Routledge
Taylor & Francis Group

Journal of Strategic Studies

ISSN: 0140-2390 (Print) 1743-937X (Online) Journal homepage: http://www.tandfonline.com/loi/fjss20

Japan's Emerging Trajectory as a 'Cyber Power': From Securitization to Militarization of Cyberspace

Paul Kallender & Christopher W. Hughes

To cite this article: Paul Kallender & Christopher W. Hughes (2017) Japan's Emerging Trajectory as a 'Cyber Power': From Securitization to Militarization of Cyberspace, Journal of Strategic Studies, 40:1-2, 118-145, DOI: 10.1080/01402390.2016.1233493

To link to this article: http://dx.doi.org/10.1080/01402390.2016.1233493

THE JOURNAL OF STRATEGIC STUDIES, 2017
VOL. 40, NOS. 1–2, 118–145
http://dx.doi.org/10.1080/01402390.2016.1233493

Routledge
Taylor & Francis Group

Japan's Emerging Trajectory as a 'Cyber Power': From Securitization to Militarization of Cyberspace

Paul Kallender[a] and Christopher W. Hughes[b]

[a]Global Security Research Institutue, Keio Gijuku Daigaku, Minato-ku, Japan; [b]Department of Politics and International Studies, University of Warwick, Coventry, United Kingdom of Great Britain and Northern Ireland

ABSTRACT

Japan has been overlooked as a 'cyber power' but it now becoming a serious player in this new strategic domain. Japanese policy-makers have forged a consensus to move cybersecurity to the very core of national security policy, to create more centralized frameworks for cybersecurity, and for Japan's military institutions to build dynamic cyberdefense capabilities. Japan's stance has moved rapidly toward the securitization and now militarization of responses to cyber challenges. Japan's cybersecurity stance has bolstered US–Japan alliance responses to securing all dimensions of the 'global commons' and extended its defense perimeter to further deter but potentially raise tensions with China.

KEYWORDS Japan; cybersecurity; China; US–Japan alliance; securitization

Amongst the multifarious potential sources of instability in the Asia-Pacific, cybersecurity is emerging as one of the most prominent and challenging of security agendas – forming an added source of contention in the United States' relations with China and North Korea; obliging the United States to strengthen its cyberdefense and other military capabilities in response; and endangering access to yet another aspect of the 'global commons' for all states of the region, and for their citizens and commerce. On top of uncertainty over the impact of cybersecurity and its relationship to the Asia-Pacific security environment, questions are inevitably raised over the reaction of Japan to these developments, given its increasingly testy security ties with North Korea but especially China, its position as a central US diplomatic and military ally in the region, and need as an economic and technological great power to safeguard the global commons for its own commercial interests. Japan's response to cybersecurity concerns to date, though, and in line with many appraisals of the evolution of its security trajectory in general, has been viewed as more tentative, highly circumscribed, and lacking in

CONTACT Christopher Hughes c.w.hughes@warwick.ac.uk

strategic intent. Japan is not seen as a 'cyber power,' much in the same way that it is often seen to still eschew behaving as and building the capabilities of a 'normal' or even great military power.[1]

The objective of this article, however, is to argue that it is vital to start to look again at Japan's stance on cybersecurity, just as there has been a pressing need and recent attempts to revise our understanding of the remilitarization of its security policy and the significance of this for the regional security system. Japan's development as a key player across all dimensions of security matters: its choices influence the stability of its relations with China and other regional states. Japan's growing power in the cyber domain undergirds the US–Japan alliance and much of the ability of the United States to respond to cyber and all forms of security threats, and thus more broadly Japan's actions are increasingly important to the strategic balance in the region. Yet, Japan's activities in cybersecurity have received minimal policy attention, especially in comparison with the reams of outputs devoted to the United States and China. Sustained scholarly work on Japan and cybersecurity in the field of the security studies, whether in English or Japanese, is highly limited in number and scope.[2]

Specifically, this article argues that Japan has initiated a trajectory of assuming the role of a nascent 'cyber power.' Now fully cognizant of the nature and security ramifications of potential cyber threats, at first steadily

[1]Subcommittee on Asia and the Pacific of the Committee on Foreign Affairs House of Representatives, *Asia: The Cyber Security Battleground* (Washington DC: Committee on Foreign Affairs House of Representatives 2013), <http://docs.house.gov/meetings/FA/FA05/20130723/101186/HHRG-113-FA05-20130723-SD002.pdf>. The literature on the extent and nature of change of Japanese security policy is very extensive. For a sample of influential views, arguing for essential continuity of Japanese security strategies, see Thomas U. Berger, *Cultures of Antimilitarism: National Security in Germany and Japan* (Baltimore MD: Johns Hopkins University Press 1998); Jennifer Lind, 'Pacifism or Passing the Buck? Testing Theories of Japanese Security Policy,' *International Security* 29/1 (2004), 92–121; Richard J. Samuels, *Securing Japan: Tokyo's Grand Strategy and the Future of East Asia* (Ithaca NY: Cornell University Press 2007); Andrew L. Oros, *Normalizing Japan: Politics, Identity, and the Evolution of Security Practice* (Stanford CA: Stanford University Press 2008); Paul Midford, *Rethinking Japanese Public Opinion and Security: From Pacifism to Realism?* (Stanford CA: Stanford University Press 2011); Adam P. Liff, 'Japan's Defense Policy: Abe the Evolutionary,' *The Washington Quarterly* 38/2 (2015), 79–99. For some counter-views detecting significant change stirring in Japan's security, see Christopher W. Hughes, *Japan's Reemergence as a 'Normal' Military Power* (Oxford: Oxford University Press 2004); Kenneth B. Pyle, *Japan Rising: The Resurgence of Japanese Power and Purpose* (New York: Public Affairs 2007); Christopher W. Hughes, *Japan's Remilitarization* (London: Routledge 2009); and Sebastian Maslow, 'A Blueprint for a Strong Japan? Abe Shinzō and Japan's Evolving Security System,' *Asian Survey* 55/4 (2015), 739–65.

[2]For one of the first looks at Japan's emerging cybersecurity policies, see Paul Kallender, 'Japan, the Ministry of Defense and Cyber-Security,' *The RUSI Journal* 151/1 (2014), 94–103. For examples of the as yet limited academic analysis in English and Japanese, see Yasuhide Yamada, Atsuhiro Yamagishi, and Ben T. Katsumi, 'Comparative Study of the Information Security Policies of Japan and the United States,' *Journal of National Security Law & Policy* 4 (2010), 217–32, <http://jnslp.com/wp-content/uploads/2010/08/14_Yamada.pdf>; Tsuchiya Motohiro, 'Cybersecurity in East Asia: Japan and the 2009 Attacks on South Korea and the United States,' in Kim Andreasson (ed.), *Cybersecurity: Public Threats and Responses* (Boca Raton FL: CRC Press 2012), 55–76; Pōru Karendā, 'Bōeishō to Saibā Sekyuritī ni Kansuru Shinten to Otoshiana,' SFC Kenkyūjo Nihon Kenkyū Purattofōm, *Rabowākingu Pēpa Shirīzu*, 8, Dec. 2013, 1–16, <http://jsp.sfc.keio.ac.jp/pdf/wp/jsp-wp_8_Paul%20Kallender.pdf>.

under previous administrations, and accelerating under current Prime Minister Abe Shinzō, Japan is starting to build its own domestic policy infrastructure and capabilities for defensive cybersecurity. Through the mechanism of the US–Japan alliance, Japan is deliberately and progressively integrating its capabilities and strategy with those of the United States in order to face down the cyber threats from China and other actors. Moreover, Japan's new seriousness of intent in cybersecurity is reflective of the broader trends of change and new assertiveness in its overall security trajectory, and further highly significant due to cybersecurity's deep interconnections with so many other dimensions of military activity. Cybersecurity's facilitation of 'cross-domain' operations means it is positioned at the leading edge of and helping to drive forward transformation in Japanese policy and capabilities across the full range of land, sea, air, and outer space activities. Japan has thus moved to first securitize its response to challenges in the domain of cyberspace by taking data assurance issues traditionally within the realm of information technology public policy governance and now defining and embedding them as central security issues and thus to be accorded higher national policy priority and resources, requiring a whole of government approach.[3] In turn, Japan has begun to militarize its response – moving elements of cybersecurity from previously purely civilian concerns and now augmenting the responsibility of its principal military institutions, namely the Japan Ministry of Defense (JMOD) and Japan Self-Defense Forces (JSDF) – to deter threats in this domain.

