Notes de l'Ifri
Asie.Visions 91

Japan: The Reluctant Cyberpower

Franz-Stefan GADY

March 2017

ifri Center for Asian Studies

The Institut français des relations internationales (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 and a non-profit organization.

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

With offices in Paris and Brussels, Ifri stands out as one of the rare French think tanks to have positioned itself at the very heart of European debate.

ISBN: 978-2-36567-691-5

How to quote this document:
Franz-Stefan Gady, "Japan: The Reluctant Cyberpower", *Asie.Visions*, No. 91, Ifri, March 2017.

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

Ifri-Bruxelles

Rue Marie-Thérèse, 21 1000 – Bruxelles – BELGIQUE

Tel.: +32 (0)2 238 51 10 – Fax: +32 (0)2 238 51 15

Email: bruxelles@ifri.org

Website: Ifri.org

Author

Franz-Stefan Gady is a senior fellow at the EastWest Institute and senior editor of its Policy Innovation Blog. He is also a founding member of the Global Cooperation in Cyberspace Initiative, and an Associate Editor with *The Diplomat*, where he covers regional conflict and Asian defense policies.

To follow him: @hoanssolo.

Abstract

Japan's cyberdefenses remain underdeveloped compared to the country's great reliance on information and communications technology. Despite Japan's initial slow response to the security challenges emerging from cyberspace, this paper posits that cybersecurity under the administration of Japanese Prime Minister Shinzo Abe has moved to the core of the country's national security policy. The 2020 Olympics Games are a major catalyst for this.

Over the last two years the Japanese government has indeed laid the structural and legal foundations for becoming a serious player in cyberspace. That effort, however, remains underfunded and is slowed by overly complicated intergovernmental coordination processes and stovepiping within the government.

While Japan remains a reluctant cyberpower with a decidedly defensive outlook and a particularly change-resistant bureaucracy, plagued by vertical compartmentalization, recent initiatives and policies have made it clear that the country is moving in the direction of potentially becoming one of Asia's more advanced cyberpowers in the not-too-distant future.

This paper first outlines an analytical framework used to evaluate Japan's current standing and progress as a cyberpower: from whole of government (WoG) to whole of nation (WoN) and whole of system (WoS). The following three sections discuss in detail the evolutionary stages in the development of Japan's national cybersecurity strategy. The last section deals with the Japan Self-Defense Forces' changing role in cyberspace and how it is slowly embracing a more militarized response to state-sponsored cyberthreats.

The administration of Prime Minister Abe has been careful not to abandon the Japan Self-Defense Forces' defensive posture in cyberspace and has not indicated that it will develop offensive cyberwar capabilities. This, however, may change should the new US administration abandon the United States' historic solid defense commitment to Japan. In that respect, Japan's deepening of engagement with like-minded countries will assume even greater importance over the next four years.

Table of contents

Introduction

Japan is a reluctant cyberpower.[1] Up until 2013, it did not follow the trend of institution-building for cybersecurity, and has only taken steps over the last two years to systematically address cyber-vulnerabilities. That effort, however, remains underfunded, and is slowed by overly complicated intergovernmental coordination processes and stovepiping within the government. Furthermore, this reluctance is reinforced by inadequate information-sharing mechanisms concerning cyberthreats, partly due to a culture of shaming victims of cyberattacks, which makes corporations reluctant to share data. This is exacerbated by Japan's "island nation" mentality, with many Japanese taking their physical security and safety for granted.[2] In addition, Japan's defensive mindset and reluctance to develop and use offensive cybercapabilities emboldens state-sponsored actors – China and North Korea remain Japan's two biggest state adversaries in cyberspace – and cybercriminals to probe Japanese networks, conduct espionage and blackmail Japan's private sector.[3]

Overall, Japan is still the world's second information and communications technology (ICT) power after the United States. Yet, despite the Japanese government's declared goal to become the world's most advanced information technology (IT) nation by 2020, Japan ranks number 10 in the United Nations International Telecommunication Union (ITU) Information and Communication Technology (ICT) Development Index, and remains tenth in the World Economic Forum's Network

1. This paper uses Adam Segal's definition of the primary components necessary for a strong cyber power: "[L]arge or technologically advanced economies; public institutions that channel the energy and innovation of the private sector; adventurous and somewhat rapacious military and intelligence agencies; and an attractive story to tell about cyberspace." In A Segal, *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital A*ge, New York, Public Affairs, 2016). There is considerable disagreement on how to define cyberpower. Hiroshi Ito argues that information ("cyber") technology itself is its primary determinant (interview with Hiroshi Ito, Deputy Director-General for Cybersecurity and Information Technology at the Ministry of Economy, Trade and Industry, February 2, 2017). For further discussion of the term, see: G. Austin, "Mapping and Evaluating China's Cyber Power", *Lau China Institute Policy Paper Series*, September 8, 2016, available at: www.kcl.ac.uk; J. Rowland, M. Rice and S. Shenoi, "The Anatomy of a Cyber Power", *International Journal of Critical Infrastructure Protection*, March 2014, available at: www.sciencedirect.com.

2. M. Pollman, "Japan's Achilles Heel: Cybersecurity", *The Diplomat*, April 13, 2016, available at: http://thediplomat.com.

3. J. Andrew Lewis, "U.S.-Japan Cooperation in Cybersecurity", *Center for Strategic and International Studies*, November 2015, available at: https://csis-prod.s3.amazonaws.com.

Readiness Index (NRI).[4] On the Cyber Readiness Index 2.0, compiled by the Potomac Institute for Policy Studies and based on the evaluation of seven "essential elements" of countries' cybersecurity-related efforts and capabilities (national strategy, incident response, e-crime and law enforcement, information-sharing, investment in R&D, diplomacy and trade, and defense and crisis response), Japan offers "insufficient evidence" in two categories, and is labeled "partially operational" in four. In no category did the country obtain the highest score of "fully operational".[5]

Japan's "reluctance" to develop nationwide cybercapabilities is juxtaposed with a rising number of sophisticated cyberattacks against Japanese critical information infrastructure, including government networks, since the early 2000s. The 2016 Deloitte Asia-Pacific Defense Outlook report notes that Japan – along with Australia, New Zealand, Singapore and South Korea – is nine times more vulnerable to cyberattacks than other Asian economies.[6] Indeed, Japan has no cybersecurity company with global presence. The *annus horribilis* that laid bare Japan's insufficient cyberdefenses was 2011, with a number of advanced persistent threat (APT) attacks against Japanese military contractors (IHI Corporation and Kawasaki Heavy Industries, among others) and the successful theft of design and production plans of some of Japan's most advanced military hardware.[7] Another watershed event occurred in May 2015 when the Japan Pension Service was successfully hacked, exposing the personal data of more than 1.25 million people. Sophisticated APT attacks against Japanese networks appear to be the new normal.

