is the recognized institutional authority charged with sharing information between government and critical industries.

emphasized the importance of collaboration and information sharing among all "cyberspace-related stakeholders, including CII operators, enterprises, and individuals."[15]

The IPA – an affiliated organization to METI – is the institutional authority responsible for facilitating information sharing between government and critical industries, and has established trusted relationships with all major companies in the country.[16] IPA operates the Cyber Security Information Sharing Partnership of Japan (J-CSIP) – a public-private partnership that provides a continuous information sharing platform as well as network-wide responses to cyber security incidents that affect critical infrastructure.[17] Members include companies and industry organizations that the government will work with to prevent cyber attacks. Moreover, IPA works closely with METI, NISC, JPCERT/CC, and the Cyber Rescue Advice Team (J-CRAT) to respond to all major cyber incidents affecting critical infrastructure.

According to the 2015 national cyber security strategy, the Japanese government intends to strengthen and expand its information gathering and analysis functions and activities so as to foresee and detect threats in cyberspace faster and more effectively. The government


Cyber Security Information Sharing Partnership of Japan
Ministry of Economy Trade and Industry
National IT Security Center
Collaboration
Reporting and Instructions as Major Events Occur
IPA
Information-Technology Promotion Agency
Computer Emergency Response Team Coordination Center
Cooperation as Allowed by Information Provider
SPECIAL INTEREST GROUPS
Critical Infrastructure Device Manufacturers
Industries
Power
Gas
Petroleum
Chemical
Information Sharing Inside and Among Special Interest Groups

Information-Technology Promotion Agency Organizational Chart, 2016. (http://www.ipa.go.jp) also plans to build a highly sophisticated detection, analysis, and crisis response cell to enable immediate detection and response actions against cyber attacks. The government will also accelerate the creation of a specialized CERT for the 2020 Olympics as a core organ responsible for information sharing among stakeholders vital to the safe management and operation of this major international event and other associated businesses.

5. INVESTMENT IN RESEARCH AND DEVELOPMENT

The 2011 "Information Security Research and Development Strategy"[18] re-emphasized the Japanese government's support for public and private ICT R&D efforts conducted under the rubric of the "Grand-Challenge Project for R&D and Technology Development" since 2005. The Grand-Challenge project sought to integrate long-term and short-term R&D technology projects, which focused on changes in Japan's ICT security environment such as innovative ICT (i.e., cloud computing), sophisticated and diverse threats (e.g., advanced persistent threats [APTs]), and building resilient ICT systems in the face of natural disasters. Despite the progress made by this project, the government's information security budget dropped by 47 percent, from 9.12 billion yen (~US $81 million) to 4.86 billion yen (~US $43 million), between 2006 and 2010. The 2011 government R&D strategy described this as an "alarming" trend in comparison to other countries' growing R&D budgets. In 2013, a report by Japan's National Information Security Center (now the National center of Incident readiness and Strategy for Cybersecurity) noted that the country had a shortage of 80,000 information security engineers and that current practicing cyber security professionals lacked the skills required to effectively counteract online threats.[19]

In preparation to host the G-7 and the 2020 Olympics, Japan's Ministry of Internal Affairs and Communications requested around 20 billion yen (~US $178 million) in government funding over four years, starting in FY2016, in relation to the Olympic Games.[20] This funding allows for training of local authorities, schools, and enterprises. The Ministry will oversee exercises to prepare for cyber attacks linked to the Games.

The Japanese Ministry of Internal Affairs and Communications requested additional funding for cyber security training in preparation for the 2020 Olympics.

In addition, the 2013 cyber security strategy emphasized lower taxes as a corporate incentive to allow small and medium businesses to increase investment in information security. Similarly, the 2015 cyber security strategy highlights the importance of innovation to the economy. Based on 2014 data, small companies get a 12 percent credit on R&D expenditures, whereas large companies get an 8-10 percent credit. Tax incentives are also available at higher amounts for companies whose sole focus is R&D.[21] These tax incentives are not solely focused on cyber security and ICT; it is unclear at present if Japan has a unique vehicle to incentivize commercial cyber R&D.