This article – as one of the very first scholarly analyses on the topic, and accessing Japanese materials not yet brought fully into the public domain – demonstrates its arguments about the evolution and significance of Japan's cybersecurity stance in three main sections. The first outlines Japanese policy-makers' increasing recognition of the type of cybersecurity challenges posed within the Asia-Pacific region, particularly from China and North Korea. The second investigates Japan's response to cybersecurity threats in recent years in fundamentally restructuring and aligning its domestic policy-making doctrines and structures – involving the Cabinet Office, National Security Council, JMOD, and other key central ministries, the JSDF, the governing Liberal Democratic Party (LDP) and main opposition Democratic Party of Japan (DPJ) – in order to generate more effective cyberdefense policies. It further examines how Japan is investing in new cyber capabilities to fend off threats and possibly even in the future to enhance its capabilities to take part in offensive cyber operations. The third explores how Japan's increasingly assertive response to cyber threats is being integrated into, and thus amplifies, the effectiveness of US–Japan alliance cooperation in this

[3]For the classic definition of securitization, see Barry Buzan, Ole Wæver, and Jaap de Wilde, *Security: A New Framework for Analysis* (Boulder CO: Lynne Rienner Publishers 1998), 25.

dimension of security. The conclusion evaluates the significance of Japan's evolution toward becoming a 'cyber power' – a state with not only a cyber capability integrated into its national security strategy (NSS), but the capabilities of which also make it a significant player in the East-Asian security architecture, even if not yet on a par with the United States or China in this domain. It examines the potential impact of Japan's growing presence for the other dimensions of its security policy, its overall security trajectory and emergence as a more muscular military power, and the impact on ties with the United States, China, and the regional strategic balance.

Japan's growing perceptions of cybersecurity challenges

Japan is becoming serious about cybersecurity, but this was not always the case. In fact, until the late 2000s, Japan's precursor of what is now termed cybersecurity focused on data assurance and the promotion of information and communications technology for economic growth; unsurprising given that it possesses the third largest economy in the world by nominal gross domestic product, the fourth largest by purchasing power parity, and is the second largest developed economy.[4] Administration of data assurance was devolved to diverse civilian and bureaucratic actors, entirely non-militarized, and with a highly limited perception of data assurance as a national security issue. The JMOD in its *Defense of Japan* White Papers contained no references to cybersecurity until 2010, and only one brief mention of cybersecurity in its 2004 revised National Defense Program Guidelines (NDPG), the document that set out Japan's defense doctrine alongside the necessary force levels.[5]

But from 2009 onward, a series of international and domestic incidents revealed Japan's cybersecurity vulnerabilities and caused it begin to securitize and then militarize its cybersecurity strategy. In that year, United States and South-Korean internet services were subject to large-scale distributed denial of service (DDoS) attacks, and Japan was affected by a sharply increasing volume of advanced persistent threats (APTs). The Ministry of Economy, Trade, and Industry (METI) noted waves of attacks specifically against Japan beginning in September 2010 and counted a sixfold increase in sophisticated spear-phishing attacks on leading corporations, research institutes, and the government between 2007 and 2011. In 2011, such spear-phishing attacks accounted for one-third of all recorded attacks, with nearly 37 per cent of APTs focused on Japan's critical infrastructure

[4]OECD, 'Country Statistical Profile: Japan,' *OECDi Library*, 28 Feb. 2013, <http://www.oecd-ilibrary.org/economics/country-statistical-profile-japan_20752288-table-jpn>.

[5]Bōeishōhen, *Bōei Hakusho 2010* (Tokyo: Zaimushō Insatsukyoku 2010), 17–18; Bōeishō, 'Heisei 17nen ikō ni Kakawaru Bōeikeikaku no Taikō ni Tsuite' (10 Dec 2004), 8–9, <http://www.mod.go.jp/j/approach/agenda/guideline/2005/taiko.pdf>.

(CI), for example, power plants and high-tech manufacturing industry.[6] High-profile breaches followed, including in 2011 attacks on Mitsubishi Heavy Industries (MHI), Japan's largest defense contractor, and its computer systems relating to the design and manufacture of ballistic missile defense (BMD) interceptor missiles, fighter planes, and space launch vehicles. Revelations followed of similar attacks on other strategically sensitive arms contractors, strategic technology, and government corporations and institutions, and not least Japan's main space agency, which is increasingly involved in highly sensitive military space development. Japan in 2015 alone was subject to cyberattacks that resulted in the leaking of over two million sets of personal data.[7] Similarly, the National Police Agency (NPA) noted a quadrupling of the number of cybercrimes reported to it in the year 2014 compared to a decade earlier.[8] Table 1 summarizes notable cyberattacks on Japan since the late 2000s.

Although North Korea and Russia are mentioned, China is often cited in Japan as the main source of APTs seeking to steal strategic information from competitor and leading industrialized nations.[9] The 2013 *Defense of Japan* White Paper devoted a lengthy section to cyberwarfare and APTs, noting that the People's Liberation Army (PLA) had a cyber unit believed to be carrying out attacks on US companies, that Japan's government agencies had been subject to cyberattacks after the acquisition of the disputed Senkaku/Diaoyu islands in September 2012, and, by inference pointed to China as the perpetrator.[10]

The result of rising concerns about APTs and China's potential involvement has been for Japan to now begin to elevate cybersecurity into the top echelons of security concerns. JMOD's *Defense of Japan* since 2011 has carried a substantial section on cyber threats, and placed it alongside weapons of mass destruction and international terrorism as the most immediate of regional and global security concerns.[11] The 2010 revision of the NDPG under the DPJ administration, and then the 2013 revision under the returning LDP, demonstrated a new cross-party consensus that cyberspace formed part of the global commons, along with the land, maritime,

[6]METI, *Cybersecurity and Economy Study Group Report of August 2011* (Tokyo: Ministry of Economy, Trade and Industry 2011). A Japanese summary of the report is held by the authors.

[7]'At least 2 million sets of personal data feared leaked after cyberattacks in 2015,' *The Japan Times*, 3 Jan. 2016, <http://www.japantimes.co.jp/news/2016/01/03/national/least-2-million-sets-personal-data-feared-leaked-cyberattacks-2015/#.VolMYoR8zzl">.

[8]Jumpei Kawahara, Director for Counter Cyber Attacks, Security Planning Division, Security Bureau, NPA, 'Cyber attacks situation and police measures,' Presentation to the International Cybersecurity Symposium – Critical Infrastructure Protection Towards 2020, Tokyo (29 Feb. 2016).

[9]National Institute for Defense Studies, *NIDS China Security Report 2014: Diversification of Roles in the People's Liberation Army and People's Armed Police* (Tokyo: National Institute for Defense Studies 2014), 52–3.

[10]Japan Ministry of Defense, *Defense of Japan 2013* (Tokyo 2013), 80–1.

[11]Bōeishōhen, *Bōei Hakusho 2011* (Tokyo: Zaimushō Insatsukyoku 2011), 23, 28–32.

Table 1. Notable reported significant cyberattacks on Japan, 2000–2015.