It's not just the quality but also the quantity of cyberattacks that has been on the rise. According to the National Institute of Information and Communications Technology (NICT), Japan experienced over 25 billion cyberattacks in 2014 alone; 40 percent of them were traced back to China, followed by South Korea, Russia and the United States.[8] In 2005, just 310 million similar attempts had been recorded.

4. International Telecommunications Union, *ITC Development Index*, 2016, available at: www.itu.int; World Economic Forum, Network Readiness Index-Japan Country Profile, 2016, available at: www3.weforum.org.

5. C. Demchak *et al.*, "Japan Cyber Readiness at a Glance", *Potomac Institute for Policy Studies*, September 2016, available at: www.potomacinstitute.org.

6. Deloitte, *Asia-Pacific Defense Outlook 2016-Defense in Four Domains*, February 24, 2016, available at: www2.deloitte.com.

7. For a good overview of cyberattacks on Japanese critical information infrastructure see P. Kallender and C. W. Hughes, "Japan's Emerging Trajectory as a Cyber Power: From Securitization to Militarization of Cyberspace", *Journal of Strategic Studies*, September 26, 2016 available at: www.tandfonline.com.

8. F.-S. Gady, "Japan Hit by Cyberattacks at an Unprecedented Level", *The Diplomat*, February 20, 2015, available at: http://thediplomat.com.

Despite Japan's initial slow uptake of the security challenges emerging from cyberspace, this paper posits that cybersecurity under the administration of Japanese Prime Minister Shinzo Abe has moved to the core of the country's national security policy.[9] The 2020 Olympic Games are a major catalyst for this. Senior Japanese officials are actively advocating within the government to continue implementing reforms and institutionalize better cybersecurity beyond the games. This push is slowly gaining momentum. And while Japan remains a reluctant cyberpower, with a decidedly defensive outlook and a particularly change-resistant bureaucracy that is plagued by *tatewari-gyoseibi* ("vertical compartmentalization"), recent initiatives and policies have made it clear that the country is moving in the direction of potentially becoming one of Asia's more advanced cyberpowers in the not-too-distant future.[10]

This paper first outlines an analytical framework that is used to evaluate Japan's current standing and progress as a cyberpower. The following three sections discuss in detail the evolutionary stages in the development of Japan's national cybersecurity strategy. The last section deals with the Japan Self-Defense Forces' changing role in cyberspace and how they are slowly embracing a more militarized response to state-sponsored cyberthreats.

9. See details in Japan's National Security Strategy: Ministry of Foreign Affairs, *National Security Strategy*, April 6, 2016, available at: www.mofa.go.jp.

10. According to the prime minister's advisor on cybersecurity, William H. Saito, in order to implement Japan's new growth strategy, called "Society 5.0", ICT technology is a fundamental requirement that also must be secure by design. "There is no economic growth under the fourth industrial revolution without cybersecurity", he said. As a result, the government's next growth strategy will also emphasize ICT security, according to Saito. Interview with William H. Saito, Special Advisor on Cybersecurity to the Prime Minister, Government of Japan, January 27, 2017.

Framework for Assessing Cyberpower[11]

Discussing the evolution of Japan as a cyberpower, this paper will draw on a useful framework first presented in the "NATO Framework Manual" outlining three distinct evolutionary stages in the development of national cybersecurity strategies: whole of government (WoG), whole of nation (WoN) and whole of system (WoS).

A WoG approach attempts to integrate the collaborative efforts of government agencies through an interagency process to achieve unity of effort, while simultaneously maximizing available resources for planning, programming and budgeting a government's cybersecurity strategy. This is often done through a central coordination body within the operational and/or policy levels of government, as the "NATO Framework Manual" points out. The next evolutionary stage in the development of national cybersecurity strategies, the WoN approach casts a wider net than WoG, and aims to integrate efforts not just within the public sector but also non-state actors including "utilities, academia, ICT companies, and even private individuals". In the specific case of cybersecurity, WoN examples are strong private-public partnerships for protecting critical (information) infrastructure and agreeing on basic risk-management standards, common risk-analysis frameworks, operational information exchange, and common operational cyberdefense structures. "Overall, it is possible to differentiate three different levels of cooperation: the defense, security, and critical infrastructure level; the commercial cyber security level, and the civil society level," according to the "NATO Framework Manual".

The WoS approach complements the WoG and WoN approaches and is the last evolutionary stage, emphasizing that countries must give special attention to the international environment – the international system – when establishing national cybersecurity strategies. Under WoS, special attention is given to interacting with like-minded countries, Internet governance stakeholders, and industry/scientific/technical working groups. Countries try to collaborate with allies and institutions such as the International Telecommunication Union (ITU), the Internet Corporation for Assigned Names and Numbers (ICANN), and the Institute of Electrical

11. This section draws on A. Klimburg (Ed.), *National Cyber Security Framework Manual*, NATO CCD COE Publication, 2012, available at: https://ccdcoe.org.

and Electronics Engineers (IEEE). While cyberdiplomacy plays a large role within the WoS approach, it goes beyond the activities of foreign ministries. Logically speaking, a government can pursue all three simultaneously, but the authors of the terms appear to see them as evolutionary stages of development: first, only government and not the nation; second, only the nation (and government) and not the international system; and last the government, nation, and the international system in an integrated whole. The model does not address or exclude the possibility that a country, including Japan, would begin to develop capabilities at any stage of the spectrum of national cyberdefense readiness whether at the government, national or international level.

Applying this framework to Japan, three things become apparent. First, Japan is still struggling towards structuring its cyberpower around a WoG approach, although recent legislation (the Basic Act on Cybersecurity of November 2014 and the Act on the Protection of Specially Designated Secrets of December 2013) and structural reforms (the establishment and empowerment of the Cybersecurity Strategy Headquarters and National Center of Incident Readiness and Strategy for Cybersecurity in 2014) have been major stepping stones toward achieving more unity of effort within the government.