Finally, Japan sponsors an annual national cyber security awareness campaign during the month of February, and currently promotes two other initiatives to raise cyber security awareness– "Kawaii," a password protection campaign and "Ghost in the Shell," an information campaign utilizing posters and cartoons.

6. DIPLOMACY AND TRADE

Japan has been actively engaged in diplomatic and trade negotiations related to cyber security and ICT components over the last ten years. In fact, the Japanese Ministry of Foreign Affairs (MFA) *Diplomatic Bluebook* lists cyber security as a top tier element of the country's foreign policy.[22] In response to growing concern about cyber security, the MFA recently established a new Cyber Security Policy Division, composed of fifteen ministry officials, specifically dedicated to promoting the cyberspace rule of law.[23] The Ministry plans to use the division to coordinate diplomatic and legal efforts with other like-minded countries on the rules governing cyberspace, as well as to support capacity-building initiatives in developing countries.

Moreover, Japan has regularly participated in a wide variety of international and bilateral meetings involving cyber security and ICTs. In February 2016, Japan signed the Trans Pa-

The Japanese Ministry of Foreign Affairs recently established a new Cyber Security Policy Division dedicated to promoting the rule of law in cyberspace.

cific Partnership (TPP), which includes cyber security, e-commerce, and encryption obligations. Japan is also currently engaged in negotiations for the Regional Comprehensive Economic Partnership (RCEP), which includes numerous cyber-related proposals – from copyright to a prohibition on the Internet retransmission of broadcasts, among others.

As a participating state in the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual Use Technologies, Japan has agreed to curb the sale of Internet surveillance and specifically modified intrusion software capable of evading monitoring tools or defeating countermeasures. Additionally, Japan has active representation in the Japan-ASEAN Information Security Policy Meeting, the Japan-US Cyber Dialogue, the Japan-US Policy Cooperation Dialogue on the Internet Economy, and the Japan-US Defense Policy Working Group. Most notably, Japan has worked to shape global norms through an active participation in the United Nations Group of Government Experts (UN GGE), and especially through its contribution to the UN GGE report on *Developments in the Field of Information and Telecommunications in the Context of International Security.*[24] In 2012, the Japanese MFA recognized that international law is applicable in cyberspace – a recognition that was reaffirmed again during the G7 Summit in Japan in May 2016.

7. DEFENSE AND CRISIS RESPONSE

Both the 2013 and 2015 Japanese national security strategies emphasize the importance of cyber defense. In 2012, the Ministry of Defense (MoD) announced plans to create a Cyber Defense Unit (CDU) with an anticipated budget of US $142 million and 100 personnel.[25] The unit was subsequently established in 2014. The CDU's key goals are to protect information systems, collect data on malware and viruses, and identify response mechanisms. Moreover, in the event of conjoined cyber and armed attacks, the MoD and the Self-Defense Forces (SDF) are tasked with responding and handling the incident. Japan plans to extend these capabilities by working closely with the US and conducting joint cyber drills and exercises. In view of the Abe Administration's efforts to change Article 9 of the Constitution to allow for collective self-defense, it is possible that as the administration's mission matures, the SDF and CDU may expand their capabilities to contribute to a larger national cyber security posture.

In 2014, the Japanese Ministry of Defense established a dedicated Cyber Defense Unit to strengthen Japan's national cyber security posture.

CRI 2.0 BOTTOM LINE

According to the CRI 2.0 assessment, Japan is on a path to becoming cyber ready, and is currently partially operational in all of the seven CRI essential elements.

The findings in this analysis represent a snapshot in time of a dynamic and changing landscape. As Japan continues to develop and update its economic (digital agenda) and national cyber security strategies, policies, and initiatives to reflect a more balanced approach that aligns its national economic visions with its national security priorities, updates to this country profile will reflect those changes and monitor, track, and evaluate substantive and notable improvements.