January 2000	STA, MOE, MOFA, MOPT,	GOJ major ministries and laboratories websites overwritten or attacked.
2010–	GOJ, CI in Japan, ROK, United States, Europe, Southeast-Asian countries, government and defense-related targets	Concerted multi-country, strategic industry spear phishing, waterhole and zero-day exploit campaign initially under the moniker Midsat that after 2015 moved to CI with a specific focus on Japan
March 2011	GOJ	Spear phishing emails tracked to servers from South-Korean and Chinese access points to provide information about the Fukushima nuclear disaster from GOJ organizations. Some of the emails were masked to appear as if originating from GOJ email accounts; used counterfeited Cabinet Office classification codes; and impersonated MOFA and JCG officials even using their real email addresses
2011	MOFA	Diplomatic missions in Asia, North America, and Africa infected with viruses capable of stealing information
May 2011	NPA	Received 24 malicious emails aimed at stealing classified information. NPA admits for the first time that it has been targeted for attack
June 2011	National Diet House of Representatives	Passwords and usernames of around 500 staff compromised, attributed to Icefog APT
August 2011	MHI	Admits APT attacks on 45 servers and infection of 38 personal computers in 11 locations with 8 or more types of viruses. The APTs targeted MHI systems for the design and production of many of Japan's most advanced military, civilian, and dual-use systems, including: the joint US–Japan SM-3 Block IIA advanced ballistic missile, military helicopters and F-2 fighter jets, submarines, the H-IIA and H-IIB space launch vehicles, and nuclear power reactors. IHI Corporation, Kawasaki Heavy Industries, and the Society of Japanese Aerospace Companies also later revealed that they had been targeted
October 2011	Geospatial Information Authority	Servers targeted
November 2011	National Diet House of Representatives and House of Councilors	APT emails linked to a China-based server
January 2012	JAXA	Attacks on personal computers, resulting in suspected leakage of information on the specifications and operation of the H-IIA Transfer Vehicle
April 2012	Nissan Motors	Data breaches and malware penetration of global information systems network. 300,000 malware installations from at least 29 malicious Android applications attack Japanese mobile phone users
July 2012	MOF	Detected an APT that had probably been able to steal confidential data from January 2010 to November 2011. A total of 123 computers inside the ministry were infected. Supreme Court and the Ministry of Land, Infrastructure, Transport, and Tourism also attacked
September 2012	GOJ and various	At least 19 Japanese websites, including the JMOD, MIC, NPA, and Tohoku University Hospital, attacked as part of a list 300 Japanese organizations noted as potential targets for cyberattack on the message board of Chinese hacktivist group, Honker Union. NPA confirmed around 4000 people had posted messages about planned attacks and schemes on China's leading chat site 'YY Chat.' The upsurge of attacks commonly attributed to Japan's 'nationalization' of the disputed Senkaku/Diaoyu islands the same month

(*Continued*)

Table 1. (Continued).

October 2012	MAFF	APT harvests approximately 3000 files, including 20 top-secret trans-Pacific Partnership-free trade initiative files dating from between October 2011 and April 2012. Other targeted documents included those for the Asia-Pacific Economic Cooperation Summit meeting in November 2011, and US–Japan summit meeting in April 2012
November 2012	JAXA	Suspected espionage of Japan's major launch vehicles targeting the *Epsilon*, H-IIA/B, HTV, and M-5
January 2013	MOFA	At least 20 internal confidential documents allegedly stolen
April 2013	JAXA	Server hack steals technical information on the HTV, the Japan Experiment Module (*Kibō*). Brute force attacks then launched via China and United States against the information system of a JAXA section that manages *Kibō*, with a total of five systems hacked
September 2013	METI, MOF, and MOFA	Watering hole attacks whereby websites visited by a large number of people are baited with malware, and the malware infects only those targeted organizations for which the attacker has the IP addresses
2014–		Dust Storm starts using watering holes
January 2014	NARO and NAIS	Hacked accounts send large amounts of English-language spams
2014	GOJ	National Institute of Information and Communications Technology estimates 25.66 billion cyberattacks on the GOJ and other bodies in 2014 with 40 per cent of them traced to China
August 2014	Japanese ISPs	DNSAmp attacks on OCN, network failures at JCOM and K-opticom
September 2014	MOJ	Unauthorized access to the Legal Affairs Bureau
2015	Power generation, oil and natural gas, construction finance and transport, including auto sectors	Dust Storm starts using second-stage backdoors with hardcoded proxy addresses and credentials, then also Android and mobile platforms
2015	Prime Minister's Office	Prime Minister's Office website subject to DDoS attacks by anonymous hacker group in protest at Japan's restart of whaling activities
June 2015	Japan Pension Service	Targeted attack; data of 1.25 million people hacked
October 2015	FSA	Phishing attack
November 2015	TOCOG	DDos attack brings down site for 12 h

FSA: Financial Services Agency; GOJ: Government of Japan; JAXA: Japan Aerospace Exploration Agency; JCG: Japan Coast Guard; JMOD: Japan Ministry of Defense; MAFF: Ministry of Agriculture, Forestry, and Fisheries; MCA: Management Coordination Agency; MEXT: Ministry of Education, Culture, Sports, Science and Technology; MHI: Mitsubishi Heavy Industries; MIC: Ministry of Information and Communications; MOE: Ministry of Education; MOF: Ministry of Finance; MOFA: Ministry of Foreign Affairs; MOPT: Ministry of Posts and Telecommunications; NARO: National Agriculture and Food Research Organization; NIAS: National Institute of Agrobiological Sciences; NIRA: National Institute for Research Advancement; NPA: National Police Agency; STA: Science and Technology Agency; TOCOG: Tokyo Organizing Committee of the Olympic and Paralympic Games.

air, and space domains, that required defending and Japan's objective should be to ensure the 'stable use of cyberspace.'[12] Japan's first ever NSS formulated under the Abe administration in December 2013 similarly identified threats in cyberspace as major risks to the global commons.[13]

Japan's response to cybersecurity: strengthening policy, institutions, doctrines, and capabilities

Japan's moves to emerge as a cyber security power, triggered in reaction to rising perceptions of APTs regionally and globally, have taken form first over the last 15 years in the gradual securitization of the cyber domain, and then second over the last 2–3 years in the more rapid militarization of Japanese cyberdefenses. Japan's foundational IT policies were initiated by the 2000 Information Technology Basic Law and the establishment in February 2000 of an Information Security Section in Prime Minister's Cabinet Office. The first 'e-Japan Strategy' of 2001 focused on harnessing the revolutionary potential of the digital economy, rather than security considerations.[14]

Centralization and securitization of responses

A December 2004 review led to the establishment of a Cabinet Office IT Strategic Headquarters, and, in 2005, the Information Security Policy Council (ISPC) tasked with devising Japan's basic strategy and a National Information Security Center (NISC) to act as its secretariat to develop strategy roadmaps, maintain a government-wide framework for coordinating cyber CI protection, and to formulate Japan's as then limited international engagement on cybersecurity issues.[15] The IPSC then released Japan's 'First National Strategy on Information Security' in February 2006.[16] But in the hinterland behind these

[12]Bōeishō, 'Heisei 23nen ikō ni Kakawaru Bōeikeikaku no Taikō ni Tsuite' (17 Dec. 2010), 2, 5, <http://www.mod.go.jp/j/approach/agenda/guideline/2011/taikou.pdfpp>; Bōeishō, 'Heisei 26nen ikō ni Kakawaru Bōeikeikaku no Taikō ni Tsuite' (17 Dec. 2013), 2, <http://www.mod.go.jp/j/approach/agenda/guideline/2014/pdf/20131217.pdf>.

[13]Naikaku Kanbō, *Kokka Anzen Hoshō ni Tsuite* (15 Dec. 2013), 7–8, <http://www.cas.go.jp/jp/siryou/131217anzenhoshou/nss-j.pdf>.

[14]The IT Basic Law, Article 22 mandates the assurance of security and reliability of advanced information and telecommunications networks and the protection of personal information. In the 'e-Japan Strategy' of January 2001, security is only mentioned twice; once in connection with promoting a shift to the use of IPv64 addressing in a discussion of targets, and the other, in passing, notes that security is important as the government should work to eliminate the use of paper, see IT Strategy Headquarters, 'e-Japan Strategy' (22 Jan. 2001), <http://www.kantei.go.jp/foreign/it/network/0122full_e.html>.

[15]National Information Security Center, 'Japanese Government Efforts to Address Information Security Issues: Focusing on the Cabinet Secretariat's Efforts' (Nov. 2007), <http://www.nisc.go.jp/eng/pdf/overview_eng.pdf>.