Second, while elements of a WoN approach exist, it is still in its infancy, particularly in the field of critical infrastructure protection. Private-public cybersecurity partnerships between Japan's large corporations and the government in a range of fields – including cyberthreat information-sharing (with the financial sector being the notable exception) and cybersecurity human resources training, among others – are also still underdeveloped. Much more needs to be done overall in WoN capacity-building.

Third, Japan from the start has emphasized a WoS approach and since 2013 has been consistently engaging with allies and partner nations, international organizations and institutions on both the technical (e.g., ASEAN Computer Emergency Readiness Team collaboration) and policy level (e.g., UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security). Japan's international engagement appeared to be ahead of its domestic efforts in 2016. Yet, up until September 2013, when it was announced that Tokyo would be the host of the 2020 Summer Olympics and Paralympics (expediently used by the Japanese government of Shinzo Abe as a rallying cry for improving the country's cybersecurity capabilities), Japan's approach was less developed, piecemeal and not proactive.

Whole-of-Government Approach: Institutions and Strategies

The 2006 strategy on information security: cybersecurity as a technical issue

In February 2006, Japan released its "First National Strategy on Information Security" under the auspices of the Information Security Policy Council (ISPC), set up in May 2005 as part of the Cabinet Secretariat's Strategic Headquarters for the Promotion of an Advanced Information and Telecommunications Network Society, and chaired by Japan's prime minister. The strategy set out to formulate a "systematic plan on information security based on a strategic vision regarding this issue" for the next three years.[12]

The National Information Security Center (NISC), created in April 2005 within the Cabinet Secretariat, was tasked with coordinating the government-wide implementation of the country's first information security strategy and to bolster security measures to guarantee the continuous development of Japan as a "major economic power".[13]

While the strategy, built upon Japan's Information Technology (IT) Basic Law in 2000, noted that "in order to ensure national security, it is necessary to give sufficient consideration to IT-related threats in light of the expansion of use and utilization of IT in these areas", the document largely focused on cybercrime and terrorism, not discussing advanced persistent threats (APTs) posed by nation states or nation-state-supported non-state actors.[14]

Overall, the 2006 strategy was weak in promoting a WoG approach, although it specifically noted "bureaucratic factionalism" as a problem. Its

12. Information Security Policy Council, *The First National Strategy on Information Security: Toward the Realization of a Trustworthy Society*, February 2, 2006, available at: www.nisc.go.jp.
13. *Ibid*. The NISC was established in 2000 as the Information Security Measures Promotion Office.
14. *Ibid*. For a summary of the 2000 IT Law, see: *Basic Law on Formation of an Advanced Information and Telecommunications Network Society*, November 29, 2000, available at: http://japan.kantei.go.jp.

main objective was merely to "give awareness" to all government entities concerned.[15] The NISC was tasked with creating partnerships with the private sector to exchange best practices; the document also outlined Japan's first international engagement strategy on information security with partner nations.

However, national security in the context of information security was only vaguely defined; the primary and foremost emphasis of the document lay on underlining the impact of IT on Japanese society and on the country's future economic development. The NISC in its 2005 form illustrated a "lack of flexibility in prioritization of a cybersecurity agenda". Cybersecurity was not "considered a top priority political issue, like the national pension program or a serious earthquake damage recovery program".[16] Cybersecurity was treated as, first and foremost, a technical issue.

As a result, the coordination and implementation of joint information security policies and responses to cyberthreats between the four key agencies dealing with cybersecurity within the Japanese government – the National Police Agency (NPA), Ministry of Internal Affairs and Communications (MIAC), Ministry of Economy, Trade and Industry (METI) and Japan's Ministry of Defense (JMOD) – was piecemeal and sectionalized, with each ministry essentially pursuing its own independent strategy to combat threats emerging from cyberspace. It decidedly failed to establish the "Japan Model" as a paragon of "high quality, high reliability, safety/security" to be emulated by other nations, as originally envisioned by the Japanese government.[17]

The 2009 strategy: a step toward a more comprehensive approach

The 2009 "Second National Strategy on Information Security", built on the previous document, focused on four subjects – central and local governments, critical infrastructure, business entities, and individuals – primarily seeking "to prevent significant influences of IT failures on the people's daily lives and socioeconomic activities", and emphasizing the

15. Information Security Policy Council, *The Second National Strategy on Information Security, Aiming for Strong 'Individual' and 'Society' in IT Age*, February 3, 2009, available at: http://www.nisc.go.jp.
16. Y. Yamada, A. Yamagishi and B. T. Katsumi, "A Comparative Study of the Information Security Policies of Japan and the United States", *Journal of National Security Law & Policy*, November 21, 2008. Available at: http://jnslp.com.
17. Information Security Policy Council, *op.cit*.

digital economy while focusing very little on the national security implications of cyberthreats. Nevertheless, the new strategy contained a more outlined approach toward forging international information security partnerships and, while focusing on cybercrime and terrorism, for the first time also discussed the threat of APTs due to a number of high-profile cyberattacks around the world at the time.

The 2009 three-year strategic plan sought to enhance the role of the NISC, which in the document was tasked with collecting "the best intelligence both at home and abroad" on information security, and maintained its role as the overall coordinator of the government's wide cyberpolicies. In 2009 the Japanese executive also divided its cybersecurity structure formally into three main supervisory bodies: the Crisis Management Center (which also deals with a range of other emergency response situations), the Cabinet Intelligence Research Office, and the NISC.[18] Furthermore, Japanese political leaders began for the first time to assert political control over cybersecurity policies: "The Prime Minister assumed the role of Director-General of the IT Strategic Headquarters [established within the Prime Minister's Cabinet in 2001 to create an advanced information and telecommunications network society], and the roles of Deputy Director-General were taken by the Chief Cabinet Secretary, Minister of State for Science and Technology Policy, Minister for Internal Affairs, METI minister, and 10 other ministers of state. The Chief Cabinet Secretary became the chair of the ISPC, with the Minister of State for Science and Technology Policy as deputy. Ministers from the NPA, MIC, METI, and JMOD sat as IPSC members."[19]

The ISPC now included six private-sector representatives, following another push for deeper public-private cybersecurity partnerships.[20] In May 2010, the ISPC issued a new four-year strategy, influenced by large-scale (possibly state-sponsored) cyberattacks in 2009 against government, news media, and financial websites in South Korea and the United States, to ensure "national security and effective crisis management".[21] The strategy specifically called for the implementation of the "Secure Japan 2009" plan, an annually reviewed security plan to boost Japan's cyberdefense capabilities and to make it the most "advanced information security country" in the world. The document appears to lay out the

18. P. Kallender and C. W. Hughes, *"Japan's Emerging Trajectory as a Cyber Power", op.cit.*
19. *Ibid.*
20. R. Masuoka and T. Ishino, "Cyber Security in Japan", Center for International Public Policy Studies, December 2012, available at: www.cipps.org.
21. Information Security Policy Council, *Information Security Strategy for Protecting the Nation*, May 11, 2010, available at: www.nisc.go.jp.

distinct Japanese mindset of the time – seeing cyberattacks as analogous to unpredictable natural disasters rather than concrete actions of state and non-state adversaries.