The CRI 2.0 offers a comprehensive, comparative, experience-based methodology to help national leaders chart a path towards a safer, more resilient digital future in a deeply cybered, competitive, and conflict prone world. For more information regarding the CRI 2.0, please see: http://www.potomacinstitute.org/academic-centers/cyber-readiness-index.

Legend

- ● **Fully Operational**
- ◐ **Partially Operational**
- ○ **Insufficient Evidence**

IDI Rank			NRI Rank	GDP Rank	National Strategy	Incident Response	E-Crime & Law Enforcement	Information Sharing	Investment in R&D	Diplomacy & Trade	Defense & Crisis Response
11	Japan	🔴	10	3	◐	◐	◐	◐	○	◐	○

ENDNOTES

1. OECD, OECD *Digital Economy Outlook 2015*, (OECD Publishing: Paris): 21, http://www.keepeek.com/Digital-Asset-Management/oecd/science-and-technology/oecd-digital-economy-outlook-2015_9789264232440-en#page1.

2. Japan Information Security Policy Council, "The First National Strategy on Information Security," February 2, 2006, http://www.nisc.go.jp/eng/pdf/national_strategy_001_eng.pdf.

3. Japan National Information Security Policy Council, "The Second National Strategy on Information Security," February 3, 2009, http://www.nisc.go.jp/eng/pdf/national_strategy_002_eng.pdf.

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

5. Mihoko Matsubara, "Assessing Japan's Internet of Things (IoT) Security Strategy for Tokyo 2020," *PaloAlto Networks*, September 19, 2016, http://researchcenter.paloaltonetworks.com/2016/09/cso-assessing-japans-internet-of-things-iot-security-strategy-for-tokyo-2020/.

6. JPCERT, "Activities: Incident Response and Analysis," https://www.jpcert.or.jp/english/pr/.

7. Information Security Policy Council, "The Basic Policy of Critical Information Infrastructure Protection," May 9, 2014, http://www.nisc.go.jp/eng/pdf/actionplan_ci_eng_v3.pdf, and Japan National Center of Incident Response and Strategy for Cyber Security, http://www.nisc.go.jp/eng/index.html.

8. JPCERT, "Incident Handling Quarterly Report," https://www.jpcert.or.jp/english/ir/report.html.

9. APCERT, "APCERT Embarks on Cyber Attacks Beyond Traditional Sources," http://www.apcert.org/documents/pdf/APCERTDrill2015PressRelease_Final.pdf.

10. CNCERT/CC, "2nd China-Japan-Korea CSIRT Annual Meeting for Cybersecurity Incident Response was held in Korea," http://www.cert.org.cn/publish/english/55/2014/ 201409161457 39295996084/ 201409161457 39295996084_.html.

11. Tim Kelly and Nobuhiro Kubo, "Japan holds first broad cybersecurity drill, frets over Olympics risks," *Reuters*, March 18, 2014, http://www.reuters.com/article/us-japan-cyber-crime-idUSBREA2G1O920140318.

12. Nicky Cappella, "Japanese government plans cyber attack institute," *The Stack*, August 24, 2016, https://thestack.com/security/2016/08/24/japanese-government-plans-cyber-attack-institute/.

13. Japan National Police Agency, *White Paper on Police 2014*, https://www.npa.go.jp/hakusyo/h26/english/Contents_WHITE_PAPER_on_POLICE2014.htm, and National Center for Incident readiness and Strategy for Cybersecurity, "Related laws and regulations," http://www.nisc.go.jp/law/index.html.

14. Ministry of Internal Affairs and Communications and Ministry of Economy, Trade, and Industry, “What is Cyber Clean Center,” https://www.telecom-isac.jp/ccc/en_index.html.

15. Information Security Policy Council, “The Basic Policy of Critical Information Infrastructure Protection,” 2014.

16. Information-Technology Promotion Agency, “About IPA,” https://www.ipa.go.jp/english/about/index.html.

17. Information-Technology Promotion Agency, “Initiative for Cyber Security Information sharing Partnership of Japan (J-CSIP) Annual Activity Report FY2012,” (April 2013).