[16]Information Security Policy Council, *The First National Strategy on Information Security: Toward the Realization of a Trustworthy Society* (2 Feb. 2006), <http://www.nisc.go.jp/eng/pdf/national_strategy_001_eng.pdf>.

new institutions and emerging strategy, cybersecurity policy and administration remained heavily sectionalized. The NPA prosecuted against cyberattacks that could be categorized as crimes; the JMOD was only responsible for its own networks; and intelligence issues were divided between the National Security Bureau of the NPA and the Defense Intelligence Headquarters (DIH) of the JMOD, both separated from the NISC.[17]

The shocks of 2009, and recognition of the importance of cyber security as a security domain in itself, accelerated Japan's subsequent reforms. The *Second National Strategy on Information Security*, released in February 2009 and running through to 2011, openly acknowledged the threat of APTs.[18] Japan divided its cybersecurity structure into three main supervisory bodies: the Cabinet Office founded a Crisis Management Center that reported to the Assistant Chief Cabinet Secretary, the Cabinet Intelligence Research Office reported to the Director of Cabinet Intelligence and on to the Assistant Chief Cabinet Secretary, and the NISC controlled the overall monitoring of governmental systems.[19] Japanese leaders also began for the first time to assert political control of cybersecurity policies. The Prime Minister assumed the role of Director-General of the IT Strategic Headquarters, 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. Nevertheless, the NISC, while centralizing cybersecurity policy under firmer direct political control, still just coordinated rather than exerted control over policy for the NPA, MIC, METI, and JMOD.

The new DPJ administration of September 2009 then overtly securitized policy. In May 2010, the ISPC's 3-year *Information Security Strategy for Protecting the Nation* for the first time framed cyberdefense in terms of national security by asking players to prepare responses to a large-scale cyberattack.[20] In June 2011, Japan enacted a cybercrime law that enabled it to finally join the Convention on Cybercrime, instituting a range of penalties regarding the distribution of malware or the acquisition or storage of a virus, the right to seize servers, and to request ISPs to store communications data. Following an anonymous hacker collective attack on several Japanese central ministries, the NISC also set up in June 2012 the Cyber Incident Mobile Assistant Team to provide coordinating emergency partnerships among

[17]Tsuchiya, 'Cybersecurity in East Asia,' 61.
[18]National Information Security Policy Council, *The Second National Strategy on Information Security, Aiming for Strong 'Individual' and 'Society' in IT Age* (3 Feb. 2009), <http://www.nisc.go.jp/eng/pdf/national_strategy_002_eng.pdf>.
[19]Tsuchiya, 'Cybersecurity in East Asia,' 61–2.
[20]Information Security Policy Council, 'Information Security Strategy for Protecting the Nation' (11 May 2010), 3, <http://www.nisc.go.jp/eng/pdf/New_Strategy_English.pdf>.

ministries and agencies.[21] IPSC's July 2012 *Information Security* plan focused on APTs and large-scale cyberattacks and suggested setting up attack drills with operators from nuclear plants, the gas distribution network, and telecommunications providers. The JMOD, together with the NPA, MIC, and METI, was then designated one of the government agencies to coordinate particularly closely with the NISC for CI defense and to bolster international cooperation against cyberattacks.[22]

The return of the LDP from late 2012, with stable majorities in both the lower and upper houses of the National Diet, has provided the platform for the even more rapid bolstering of Japanese efforts to centralize cybersecurity policy – the party when in opposition having witnessed with growing concern a series of sophisticated APTs in the aftermath of the March 2011 Fukushima nuclear power plant disaster (Table 1). The LDP Policy Research Council's Special Committee on IT Strategy in October 2011 presented 16 action items, including rethinking information security within the framework of national security and diplomacy, and charging the JMOD, NPA, and JCG with the responsibility to design a comprehensive architecture in their areas of information security modeled on that of the United States.[23] In February 2012, the LDP's 'Proposal on Information Security' designated cybersecurity as a critical part of national security, and matching broader ongoing defense reform efforts to transform the JSDF into a 'dynamic defense force' (*dō-teki bōeiryoku*) that could counter security threats proactively and beyond Japan's immediate territory, urged that the JMOD, NPA, and JCG should strengthen 'dynamic defense capabilities' (*dō-teki bōgyōryokyu*) against cyberattacks. The LDP further proposed revising the existing domestic emergency legislation for wartime contingencies to include cyberattacks and enact a law to protect classified information to make cooperation easier with major partners such as the United States, United Kingdom, Australia, and India.[24]

Then, the IPSC, in June 2013, in the wake of the March cyberattacks of the same year against South Korea's finance and media industries, finally replaced the term 'information security' with the term 'cybersecurity' in its new strategy, so recognizing it as a national security issue and a strategic domain along with land, sea, air, and outer space.[25] The *Cybersecurity Strategy* contained an entirely new section that for the first time elaborated

[21]Taipei Times, 'Japan Probes Website Attacks Amid Anonymous Claims,' *AFP*, 27 Jun. 2012, <http://www.taipeitimes.com/News/world/archives/2012/06/29/2003536553>.
[22]Information Security Policy Council, 'Information Security 2012' (4 Jul. 2012), 21–2, <http://www.nisc.go.jp/eng/pdf/is2012_eng.pdf>.
[23]Jiyū Minshutō Seisaku Chōkai IT Senryaku Tokubestu Iinkai, *Jōhō Sekyuritī Taisaku ni Kansuru Mōshiire* (28 Oct. 2011), 1–2, <http://www.jimin.jp/policy/policy_topics/pdf/seisaku-088.pdf>.
[24]Jiyū Minshutō, *Jōhō Sekyuritī ni Kansuru Teigen* (24 Feb. 2012), 4, 16, <https://www.jimin.jp/policy/policy_topics/pdf/seisaku-096.pdf>.
[25]Informational Security Policy Council, *Cybersecurity Strategy: Towards a World-Leading, Resilient and Vigorous Cyberspace* (10 Jun. 2013), 4, <http://www.nisc.go.jp/eng/pdf/cybersecuritystrategy-en.pdf>.

on the role of the JMOD and JSDF in responding to 'cyberattacks carried out as part of an armed attack by foreign governments and other national level cyberattacks for which the involvement of foreign governments is suspected.' Accordingly, the JSDF was designated as responsible for countering cyberattacks when they constituted part of armed attacks; and the JMOD was mandated to establish a Cyber Defense Unit (CDU) under the JSDF.[26]

The Abe administration then passed in December 2013 the Protection of Specially Designated Secrets Law, and then in November 2014 the Cyber Security Basic Act. The former systematized the designation of certain types of information – including JSDF-related operational information, signals or imagery data, defense communications networks and cryptography and data on weapons and hardware performance used in defense – as national security secrets subject to restrictions and penalties for breaches.[27] The latter mandated the formulation of a *Cybersecurity Strategy* that would be drawn up based on a Cabinet Decision requested by the prime minister.[28]

Following recommendations from NISC, in November 2014 the IPSC adopted the 'Policy to Enhance Japan's Cyber Security' and transformed into the Cyber Security Strategy Headquarters (CSSH), responsible for creating Japan's new 'whole of government' *Cyber Security Strategy* of September 2015. The Cyber Security Basic Act gave CSSH much more comprehensive powers to assert a national strategy for cybersecurity – preventing continued stovepiping by making one of its prime missions under the law's first provision '3. General Policy' the assurance of cybersecurity at national administrative organs.[29] The CSSH, placed as it is within the increasingly powerful Cabinet Office, should now have the authority to formulate common security standards for all central ministries and to evaluate their performance, especially in the light of any breaches or inadequacies exposed. It also has the authority to monitor expense budgeting plans for cybersecurity in ministries and Independent Administrative Institutions (IAIs), placing it above competitor agencies such as METI and the MIC.[30]

The 2015 revised *Cyber Security Strategy* most fully expresses the Abe administration's determination to securitize the cyber domain. Especially mindful of the risks posed to the Tokyo 2020 Olympics, the strategy stresses that cyberspace is now a key element of Japan's overall national security,

[26]Information Security Policy Council, *Cybersecurity Strategy*, 41–2.
[27]Cabinet Secretariat, 'Overview of the Act on the Protection of Specially Designated Secrets,' <http://www.cas.go.jp/jp/tokuteihimitsu/gaiyou_en.pdf>.
[28]NISC, *Saiba Sekuritī Kihon Hōan no Gaiyō*, 10 Aug 2014, <http://www.nisc.go.jp/conference/seisaku/dai40/pdf/40shiryou0102.pdfhttp://www.nisc.go.jp/conference/seisaku/dai40/pdf/40shiryou0102.pdf>.
[29]Yasu Taniwaki, 'Cybersecurity Strategy in Japan,' Deputy Director-General NISC (9 Oct. 2014), <http://www.nisc.go.jp/security-site/campaign/ajsympo/pdf/keynotelecture.pdf>; and Hiroshi Kawaguchi, 'Cybersecurity Strategy in Japan, Japan Security Operation Centre' (21 Jan. 2015), <http://staff.cs.kyushu-u.ac.jp/en/event/2015/01/data/17%20kawaguchi.pdf>.
[30]Kawaguchi, 'Cybersecurity Strategy in Japan.'