However, subtle shifts of policy change can be found in the new strategy. For the first time, Japan advocated developing more active and across-government coordinated responses to large-scale cyberattacks. It also called for the "building up of international alliances". To facilitate more international cooperation, Japan amended cybercrime laws that enabled it to accede to the Budapest Convention on Cybercrime.[22] The treaty came into effect in November 2012. However, the document failed to break the "silo approach" of Japanese government entities when dealing with cyberattacks, and did not endow the NISC with extensive new powers.

From 2012, the formulation of a real cybersecurity strategy to counter concrete threats

Incremental changes followed a wave of four major cyberattacks between July and November 2011, targeting the Japanese Diet, a number of Japanese embassies abroad, and the Japanese defense contractor, Mitsubishi Heavy Industries. These cyberattacks laid bare the lack of authority of the NISC to coordinate a WoG response to cyberincidents.[23] As a result, a new IPSC document from July 2012, titled "Information Security 2012", outlined the need to establish closer private-public collaboration and strengthen response capabilities in government agencies. It also re-emphasized the central role of the Cabinet Secretariat and the NISC as the government's principal coordinator of responses to attacks from cyberspace.[24]

In addition, the document proposed voluntary attack drills for government ministries and agencies, and called for Japan to contribute to the development of "international behavioral norms in cyberspace".

In June 2013, the ISPC issued its first "Cybersecurity Strategy", using the "cyber" prefix rather than "information", as was the case in previous strategy documents, to illustrate a wider and more comprehensive

22. P. Kallender and C. W. Hughes, "Japan's Emerging Trajectory as a Cyber Power", *op.cit*.
23. One notable improvement in 2011 was the merging of Japan's Cyber Clean Center with the Telecom Information Sharing and Analysis Center Japan – set up by the Japan Computer Emergency Response Team Coordination Center, Internet service providers, and security vendors – to better combat botnets and other malware.
24. Information Security Policy Council, "Information Security 2012", July 4, 2012, available at: www.nisc.go.jp.

approach to dealing with cyberspace threats.[25] The new government policy outlined in the document was to establish a resilient "cybersecurity nation" as cyberattacks had become both "national security" and "crisis management" issues. This indicated an important shift in the perception of cyberthreats. Thus, for the first time, a large section outlined the role of the Ministry of Defense in defending cyberspace – particularly when it came to "national level cyberattacks for which the involvement of foreign governments is suspected". The strategy—likely influenced by US thinking on the subject – also referred to cyberspace as a new domain of warfare, and called for the systematic strengthening of the cyberdefense capabilities of the Japan Self-Defense Forces (JSDF), in part through the establishment of a new JSDF Cyber Defense unit. The document also discussed the need for a clear delineation of responsibilities between the JMOD and civilian ministries when it came to defending critical infrastructure and "other than defense-related systems" during "times of emergency" – a clear shift toward militarizing Japanese cyberdefense. The strategy also called for a strengthening of private-public partnerships, the establishment of a "confidentiality agreement-based information-sharing system", and the reinforcement of the Government Security Operation Coordination Team, the Computer Security Incident Response Team, and the Japan Computer Emergency Response Team Coordination Center.

The new cyberstrategy offered the most comprehensive outline yet of Japan's approach to cyberdiplomacy. Next to emphasizing the need for international alliances and continuous dialogues with like-minded countries, the document elaborated on Japan's efforts to shape international norms of behavior in cyberspace. It also stressed the importance of the US-Japan alliance in formulating these norms, and expressed Tokyo's support for a multi-stakeholder approach toward Internet governance. Under Japan's first cyberstrategy, the NISC, however, continued to lack legal authorization – leaving Japan's cybersecurity landscape as fragmented as ever.

Institutions and strategy in 2017

Following the passing of the December 2013 Act on the Protection of Specially Designated Secrets – designating as state secrets certain ssinformation,s including ICT technology relevant for national defense – and the November 2014 Basic Act on Cybersecurity – mandating the government to establish uniform cybersecurity standards for government

25. Information Security Policy Council, *Cybersecurity Strategy: Towards a World-Leading, Resilient and Vigorous Cyberspace*, June 10, 2013, available at: www.nisc.go.jp.

agencies, monitor the government information network system, and detect and analyze unauthorized intrusions and cyberattacks, among other things – a second iteration of Japan's "Cybersecurity Strategy", outlining the country's approach to cybersecurity for the next three years, was published and, for the first time, approved by the Japanese Cabinet in September 2015.[26]

While the new document highlighted the economic potentials of cyber-enabled technologies (e.g., "The Internet of Things"[27]), it mainly stressed the importance of a more comprehensive national cybersecurity strategy in the run-up to preparation for the 2020 Tokyo Olympics and Paralympic Games.[28] Cybersecurity, the document made clear, had been elevated to one of Japan's top national security concerns, and demanded a unified WoG approach.

Reflecting the principle of "Proactive Contribution to Peace" promoted by Shinzo Abe's administration, the document noted that, to ensure "a free, fair, and secure cyberspace", Japan should pursue more proactive policies in cyberspace.

The document also highlighted the increasingly greater role the JMOD was playing in defending Japan against large-scale and sophisticated cyberattacks, and the importance of the cooperation between the JSDF and the US military under the new Guidelines for Japan-US Defense Cooperation.

In detail, the 2015 cyberstrategy reiterated that, to ensure national security, "Japan will further advance the centralization of relevant information [...], and enhance its common external responses". This entailed "enhancing its capabilities of early identification and situational awareness", strengthening information-gathering (cyberintelligence) and information-sharing, including with foreign governments, and finally promoting "cross-sectoral and cross-cutting efforts comprehensively". The pivotal role of private-public partnerships in that respect was also once again underlined.