18. Japan Information Security Policy Council, “Information Security Research and Development Strategy,” (July 8, 2011).

19. Government of Japan, “Cybersecurity Strategy,” http://www.nisc.go.jp/eng/pdf/cs-strategy-en.pdf.

20. Doug Drinkwater, “Japan to train thousands on cybersecurity pre 2020,” *SC Magazine*, July 22, 2015, http://www.scmagazineuk.com/japan-to-train-thousands-on-cyber-security-ahead-of-2020-olympics/article/427765/.

21. “2014 Global Survey of R&D Tax Incentives,” *Deloitte* (2014): 26, https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Tax/dttl-tax-global-rd-survey-aug-2014.pdf.

22. Japanese Ministry of Foreign Affairs, *Diplomatic Bluebook*, http://www.mofa.go.jp/policy/other/bluebook/.

23. “Foreign Ministry sets up division to push rule of law in cyberspace,” *Japan Economic Newswire*, July 12, 2016.

24. UNODA, *Developments in the Field of Information and Telecommunications in the Context of International Security*, https://www.un.org/disarmament/topics/informationsecurity/.

25. Japan Ministry of Defense, “Defense Programs and Budget of Japan: Overview of FY2014 Budget Request,” http://www.mod.go.jp/e/d_budget/pdf/251009.pdf.

For more information or to provide data to the CRI 2.0 methodology, please contact:

CyberReadinessIndex2.0@potomacinstitute.org

ABOUT THE AUTHORS

Melissa Hathaway is a leading expert in cyberspace policy and cybersecurity. She serves as a Senior Fellow and a member of the Board of Regents at Potomac Institute for Policy Studies and is a Senior Advisor at Harvard Kennedy School's Belfer Center for Science and International Affairs. She served in two Presidential administrations where she spearheaded the Cyberspace Policy Review for President Barak Obama and led the Comprehensive National Cybersecurity Initiative for President George W. Bush. She developed a unique methodology for evaluating and measuring the level of preparedness for certain cybersecurity risks, known as the Cyber Readiness Index. She publishes regularly on cybersecurity matters affecting companies and countries. Most of her articles can be found at the following website: *http://belfercenter.ksg.harvard.edu/experts/2132/melissa_hathaway.html*.

Chris Demchak is a subject-matter expert on the Potomac Institute for Policy Studies' Cyber Readiness Index project. Her research areas are digital resilience, cyber conflict, and the structures and risks of cyber space. She designed a digitized organization model known as "Atrium" that helps large enterprises respond to and accommodate surprises in their systems. She is also the author of *Wars of Disruption and Resilience: Cybered Conflict, Power and National Security*.

Jason Kerben is a subject-matter expert on the Potomac Institute for Policy Studies' Cyber Readiness Index project. He also serves as senior advisor to multiple Departments and Agencies in matters related to information security and cyber security. In particular, he focuses on legal and regulatory regimes that impact an organization's mission. He develops methodologies and approaches to assess and manage cyber security risk and advises on a myriad of specific cybersecurity activities including international principles governing information and communications technologies, identity and access management, continuous diagnostics and mitigation and cyber insurance.

Jennifer McArdle is a Non-Resident Fellow at the Potomac Institute for Policy Studies and an Assistant Professor of Cybersecurity at Salve Regina University in Newport, RI. Jennifer's academic research and publications focus on cyber conflict, escalation management, and military innovation. She is a PhD candidate in War Studies at King's College London.

Francesca Spidalieri is a subject-matter expert at the Potomac Institute for Policy Studies' Cyber Readiness Index Project. She also serves as the Senior Fellow for Cyber Leadership at the Pell Center, at Salve Regina University, and as a Distinguished Fellow at the Ponemon Institute. Her academic research and publications focus on cyber leadership development, cyber risk management, cyber education, and cyber security workforce development. She also published a report, entitled *State of the States on Cybersecurity*, that applies the Cyber Readiness Index 1.0 at the US state level.

POTOMAC INSTITUTE FOR POLICY STUDIES
901 N. Stuart St. Suite 1200, Arlington, VA 22203
www.potomacinstitute.org