and that Japan will look for the stable use of cyberspace in line with the administration's broader security strategy of a 'proactive contribution to international peace'. The JSDF is again charged with defending against cyberattacks through a qualitative and quantitative strengthening of its capabilities that encompass the defense of not only its own networks and infrastructure, but also to now 'deepen coordination with stakeholders relevant to the assurance of the missions of the Self Defense Forces in light of the possibility that cyberattacks against social systems indicated above may become a major impediment to the accomplishment of their mission,' so indicating the broader militarization of cyberdefense and its potential stretching into formerly exclusive civilian domains across Japanese society.[31]

The role of JMOD and JSDF: starting to militarize responses

The JMOD and JSDF have moved concomitantly to develop a cyber doctrine for domestic defense and increasingly international cooperative purposes. The JDA first formally adopted information security provisions in December 2000 when it set up its first cyber-surveillance unit in the Japan Air Self-Defense Force (JASDF), followed by other units within the Japan Ground Self Defense (GSDF) and Maritime Self-Defense Force (MSDF).[32] In 2007 the JMOD created a combined command – the Defense Information Infrastructure (DII) – to tackle threats, and in March 2008, the JMOD and JSDF inaugurated the SDF C4 (Command, Control, Communications and Computers) System Command.[33] The JMOD's 2010 *Defense of Japan* White Paper announced the policy of 'Six Pillars of Comprehensive Defense Against Cyber Attacks,' focusing on: improving cyberattack defences; intrusion prevention systems; upgrading monitoring and device analysis; development of regulations and directives on information assurance; bolstering training through the dispatch of personnel to the United States; information-sharing with organizations such as NISC; increased research on the latest technology for countering cyberattacks; the establishment of a

[31]Government of Japan, *Cybersecurity Strategy* (4 Sep. 2015), 35, 37, 38, 53, <http://www.nisc.go.jp/eng/pdf/cs-strategy-en.pdf>.

[32]Paul Kallender-Umezu, 'Japan Takes Action Against Complex Cyber Threats,' *Defense News*, 9 Oct. 2012, <http://archive.defensenews.com/article/20121009/C4ISR01/310090010/Japan-Takes-Action-Against-ComplexCyber-Threats>.

[33]For further details on the DII and the Central Command System (a system that performs operations such as intensive processing of data while connected online with various command systems of the GSDF, MSDF and ASDF, Maritime, and Air Self-Defense Forces), see Bōeichō, 'Bōeichō, Jietiai ni Okeru Jōhō Tsūshin Gijutsu Kakumei e no Taio Sōgō-teki Shisaku no Suishin Gaiyō: Jōhō Yūetsu no Tame no Kiban Kōchiku o Mezashite' (Dec. 2000), <http://www.mod.go.jp/j/approach/others/security/it/youkou/index.html>; Bōeishō, 'Kaisetsu: Jieitai Shiki Tsūshin Shisutemutai Kashō no Shinhen' (2007), <http://www.clearing.mod.go.jp/hakusho_data/2007/2007/html/j22c1000.html>.

coordinator for cyber-planning in the Joint Staff Office; and requesting the DIH conduct long-term specialist research into cyber-warfare trends.[34]

The 2011 Mid-Term Defense Program, then called for the JMOD to establish a cyberdefense doctrine and to create the forerunner of the CDU later established in 2014.[35] Following this, in 2012 the Japanese government for the first time acknowledged the status of cyberspace as an operational domain under international law, and thereby Japan's right to self-defense. In January 2012, Gemba Kōichirō became the first serving Japanese foreign minister to attend an ISPC meeting. In April, he talked about the relationship between cyberattacks and international law, which the media interpreted as a declaration of Japan's right to self-defence against cyberattacks under existing international law, including the UN Charter.[36]

In turn, in July 2012 JMOD's *Defense Posture Review Interim Report* cited response to cyberattacks as amongst it 10 top priorities, along with items such as strengthening information, surveillance and reconnaissance (ISR) and maritime security capabilities, and promoting the use of outer space.[37] In September 2012, JMOD's *Toward Stable and Effective Use of Cyberspace* formulated Japan's preliminary cyberdefense doctrine. JMOD and the JSFDF were to prepare for cyberattacks as part of an armed attack; cyberspace was a domain for defense operations in the same way as land, sea, air, and outer space; and responses were on the basis of individual self-defense. The document acknowledged the challenges of responding to cyberattacks given the involvement of state and non-state actors resulting from the ready availability of information technologies; the variety of means available for cyberattacks including malware, DDoS, and infiltration of systems; that cyberattacks may occur in contingencies ranging from peacetime to wartime; that attacks might be characterized by stealth, anonymity, and offensive dominance; and that deterrence was difficult due to the asymmetric nature of attacks, meaning that it was hard to impose costs on an attacker committing cheap and expendable assets, but that deterrence by punishment or denial might be involved. The JMOD and JSDF were to strengthen their cyberdefenses specifically by the creation of the DII; establishment of the CDU; improvement of situational awareness and early-warning capabilities; promotion of cooperation with other government agencies and the private sector; and enhanced cooperation with the United States and other

[34]Japan Ministry of Defense, *Defense of Japan 2010* (Tokyo: Urban Connections 2010), 184–5.
[35]Japan Ministry of Defense, 'Mid-Term Defense Program (FY2011–FY2015)' (17 Dec. 2010), 4, 6, <http://www.mod.go.jp/e/d_act/d_policy/pdf/mid_termFY2011-15.pdf>.
[36]Shozo Nakayama, 'Govt. Claims Cyberdefense Right/Says International Laws Should be Applied to Computer Infiltration,' *Yomiuri Shimbun*, 17 May 2012, <http://news.asiaone.com/print/News/AsiaOne%2BNews/Asia/Story/A1Story20120518-346660.html>.
[37]Bōeiryoku no Arikata Kentō no Tame no Iinkai, *Bōeiryoku no Arikata Kentō ni Kansuru Chūkan Hōkoku* (26 Jul. 2012), 1, 3, 8, <http://www.mod.go.jp/j/approach/agenda/guideline/2013_chukan/20130726.pdf>.

partners and friendly nations such as Australia, the United Kingdom, Singapore, and the North Atlantic Treaty Organization (NATO).[38]

JMOD, following the return of the LDP to government, then requested in December 2012 a budget of ¥1.2 billion to establish the CDU with an initial staff of ninety personnel.[39] The CDU, reporting directly to the defence minister, has taken control of previously stovepiped units. Until this point, each service, including the JGSDF System Protect Unit, the JMSDF Communications Security Group, and the JASDF Computer Security Evaluation Unit, had defended its own systems under the coordination of the C4 Systems Command. Under the new system, finally, the CDU and the cybersecurity coordinator in the Joint Staff Office took responsibility for the full SDF DII Network and Central Command System.[40] The revised 2013 NDPG and MTDP stressed the JSDF's priority was to preserve and enhance joint operations through developing capabilities for persistent ISR in cyberspace and for the survivability of command and control systems.[41]

International strategy for cyberspace and US–Japan alliance cooperation

Japanese cyberspace diplomacy

Japanese policy-makers in conjunction with the development of a national cybersecurity strategy have also placed increasing importance on international cooperation, recognizing the inherently trans-border nature of the challenge of cybersecurity issues demanding multilateral coordination and the possibility to acquire policy lessons and advanced capabilities from other states. Moreover, as Japan has progressively securitized, and most recently militarized, the cyber domain, the JMOD, and JSDF have emphasized the importance of working with the United States and other international partners on cybersecurity for information assurance relating to defense equipment production and the broader military strategic purposes of securing the global commons.

Japan's 2006 *First National Strategy on Information Security* stated Japan's ambition to contribute to the stable use of cyberspace internationally and even to develop a 'Japan Model' that could be applied on a global scale to

[38] Japan Ministry of Defense, *Toward Stable and Effective Use of Cyberspace* (Sep. 2012), 3, 5, 7–12, <http://www.mod.go.jp/e/d_act/others/pdf/stable_and_effective_use_cyberspace.pdf>.