26. Government of Japan, *Cybersecurity Strategy*, September 4, 2015, available at: www.nisc.go.jp. Interestingly, the State Secrets Law was already being written in detail exactly when the Snowden revelations first started pouring out in the summer of 2013. The Snowden revelations helped frame the mood and bolstered the smooth passage of the law by the Japanese Diet on December 13.
27. It outlines the need for essential requirements to ensure users' safety, including safety standards. See: National Center of Incident Readiness and Strategy for Cybersecurity, *General Framework for Secure IoT Systems*, August 26, 2016, available at: www.nisc.go.jp.
28. Government of Japan, *op.cit*.

Moreover, the importance of international cooperation with like-minded countries featured heavily in the document. The 2015 strategy notably stressed the importance of confidence-building measures in cyberspace, the need to develop more comprehensive international rules and norms, including establishing international rules of law in cyberspace, and the importance of bilateral and multilateral diplomacy in devising global strategies to combat the rise of cybercrime and malicious cyberactivities.

What makes the 2015 cybersecurity strategy different from previous strategies are legal and structural changes in Japan's cybersecurity landscape that occurred in 2014.

Under the Basic Act on Cybersecurity, the IPSC was transformed into the Cyber Security Strategy Headquarters (CSSH), with the newly designated National Center of Incident Readiness and Strategy for Cybersecurity (NISC) acting as its secretariat, effective as of March 2016.[29] Both the CSSH and NISC's roles were legally formalized; they were given comprehensive powers to coordinate and implement the national cybersecurity strategy.[30] Under the new law, the CSSH, currently chaired by Chief Cabinet Secretary Yoshihide Suga, is "the command and control body of national cybersecurity" endowed with strong authority, "such as making recommendations to national administrative organs".[31] The NISC's main task is to "promote cybersecurity policies" laid out in the 2015 cybersecurity strategy, and it is supported in the task by the Government Security Operation Coordination Team. The CSSH is collaborating with the National Security Council (NSC) created in 2013, but they do not have a joint-meeting mechanism or other regular formal meetings to convene. The NSC will deal with a cybersecurity issue only if it is deemed an emergency and crisis management matter.[32] The CSSH retains a peacetime direction-setting function on Japan's cybersecurity policy, and is also responsible for

29. National Center of Incident Readiness and Strategy for Cybersecurity, 2015, *Organizational Structure*, available at: www.nisc.go.jp.

30. According to Paul Kallender: "The creation of the CSSH has to be seen in the context of attempts by activist politicians to assert Cabinet Office control over the sectionalism of the ministries, in particular to assert control over new strategic areas where the bureaucratic layer has proven itself to be demonstrably incapable of responding [...] The CSSH does not have budget authority but it does have the right to investigate and coordinate policy and implementation. The very powerful MIC for example maintains its budget and bailiwick and power, provided that it is seen to comply with the strategy." Interview with Paul Kallender, Global Security Research Institute, Keio University, Tokyo, January 27, 2017.

31. Government of Japan, *op.cit.*

32. Interview with Motohiro Tsuchiya, Professor, Graduate School of Media and Governance, Keio University, Tokyo, January 27, 2017.

producing an annual report reviewing the progress in policy implementation. So far two reports have been made publicly available.[33]

The 2015 strategy document lays out in detail the NISC's new responsibilities: "These include: the network-based vigilance and monitoring of malicious activities against information systems of administrative organs; fact-finding on the cause of incidents and audit of relevant governmental bodies; information gathering and analysis on domestic and foreign cybersecurity; the promotion of international cooperation and collaboration; and cybersecurity workforce development for and by the governmental bodies."[34] Furthermore, the NISC now also has the authority to monitor cybersecurity budgets within government agencies. Following the passing of the Basic Act on Cybersecurity, the NISC can investigate cyberattacks against government-linked administrative organizations such as the Japan Pension Service. Given the scope of the NISC's new responsibilities, an April 2016 amendment to the Basic Act on Cybersecurity allowed the former to delegate a part of its operations to the Information Technology Promotion Agency, which advises Japan's private sector on cybersecurity, and operates the Cyber Security Information Sharing Partnership of Japan, facilitating information-sharing between government and the private sector.[35]

The Cyber Security Strategic Headquarters, led by the Chief Cabinet Secretary, with the Minister of State for Science and Technology Policy acting as deputy chairman, also includes the ministers of foreign affairs, of defense, of economy, trade & industry, and of internal affairs, and the National Public Safety Commission chairman.[36] The four key cyber ministries remain the NPA, MIAC, METI, and JMOD.

33. National Center of Incident Readiness and Strategy for Cybersecurity, *Major Publications*, available at: www.nisc.go.jp. The reports focus on the continued need for: capacity-building at home and abroad, the promotion of cyber best practices in the public and private sectors, more cyberexercises, better information-sharing, and cryptographic standards. The reports decidedly leave the impression of work in progress on almost all cyber fronts in Japan.
34. *Ibid*.
35. S. Umeda, "Japan: Cyber Security Basic Act & Information Processing Promotion Act Amended", *Library of Congress Global Legal Monitor*, June 15, 2016, available at: www.loc.gov.
36. For details of responsibilities and overall placement within the national security structure of Japan, see: Government of Japan, *The Basic Act on Cybersecurity*, November 12, 2014.

The Whole-of-Nation Approach and Private-Public Partnerships

The successful implementation of a WoN approach for cybersecurity largely depends on robust private-public partnerships to maximize a country's cyberdefenses. This requires adequate cyberthreat information-sharing systems in place and a strong commitment by government and companies to work with one another. However, information-sharing remains a touchy subject in Japan. According to a PwC (PricewaterhouseCoopers) study, Japanese businesses are less willing to share cyberthreat data than other companies in Europe and the United States—30.4 versus 64.7 percent.[37] According to the same survey, 39 percent of companies lack an adequate information-sharing framework. This is partially due to an inadequately trained workforce:

"According to a 2015 METI study, Japanese companies lack IT and cybersecurity professionals who can judge which threat intelligence should be shared, when, and with whom, largely because Japanese companies tend to outsource cybersecurity-related work to system integrators."[38]

Japan is indeed facing a shortage of up to 90,000 trained cybersecurity experts. According to the government, Japan needs a workforce of 350,000 to assure adequate network protection. At the moment that number stands at 265,000, but 160,000 of those are insufficiently trained.[39] Cultural factors such as the fear of losing face might also play a role in Japanese businessmen's unwillingness to share data of cyberbreaches.