[39] Bōeishō, *Heisei 24nendo Bōei Yosanan no Gaisan no Gaiyō* (Dec. 2012), 3, <http://www.mod.go.jp/j/yosan/2012/kankei.pdf>.

[40] Paul Kallender-Umezu, 'Experts: Japan's New Cyber Unit Understaffed, Lacks Skills,' *Defense News*, 9 Jul. 2013, p. 10.

[41] Japan Ministry of Defense, 'National Program Guidelines for FY2014 and Beyond' (17 Dec. 2013), 14–15, 20, <http://www.mod.go.jp/j/approach/agenda/guideline/2014/pdf/20131217_e2.pdf>; Japan Ministry of Defense, 'Medium Term Defense Program (FY2014-FY2018)' (17 Dec. 2013), 13–14, <http://www.mod.go.jp/j/approach/agenda/guideline/2014/pdf/Defense_Program.pdf>.

promote cooperation.[42] The 2010 *Second National Strategy on Information Security* reemphasized the importance of international cooperation and partnerships, particularly with the United States and Europe, and the possibility of Japanese leadership in information assurance across Asia.[43] The May 2011 *Information Security Strategy for Protecting the Nation* and *Information Security 2012* plan stressed the strategic and political strengthening of 'alliances' for cybersecurity cooperation with the United States, European Union (EU) countries, and the Association of Southeast Asian Nation (ASEAN) states.[44] The 2013 *Cybersecurity Strategy* focused on Japan's role in working multilaterally to ensure the freedom of cyberspace, and cooperation with countries that share the basic values of 'democracy, respect for human rights and the rule of law' – so drawing on the same language of the Abe administration's broader strategy of values-oriented diplomacy, often provided in implicit contradistinction to China's alleged lack of respect for international norms in domains such as cyberspace.[45] The 2015 *Cybersecurity Strategy* again stressed that Japan's cyber efforts were fully part of its larger diplomatic strategy to reinforce international rules and norms for governance of the global commons and that the United States, Europe, and Asia-Pacific were key partners in this campaign, along with now Latin America, the Caribbean, Middle East, and Africa.[46]

Japan's diplomatic efforts relating to cybersecurity took specific form with MOFA's creation of a Cyber Task Force in February 2012 under the control of Ambassador Shinotsuka Tamotsu, consisting of five policy units: international rule-making, cybercrime, system security and protection, economic issues, and national cybersecurity.[47] In October 2013, the ISPC launched a new international campaign to assert Japan as an active stakeholder in global cybersecurity. Japan committed to international rule-making and capacity-building at the UN, Group of Eight, ASEAN Regional Forum, Organization for Economic Cooperation and Development, Asia-Pacific Economic Cooperation, and NATO. In respect of policies for CI protection and rapid incident response, global initiatives have also been undertaken at the Meridian and the International Watch and Warning Network (IWWN), which are for government agencies; as well as at such meetings as FIRST (Forum of Incident Response and Security Teams), APCERT (Asia-Pacific Computer Emergency Response Team), which is a community of CSIRTs

[42]Information Security Policy Council, *The First National Strategy on Information Security*, 5, 29.
[43]National Information Security Policy Council, *The Second National Strategy on Information Security*, 68–9.
[44]Information Security Policy Council, *Information Security Strategy for Protecting the Nation*, 17–18; and Information Security Policy Council, *Information Security 2012*, 92–3.
[45]Informational Security Policy Council, *Cybersecurity Strategy*, 49.
[46]The Government of Japan, *Cybersecurity Strategy*, 41–4.
[47]Ministry of Foreign Affairs Japan, 'Press Conference by Minister for Foreign Affairs Koichiro Gemba' (14 Feb. 2012), <http://www.mofa.go.jp/announce/fm_press/2012/2/0214_01.html>; Kallender-Umezu, 'Japan Takes Action'.

from the Asia-Pacific region, and follow-up meetings to the London Conference on Cyberspace, each of which is attended by a broad range of entities from both the public and private sectors. In addition, with respect to investigating cybercrime, efforts are being undertaken to deepen international cooperation through frameworks such as the International Criminal Police Organization (ICPO).[48] Japan's building of relationships in the Asia-Pacific has been a major priority, given increased investment by Japanese enterprises in ASEAN countries.[49]

US–Japan military alliance extended into the cyber domain

Japan's diplomatic and technical international campaigns have shadowed and supported the efforts by the JMOD to begin to militarize the response to cybersecurity through deepening cooperation with US military cyber strategy regionally and globally. Japan–US cooperation first stressed information assurance for bilateral defense production. As a result of US concerns over Japanese data protection in the transfer of BMD technology, the JDA adopted information security provisions in December 2000 and set up its first cyber-surveillance unit. Japan and the United States, via the working-level Defense Policy Review Initiative from 2002 to 2007, and via successive Security Consultative Committee (SCC) 'Two-Plus-Two' meetings involving the foreign and defense ministers of both states from the early 2000s onward, have focused increasingly on bilateral military integration in BMD, air defense, maritime security, extended deterrence, ISR, CI protection, and mutual logistics support – all data-centric operations and necessitating enhanced information assurance measures. Japan's revealed vulnerabilities in 2006–07 over the handling of data relating to the *Aegis* naval air-defense system and the stovepiping between mutually exclusive cyberdefence systems operated by the ASDF, GSDF, and MSDF drove further change in bilateral data assurance.[50] In April 2006, Japan and the United States signed the Memorandum of Understanding Concerning Cooperation Regarding Information Assurance and Computer

[48]Information Security Policy Council Japan, *International Strategy on Cybersecurity Cooperation – j-Initiative for Cybersecurity* (2 Oct. 2013), <http://www.nisc.go.jp/eng/pdf/InternationalStrategyonCybersecurityCooperation_e.pdf>.

[49]Japanese Ministry of Internal Affairs and Communications, 'Joint Ministerial Statement of the ASEAN-Japan Ministerial Policy Meeting on Cybersecurity Cooperation, Tokyo' (13 Sep. 2013), http://www.soumu.go.jp/main_content/000249127.pdf; Koji Nako, 'Toward Proactive Response Against Cyber-Attacks Based on Global Monitoring and Analysis: PRACTICE Project (Research Part)', 2013 < https://sicherheit.eco.de/wp-content/blogs.dir/27/files/1145_nakao2.pdf>.

[50]Taipei Times, 'Japanese Navy Officer Arrested for Leaking Secret Data: Police,' *AFP*, 13 Dec. 2007, <http://www.taipeitimes.com/News/world/archives/2007/12/14/2003392484>. In an embarrassing incident in 2006–2007, it was discovered that details of the US *Aegis* system had been copied by a 34-year old lieutenant commander onto a CD and passed to other MSDF officers, who had themselves made copies, causing the United States to temporarily halt the shipment of parts *Aegis* radar upgrades on the Japanese destroyer *Kongō* just as Japan was pressing the United States to allow it to procure the F-22 fighter and stealth technologies.

Network Defense.[51] The May 2007 SCC two-plus-two meeting committed Japan and the United States to sharing of BMD and related operational information on a direct, real-time, and continuous basis; and in August 2007, Japan and the United States signed a General Security of Military Information Agreement to facilitate further confidence in military information exchange.[52]

Since 2009, bilateral cooperation in cyberspace has further deepened and taken a new direction as the United States has sought to harness Japan's support for its global cybersecurity agenda. In turn, Japan has increasingly integrated its cyberdefense capabilities into the United States' broader alliance strategy to support the US 'rebalance' to the Asia-Pacific and to counter the rise of China militarily. The United States' stocktaking of its approach to cybersecurity – comprising the May 2009 US *Cyberspace Policy Review*, June 2009 establishment of US Cyber Command, May 2011 *International Strategy for Cyberspace*, and February 2010 *Quadrennial Defense Review*, and more broadly its doctrine of the Joint Operating Environment recognizing the crucial importance of data-centric operations – sought to incorporate cyberspace as the fifth domain into a combined warfighting strategy, involving more centralized control and a cooperation with a range of international partners for collective security ends.[53] A new phase was initiated where Japan was expected to stretch to follow the US global lead.