Japan's critical infrastructure protection efforts are guided by the third edition of "Basic Policy of Critical Information Infrastructure

37. PwC, *Global State of Information Security Survey 2016*, February 2016, available at: www.pwc.com.

38. M. Matsubara and D. Kriz, "Putting the METI Cyberthreat Information Sharing Recommendation into Action in Japan", *PaloAlto Networks Blog*, July 25, 2016, available at: http://researchcenter.paloaltonetworks.com.

39. R. Smart, "Japan Gets Serious about Cybersecurity as Olympics Approach," *The Journal for the American Chamber of Commerce in Japan*, February 4, 2016, available at: www.japantoday.com.

Protection" in conjunction with the 2015 cybersecurity strategy.[40] In December 2015, METI also released non-legally binding "Cybersecurity Guidelines for Business Leadership Vision 1.0" to help Japanese companies to improve their cybersecurity performance.[41] According to the document, business leaders should "actively participate in and contribute to cyberthreat information-sharing activities". This initiative followed an alarming report published by PwC that only 27 percent of Japanese business executives were properly implementing cybersecurity measures, in comparison to a global average of 59 percent.[42] Within METI, the Information Technology Promotion Agency advises Japan's private sector on cybersecurity and runs the Cyber Security Information Sharing Partnership of Japan, which facilitates information data sharing. METI also is in the process of setting up a Cybersecurity Promotion Agency as an additional way to train and interact with the private sector in order to step up efforts to protect Japan's critical infrastructure, including the electrical power, gas and oil industries, and nuclear-power facilities.[43] However, the center is to be allocated a budget of just Yen 2.5 billion, and it will not cover other infrastructure sectors such as communications, finance and transport.[44]

Nevertheless, the government's efforts have had some impact. Cybersecurity is gaining increasing traction among the Japanese business community now that the government has outlined (through the documents cited above) its baseline expectations of the private sector in the matter.[45] Notably in 2015, the Japanese Business Federation formed a "Cybersecurity Working Group" consisting of representatives of over 30 of Japan's largest companies, and produced actionable recommendations to improve cybersecurity practices in the private sector, thus underlining the growing appreciation of the need for better cybersecurity in the private

40. National Center of Incident Readiness and Strategy for Cybersecurity, "Basic Policy of Critical Information Infrastructure Protection", May, 2014.
41. METI, *Cybersecurity Guidelines for Business Leadership Vision 1.0*, December 28, 2015, available at: www.meti.go.jp.
42. M. Matsubara and D. Kriz, "Putting the METI Cyberthreat Information Sharing Recommendation into Action in Japan", *op.cit*.
43. M. Santillan, "Japan to Form New Cybersecurity Agency to Protect its Critical Infrastructure", *Tripwire*, May 20, 2016, available at: www.tripwire.com.
44. "Japan's Weak Cyberdefense", *The Japan Times,* December 26, 2016.
45. In September 2015, the Japanese government also revised the Personal Information Protection Act, requiring all companies to adopt cybersecurity standards to protect and prevent breaches of personal information. Cf. M. Matsubara and D. Kriz, "Putting the METI Cyberthreat Information Sharing Recommendation into Action in Japan", *op.cit*.

sector.[46] A second set of recommendations was published in January 2016. The results are showing. The financial sector is generally regarded to have put in place cybersecurity standards and network protection on a par with institutions in Europe and the United States. In October 2016, the G7 also agreed to non-binding cybersecurity guidelines for their respective financial sectors.[47] However, this short overview illustrates that all of this is only a starting point. Japan will not be able to move on to an overall WoN approach in its national cybersecurity strategy without stronger private-public partnerships.

46. Recommendations included strengthening public-private information-sharing systems, holding cybersecurity training exercises, and building international partnerships. Keidanren, *Policy & Action*, February 17, 2015, available at: www.keidanren.or.jp.
47. Kyodo News Agency, "G-7 Adopts Financial-Sector Cybersecurity Guidelines", October 12, 2016.

The Whole-of-System Approach and Japan's Cyber Diplomacy

As the review of Japan's past cybersecurity strategies makes clear, international engagement with a range of international partners and institutions has been crucial for Japan from the outset. Next to Japan's four key cyber ministries, the Ministry of Foreign Affairs (MOFA) has increasingly been playing a larger role in the cyber field. For example, in July 2016 the MOFA established a new office, the Cyber Security Policy Division, composed of 15 ministry officials, to deepen Japan's international engagement on the subject.[48] The MOFA's "Diplomatic Bluebook" also lists cybersecurity as one of the primary foci of Japan's foreign policy.[49]

When it comes to cyberdiplomacy, Japan in essence is pursuing a norm-based approach with like-minded countries that share the basic values of "democracy, respect for human rights and the rule of law", as outlined in the 2013 "Cybersecurity Strategy" and reiterated in the 2015 edition, with Europe and the United States as the key partners in that effort.[50]

Japan's international engagement on cybersecurity is wide in scope and range and, according to the evolutionary WoG, WoN and WoS approaches, uncharacteristic of a country still struggling with implementing the former two. One explanation for this is the expeditious use of the upcoming 2020 Olympic and Paralympic Games in Japan by the Abe administration to place cybersecurity at the core of Japan's national security strategy. The international sports event is being used as a rallying point to convince the government and the private sector of the necessity to forge closer international cooperation and collaboration on cybersecurity-related issues.

48. Ministry of Foreign Affairs of Japan, "Establishment of Cyber Security Policy Division, Foreign Policy Bureau", July 12, 2016, available at: www.mofa.go.jp.
49. Japanese Ministry of Foreign Affairs, "Diplomatic Bluebook", 2015, available at: www.mofa.go.jp.
50. Information Security Policy Council, June 10, 2013, *op.cit.*

It was also around the time of the announcement that Japan would host the Games that Tokyo's more systematic engagement with other countries began. Beginning in 2014, Japan and the United Kingdom have met a number of times to discuss possible cybersecurity threats based on the UK's experience of hosting the Games back in 2012. In 2014, Japan and France also held a cyber dialogue in Paris to discuss critical infrastructure protection, the establishment of international norms, and joint efforts toward cybersecurity capacity-building.[51] This was followed by Japan-Estonia and Japan-Israel cyber dialogues with similar agendas. In Asia, Japan notably is pursuing cyber dialogues with a number of countries including Australia, India and South Korea. The most important partner for Japan remains the United States, with a number of fora such as the Japan-US Cyber Dialogue, the Japan-US Policy Cooperation Dialogue on the Internet Economy, and the Japan-US Defense Policy Working Group.[52] The Japanese government also hosted an international cybersecurity conference, the Cyber3 Conference Okinawa 2015, which was supported by the World Economic Forum (WEF), in November 2015.[53] However, no follow-up event has been held.

Japan is also involved in international cyber capacity-building, particularly in ASEAN countries, and has been establishing working partnership on critical infrastructure protection and rapid-incident response. For example, in January 2016, India, Malaysia, Singapore and Japan signed an agreement on CERT cooperation.[54] Japan is also cooperating with China and South Korea at the CERT level. Representatives from the three countries meet annually, share information including threat data, have established a 24/7 technical hotline, and purportedly have a protocol for crisis escalation in place in the event of major cyberattacks.[55] Japan participates in similar meetings with the Asia-Pacific Computer Emergency Response Team (APCERT) next to a number of other critical infrastructure-protection and rapid-incident response international entities such as International Watch and Warning Network.

51. F.-S. Gady, "Japan and Europe Step Up Cooperation in Cyberspace", *The Diplomat*, January 13, 2016, available at: http://thediplomat.com.
52. C. Demchak *et al.*, "Japan Cyber Readiness at a Glance", *op.cit*.
53. Cyber3 Conference Okinawa 2015, Conference website, available at: http://spfusa.org.
54. Press Trust of India, "India, Malaysia, Singapore, and Japan Sign Pacts for Cybersecurity", January 27, 2016, available at: www.ndtv.com.
55. F.-S. Gady, "Can the US and China Cooperate on the First (and Last) Line of Cyber Defense?", *The Diplomat*, October 30, 2015, available at: http://thediplomat.com.

On top of the agenda for Japan is to reach a consensus with like-minded countries about responsible state behavior in cyberspace. In November 2015, the G20 countries agreed that international law, including the United Nations Charter, applies to the behavior of nations in cyberspace. A UN Group of Government Experts came to the same non-binding resolution in 2013, which was reaffirmed again during the G7 summit in Japan in May 2016. Furthermore, with the support of Japan, the UN Group of Government Experts laid out a set of norms and confidence-building measures (CBM) in 2015. Japan has also been pushing for CBM (and the multi-stakeholder model) in several regional and international fora.

Japan's cyberdiplomacy is one of the most important and developed elements of its cybersecurity strategy. Given that a WoS approach mandates going beyond the activities of the relevant foreign ministries, Japan's multipronged international approach toward cybersecurity is holding up well when compared to the activities of other similar countries (e.g., Germany). However, it cannot be denied that Japan's sophisticated international engagement is uncharacteristic of a country with relatively weakly developed WoG and WoN approaches.

Japan's Slow Militarization of Cyberspace and Military Alliances

Japan's least developed aspect in its national cybersecurity posture remains in the military domain. This is primarily due to a lack of adequate resources and a reluctance to move beyond a purely defensive mindset in cyberspace. Since at least 2006, the United States has increased pressure to improve cyberdefenses because of the need to secure information assurance for ballistic missile defense systems and related US technology transfers. However, the JMOD did not create its first (90-member) Cyber Defense Unit (CDU) until 2014, and overall the JSDF is estimated to field only a few hundred soldiers tasked with protecting military networks and infrastructure.[56] Military cyber intelligence-gathering also remains a problem for the JMOD and the Japanese government overall.[57] Furthermore, one can deduce from past statements by Prime Minister Abe that the reinterpretation of article 9 of Japan's pacifist constitution (the 2015 "Legislation for Peace and Security"), outlining under what circumstances Japan can come to the aid of allies abroad, does not apply to cyberspace and is confined to JSDF logistical support of allies since the use of force beyond self-defense remains unconstitutional.[58]

According to Deloitte's 2016 Asia-Pacific Defense Outlook, Japan in the military realm, given the traditional close integration and supervision of JSDF with the civil government, is pursuing a WoG approach.[59] However, by placing a premium on the US-Japan alliance to increase its cyberwarfare capabilities, with Washington providing a cybersecurity umbrella a guarantee by a major cyberwarfare power to defend a less capable ally – Japan's approach has also been influenced by WoN and WoS

56. The CDU does not defend critical infrastructure or defense industry networks. J Andrew Lewis, *op.cit*.
57. Y. Nitta, "Cyber Intelligence: The Challenge for Japan", *Georgetown Journal of International Affairs*, March 17, 2015, available at: http://journal.georgetown.edu; M. Matsuzaki, "The Cybersecurity Challenges for the Ministry of Defense and Self-Defense Forces", *IIPS Quarterly*, July 2015, available at: www.iips.org.
58. F.-S. Gady, "Why China Should Not Worry about Japan's New Security Laws", *The Diplomat*, March 31, 2016, available at: http://thediplomat.com.
59. Deloitte, *op.cit*.

elements.[60] Yet, these approaches remain underdeveloped. For example, the 2015 Guidelines for US-Japan Defense Cooperation do not specifically include cyberwar and cybersecurity in the lifting of the self-imposed ban on collective self-defense, which allows Japan to defend allies, even when the country is not under attack itself.[61] Indeed, cyberattacks remain classified as "crimes" and not as "armed attacks" under Japanese law, even when military forces of another state are involved.[62] This is despite the fact that cybersecurity was designated as an alliance "common strategic objective" in June 2011 following a Security Consultative Committee (SCC) "Two-Plus-Two" meeting.