The June 2011 SCC meeting for the first time designated cybersecurity, along with outer space, as an alliance 'common strategic objective' and aimed to strengthen bilateral deterrence and contingency responses in cyberspace.[54] The SCC agreed to establish a US–Japan Cyber Dialogue, led by MOFA on the Japanese side, which first met in May 2013.[55] In April 2012, DPJ Prime Minister, Noda Yoshihiko, announced at his summit with

[51]Bōeichō, 'Nihon Bōeichō to Beikoku Kokubōshō no Jōhō Hoshō to Konpyūtā Nettowāku Bōgyō ni Okeru Kyōryoku ni Kansuru Ryōkai Obegaki (MOU) no Teiketsu ni Tsuite' (18 Apr. 2006), <http://www.mod.go.jp/j/press/news/2006/04/18a.html>.

[52]Ministry of Foreign Affairs Japan, 'Joint Statement of the Security Consultative Committee. Alliance Transformation: Advancing United States-Japan Security and Defense Cooperation' (1 May 2007), <http://www.mofa.go.jp/region/n-america/us/security/scc/joint0705.html>.

[53]Executive Office of the President of the U.S., *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications* (May 2009), 20–1, <https://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf>; Executive Office of the President of the United States, *International Strategy for Cyberspace Prosperity, Security, and Openness in a Networked World* (May 2011), 11–15, 18, 21, <https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf>; Department of Defense, *Quadrennial Defense Report* (Feb. 2010), 38–9, <http://www.defense.gov/Portals/1/features/defenseReviews/QDR/QDR_as_of_29JAN10_1600.pdf>; United States Joint Forces Command, *The Joint Operating Environment (JOE) 2010* (18 Feb. 2010), 34–6, <http://fas.org/man/eprint/joe2010.pdf>.

[54]Ministry of Foreign Affairs Japan, 'Joint Statement of the Security Consultative Committee. Toward a Deeper and Broader U.S.-Japan Alliance: Building on Fifty Years of Partnership' (21 Jun. 2011), 6, <http://www.mofa.go.jp/region/n-america/us/security/pdfs/joint1106_01.pdf>

[55]The US–Japan Cyber Dialogue involves representatives from Japan's MOFA, Cabinet Secretariat, NISC, Cabinet Intelligence and Research Office, NPA, MIC, METI, and JMOD. The US Department of State, 'Joint Statement on U.S.-Japan Cyber Dialogue' (10 May 2013), <http://www.state.gov/r/pa/prs/ps/2013/05/209238.htm>.

President Barack Obama in Washington DC that Japan along with other alliance initiatives would join the Convention on Cybercrime of which the United States was already a party.[56] The October 2013 SCC classified cyberspace as an emerging strategic domain necessitating bilateral cooperation to deal with shared threats and enhanced interoperability across a range of alliance military activities. The SCC further signed terms of reference for a new JMOD-Department of Defense (DOD) Cyber Defense Policy Working Group (CDPWG) to meet biannually to enhance cooperation among their respective cyber units. The JMOD participants include representatives from the Joint Chiefs of Staff, signaling the importance placed on the meetings.[57]

The April 2015 SCC and the simultaneous release of the revised US–Japan Guidelines for Defense Cooperation demonstrated the growing extent of bilateral ambitions in cyberspace. Japan and the United States stated their intention to cooperate in cyberspace and outer space to conduct 'cross-domain operations,' information sharing on threats, mission assurance, and CI protection.[58] The revised Defense Guidelines contained an entire section on cyberspace cooperation:

> To help ensure the safe and stable use of cyberspace, the two governments will share information on threats and vulnerabilities in cyberspace in a timely and routine manner…. The two governments also will share … information on the development of various capabilities in cyberspace, including the exchange of best practices on training and education. The two governments will cooperate to protect critical infrastructure and the services upon which the Self-Defense Forces and the United States Armed Forces depend to accomplish their missions, including through information-sharing with the private sector…. 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.

[56]Ministry of Foreign Affairs Japan, 'Fact Sheet: U.S.-Japan Cooperative Initiatives' (Apr. 2012), <http://www.mofa.go.jp/region/n-america/us/pmv1204/pdfs/Fact_Sheet_en.pdf>.

[57]Ministry of Foreign Affairs Japan, 'Joint Statement of the Security Consultative Committee. Toward a More Robust Alliance and Greater Shared Responsibilities' (3 Oct. 2013), 2, 4, <http://www.mofa.go.jp/mofaj/files/000016028.pdf>; Japan Ministry of Defense, 'Joint Statement of the U.S.-Japan Cyber Defense Policy Working Group' (30 May 2015), http://www.mod.go.jp/j/press/news/2015/05/30a_1.pdf; Bōeishō, 'Nichbei Saibā Bōei Seisaku Wākingu Gurūpu no Gaiyō Honnen Hachigatsu no Nichbei Bōei Kaidan ni Okeru ni Motozuki, Jieitai to Beigun no Saibā, Kyōryoku o Shinka suru Nichbei Bōei Tōkyoku de Giron o Okonau Tame no Wakugumi toshite Secchi' (3 Oct. 2013), <http://www.mod.go.jp/j/press/youjin/2013/10/03_cdpwg_gaiyou.html>.

[58]Ministry of Foreign Affairs Japan, 'Joint Statement of the Security Consultative Committee. A Stronger Alliance for a Dynamic Security Environment: The New Guidelines for Japan-U.S. Defense Cooperation' (27 Apr. 2015), 3–4, <http://www.mofa.go.jp/mofaj/files/000078186.pdf>.

> In the event of cyber incidents against Japan, including those against critical infrastructure and services utilized by the Self Defense Forces and the United States Armed Forces in Japan, Japan will have primary responsibility to respond, and based on close bilateral coordination, the United States will provide appropriate support to Japan. The two governments also will share relevant information expeditiously and appropriately. In the event of serious cyber incidents that affect the security of Japan, including those that take place when Japan is under an armed attack, the two governments will consult closely and take appropriate cooperative actions to respond.[59]

The revised Defense Guidelines aim for the close integration of Japanese and US cyberdefense strategies and thus form a pivotal component of the Abe administration's broader attempts to develop an increasingly assertive Japanese military stance supporting the US 'rebalance.' The United States is now providing a 'cybersecurity umbrella' for its ally to accompany the extended deterrent 'nuclear umbrella' and tighter cooperation in outer space, maritime security, and air defense. The cybersecurity component of the revised Defense Guidelines, unlike the treatment of the other strategic domains in the document, stopped short of making cybersecurity an explicit element of the Abe administration's intention and then later successful moves in 2015 to breach the ban on the exercise of the right of collective self-defense in support of the United States and other states. Nevertheless, the potential for cyberspace to reinforce US–Japan collective self-defence activities is evident. In May 2015, the CDPWG announced that the JMOD and DOD intend to forge options for 'enhanced operational cooperation' between their cyber units.[60] Most recently, at the 4th US–Japan Bilateral Cyber Dialogue, held in Washington in July 2016, the partners focused on military-to-military cyber cooperation.[61]

The Abe administration's revised September 2015 *Cybersecurity Strategy* in arguing that the maintenance of the stable usage of the international order around cyberspace is intrinsically linked with Japan's own national security, has essentially repeated the arguments utilized by Abe throughout 2014 and 2015 that Japan's own security is no longer divisible from that of the international community, so indicating that the exercise of collective self-defence and accompanying security legislation in September 2015 were now justified. Moreover, as pointed out above, US policy documents have made clear that cyberspace should be a domain for collective security actions with its alliance partners. JMOD and JSDF emerging capabilities also readily lend themselves to collective self-defense roles with the United States in the same way as their

[59]Ministry of Foreign Affairs Japan, 'The Guidelines for Japan-U.S. Defense Cooperation' (27 Apr. 2015), 21, <http://www.mofa.go.jp/mofaj/files/000078188.pdf>.
[60]Japan Ministry of Defense, 'Joint Statement of the U.S.-Japan Cyber Defense Policy Working Group' (29 May 2015), 1, <http://www.mod.go.jp/j/press/news/2015/05/30a_1.pdf>.
[61]U.S. Department of State, 'The 4th U.S.-Japan Bilateral Cyber Dialogue' (27 Jul. 2016), <http://www.state.gov/r/pa/prs/ps/2016/07/260572.htm>.

extant conventional capabilities. Japan has pledged cooperation with the United States in cyberspace in the particular areas of information-sharing, detection and early warning, and CI protection – exactly the same type of capabilities that Japan has stated in the revised Defense Guidelines it will provide to the United States for collective self-defense contingencies in the maritime and air-defense domains. Moreover, Japan and the United States' open acknowledgement of the cross-domain nature of cyberdefense capabilities, and their indispensable role in safeguarding the information systems that enable the coordination and operation of maritime and air-defense assets, means that Japan's capabilities are highly likely to be drawn upon in any type of military contingency. Japan's cyberdefense capabilities cannot in practice stand outside the collective self-defense framework and will form a central plank of bilateral warfighting operations.