Nevertheless, as the discussion of Japan's cybersecurity strategies in the previous sections have shown, Japan is slowly embracing a more militarized response to state-sponsored threats from cyberspace. Paul Kallender and Christopher W. Hughes, in the most thorough recent examination of the subject, note Japan's gradual move from securitization to militarization of cyberspace. [63] The 2016 Defense of Japan White Paper specifically notes that the JSDF aim to "strengthen capability to collect intelligence regarding cyberattacks" and to increase the number of analysts in the CDU.[64] Also, the Guidelines for US-Japan Defense Cooperation include an entire section dedicated to cyberspace, illustrating how central cybersecurity will be for the US-Japan in the future. A part reads: "The Self-Defense Forces and the United States Armed Forces will:

- maintain a posture to monitor their respective networks and systems;
- share expertise and conduct educational exchanges in cybersecurity;
- ensure resiliency of their respective networks and systems to achieve mission assurance;
- contribute to whole-of-government efforts to improve cybersecurity;
- and conduct bilateral exercises to ensure effective cooperation for cybersecurity in all situations from peacetime to contingencies."[65]

60. T. Kelley, "U.S. to Bring Japan under its Cyber Defense Umbrella", *Reuters*, May 30, 2015.
61. Ministry of Defense, *The Japan-U.S. Defense Guidelines*, April 27, 2015, available at: www.mod.go.jp. For details on the new laws, see: F.-S. Gady, "Why China Should Not Worry about Japan's New Security Laws", *op.cit*.
62. "Japan's Weak Cyberdefense", *The Japan Times*, December 26, 2016, available at: www.japantimes.co.jp.
63. P. Kallender and C. W. Hughes, "Japan's Emerging Trajectory as a Cyber Power", *op.cit*.
64. Ministry of Defense, *Defense of Japan 2016 White Paper*, August 2, 2016, available at: www.mod.go.jp.
65. *Ibid*.

That section is the most comprehensive public statement by the JMOD on its cyberwarfare doctrine to date. However, the application of Article V of the US-Japan Treaty of Mutual Cooperation and Security, outlining US defense commitments in the event of an attack on Japan, does not offer concrete guidelines on whether a cyberattack or cyber-enabled attacks constitute a *casus foederis*. According to James Lewis, to solidify their alliance in cyberspace Japan and the United States need to make progress in six areas:

- "Assigning adequate resources to cybersecurity, particularly for Japan;
- Agreeing on how collective defense in cyberspace is defined and implemented, including clear guidance on Article V thresholds and a joint public statement on cyber activities that could trigger the mutual self-defense commitment;
- Creating bilateral mechanisms for cooperation and for sharing information on cyber threats and the techniques used to mitigate them;
- Developing robust, realistic joint training and exercises;
- Expanding national and joint efforts for civilian critical infrastructure protection and counterespionage;
- Coordinating efforts to create a framework for cybersecurity discussions and CBMs [confidence-building measures] in Northeast Asia."[66]

Japan would also do well to deepen its partnerships with like-minded countries in the region such as Australia and Singapore. It could, for example profit greatly from a reinforced Japan/Singapore/US/Australia cybersecurity nexus at the defense ministry level. Singapore, in particular, could be a good example for Japan to emulate since it is the most advanced Asian country in cybersecurity. It has a cyber component in its smart-nation strategy, and its military has devoted substantial thought and resources to developing comprehensive WoG, WoN and WoS approaches to cybersecurity in a way that no other country in Asia has.[67] Deeper Japan-Singapore ties could perhaps influence Tokyo to jointly develop offensive cybercapabilities in the face of growing Chinese and North Korean

66. James Andrew Lewis, November 2015, *op.cit.*

67. M. Raska, "Cyber Conflicts and Singapore's 'Total Defence' Strategy", *RSIS Commentary*, June, 2016, available at: www.rsis.edu.sg; H. Hung, "Confronting Cybersecurity Challenges through US-Singapore Partnership", *RSIS Commentary*, August, 2016, available at: https://dr.ntu.edu.sg; Cyber Security Agency of Singapore, 2016, *Cyber Security Associates and Technologists (CSAT) Programme*, available at: www.csa.gov.sg; Lee Hsiang Wei, "The Challenges of Cyber Deterrence", *Journal* of the Singapore Armed Forces, April 16, 2015, available at: www.mindef.gov.sg.

capabilities in this field. As James Lewis notes: "A force without cyber capabilities is increasingly outdated and more dangerous to itself than its opponents."[68] However, political and legal limitations to Japanese offensive military capabilities make this unlikely, and the military component of cybersecurity will remain the weakest part of Japan's overall national cybersecurity posture for the foreseeable future. This is corroborated by Motohiro Tsuchiya, one of Japan's leading cybersecurity scholars, who says that the Japanese military is "still cautious" in its cyberspace operations and primarily concerned with defending its own systems and networks, not the private sector.[69]

68. J. Andrew Lewis, "U.S.-Japan Cooperation in Cybersecurity", *op.cit.*
69. Interview with Motohiro Tsuchiya, Professor, Graduate School of Media and Governance, Keio University, Tokyo, January 27, 2017.

Conclusion

Japan remains a reluctant cyberpower but over the last two years has laid the structural and legal foundations for becoming a serious player in cyberspace. With the creation of the CSSH and NISC and the passing of the Cybersecurity Basic Act in conjunction with a new cybersecurity strategy, Japan has the proper framework in place to increase its overall national cybersecurity capabilities. Whether it will succeed in becoming a leading cyberpower will, however, to a large degree depend on adequate funding and political will. Japan's military capabilities in cyberspace remain in their infancy. The Abe administration has been careful not to abandon the JSDF's defensive posture in cyberspace, and has not indicated that it will develop offensive cyberwar capabilities.[70] This, however, may change should the new US administration abandon the United States' historic solid defense commitment to Japan.There is reason to believe that President Donald Trump may loosen cyber alliances, including US-Japanese cooperation, abandon the quest for norms of state behavior in cyberspace, and trigger an offensive cyber arms race. These developments could force Japan's hand. I noted in a separate analysis: "At present, United States' allies can no longer take for granted that they will be shielded under the U.S. 'cyber umbrella', i.e. U.S. support in defending their networks paired with the threat of retaliatory U.S. cyber strikes."[71] In that respect, Japan's deepening of engagement with like-minded countries in the region such as Australia and Singapore will assume even greater importance over the next few years. From a structural perspective, Japan is still struggling toward organizing its cyberpower around a WoG approach, and also faces substantial challenges in fully implementing the WoN and WoS approaches.

70. According to Hiroshi Ito, offensive cyberweapons remain unconstitutional, although he sees cyberweapons that are not directly responsible for the death of people as "good and suitable" for Japan. Interview with Hiroshi Ito, Deputy Director-General for Cybersecurity and Information Technology at the Ministry of Economy, Trade and Industry, February 2, 2017.

71. F.-S. Gady, "Trump and Offensive Cyber War", *China US Focus*, January 10, 2017, available at: www.chinausfocus.com.