Japanese cyberspace capabilities and collective self-defense approach should also be extendable to a range of other international partners and 'quasi-alliances' (*jun-dōmei*). In November 2014, Abe, Obama, and Australian Prime Minister Tony Abbott, pledged during the the G20 Leaders' Summit to bolster cybersecurity capacity-building. Japan has also been steadily working with Australia, India, the United Kingdom, and France over the exchange of defense technologies, consequent data assurance needs, and in some cases plans for more active cooperation on cybersecurity as a strategic domain.[62] For example, via the bilateral Japan–UK Cyber Dialogue, cybersecurity cooperation has joined the outer space and maritime domains as priority areas of cooperation.[63] Japan conducts a bilateral Japan–India Cyber Dialogue, and in October 2014, there was launched an EU–Japan Cyber Dialogue.[64]

Conclusion: Japan's cybersecurity policy, strategic trajectory, and the regional military balance

Japan since the late 2000s has begun to shake off its reputation as a reactive player in cybersecurity and moved to assume the trajectory and role of an emerging 'cyber power.' Japanese policy-makers from all political spectrums

[62]Ministry of Foreign Affairs Japan, 'Prime Minister Abe and Prime Minister Turnbull Joint Statement "Next Steps of the Special Strategic Partnership: Asia, Pacific and Beyond"' (18 Dec. 2015), <http://www.mofa.go.jp/a_o/ocn/au/page4e_000362.html>; Ministry of Foreign Affairs Japan, 'Japan and India Vision 2025 Special Strategic and Global Partnership: Working Together for Peace and Prosperity of the Indo-Pacific Region and the World' (12 Dec. 2015), <http://www.mofa.go.jp/s_sa/sw/in/page3e_000432.html>; Ministry of Foreign Affairs Japan, 'Joint Statement by the Prime Minister of the U.K. and Japan: A Leading Strategic Partnership for Global Prosperity and Security' (10 Apr. 2012), <http://www.mofa.go.jp/region/europe/uk/joint1204.html>.

[63]Ministry of Defense Japan, 'Second Japan-U.K. Foreign and Defence Ministerial Meeting 8 January 2016 Joint Statement', 2016 <http://www.mod.go.jp/j/press/youjin/2016/01/08_js_e.pdf>.

[64]Ministry of External Affairs, 'Fact Sheet: India and Japan, Working Together for Peace and Prosperity,' (12 Dec. 2015), <http://www.mea.gov.in/bilateral-documents.htm?dtl/26179/Fact_Sheet_India_and_Japan_Working_Together_for_Peace_and_Prosperity>; Ministry of Foreign Affairs Japan, 'Japan-EU Relations February 2016,' (2016), 3–4, <http://www.mofa.go.jp/files/000033265.pdf>.

and agencies, and provided with added momentum under the current Abe administration, have moved cybersecurity to the very core of national security policy to create more centralized institutions for formulating responses on cyber security, and for the JMOD and JSDF to build dynamic cyberdefense doctrines and capabilities. Japan's stance has thus moved rapidly toward the securitization and now increasing militarization of responses to challenges in the cyber domain.

Japan's cybersecurity policies are still under construction and there are challenges aplenty to be overcome. The JMOD and JSDF clearly require the steady input of resources to strengthen cyberdefense capabilities, eventually needing to recruit and train several hundred personnel to the CDU, although the defense budget request for 2016 does contain a substantial request for ¥17.5 billion for these cyberspace purposes.[65] The JMOD may also need further bolstering of its authority to extend cyberdefense activities into the civilian domain for CI protection, probably requiring a revision of the Self-Defence Forces Law. In addition, Japan's overall defense posture of 'exclusively defense-oriented defense' will for the time being remain primarily oriented to deterrence by denial, so contrasting strongly with other cyber powers reserving the right to utilize deterrence by punishment.[66]

Japan's cyberdefense capabilities are, though, magnified significantly by their integration with those of the US. Cybersecurity has moved also to the core of alliance strategy and plans for 'seamless interoperability' of bilateral capabilities, as seen from the 2015 revised Defense Guidelines. Japan's upgraded alliance role helps free up the United States to project retaliatory and offensive operations in the cyber and other strategic domains, reinforcing US capacity to continue to dominate the global commons. The US–Japan alliance's cybersecurity cooperation therefore opens the strong probability that Japan will be at some point in the future drawn into collective self-defense in this domain alongside such emerging and acknowledged commitments in maritime and air-defense operations.

Japanese efforts in cyberspace, therefore, closely correspond with, and indeed have formed an integral driver of, the broader transformation of its security posture and the US–Japan alliance in recent years, and especially under the Abe administration. The revised Defense Guidelines have removed the previous rigid separation of bilateral cooperation into 'peacetime,' 'Japan' and 'regional' contingencies. The intention is that future military cooperation will operate more smoothly across all potential

[65] James Andrew Lewis, *U.S.-Japan Cooperation in Cybersecurity: A Report of the CSIS Strategic Technologies Program*, CSIS, Washington DC (Nov. 2015), 11, <http://csis.org/files/publication/151105_Lewis_USJapanCyber_Web.pdf>; Bōeishō, *Waga Kuni no Bōei to Yosan: Heisei 28nendo Yosan no Gaiyō* (24 Dec. 2015), 13, <http://www.mod.go.jp/j/yosan/2016/yosan.pdf>.

[66] The Department of Defense, *The DoD Cyber Strategy* (Apr. 2015), 5–6, <http://www.defense.gov/Portals/1/features/2015/0415_cyberstrategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf>.

scenarios and levels of conflict escalation. Japanese security policy has been incrementally pushing forward, with at certain times more rapid advances, the development of JSDF capabilities characterized by an emphasis on joint operations among the MSDF, ASDF and GSDF, greater proactivity in responding to contingencies around Japan's periphery, and the procurement of power projection capabilities.[67]

Cyberdefense doctrine and capabilities stand at the forefront of this process of Japanese defense policy transformation and impact on Asia-Pacific security. Japan, in line with its ambitions for a more proactive defense posture and the expansion of the scope of alliance cooperation, has now maneuvered its security responsibilities into the entirely new domain of cyberspace, which by its very nature stretches, with no necessary functional or geographical limits, into all other strategic domains. Japan with its pervasive capabilities is therefore supporting the US goal for 'full-spectrum dominance' of the global commons as a whole and has moved from a previous purely supporting role into the very frontline of responding to potential conflicts in the region.

All this is likely to be perceived by China as another means to contain its rise, thereby leading to heightened Sino-Japanese tensions along this new strategic frontier, and spilling over into further compounding existing tensions in the maritime security and air-defense domains. Japan's expanding defense perimeter in cyberspace is not only likely to provide an arena to bring it into further direct tensions with China, but could also prove a ready channel for open and broader conflict. If China feels that Japan and the United States seek to gain near full superiority in cyberspace, and that their cyber capabilities, along with other enhanced capabilities in areas such as space-based and maritime ISR, BMD, and signals and electronic intelligence, mean that the PLA can no longer evade, hide, or strike back at the alliance, then China's asymmetric warfare doctrine behooves it to launch preemptive actions directed at and via Japan's cyber capabilities with the ultimate aim to disrupt JSDF joint operations and support for the US. Cyberspace, then, renders irrelevant geographical distance and denudes the concomitant strategic buffers that previously moderated Sino-Japanese security dilemmas and now presents the possibility of both sides being thrust into immediate confrontation. Japan and China will thus need to be cognizant of the risks of rapid escalation and conflict in cyberspace and feed through into other forms of military confrontation, and carefully manage their interactions in this domain and in the same way as they are searching with yet uncertain results for a modus vivendi in the maritime and air-defense spaces, if they are not to destabilize bilateral ties and the wider Asia-Pacific region security outlook.

[67] Christopher W. Hughes, *Japan's Foreign and Security Policy Under the 'Abe Doctrine'* (New York: Palgrave Macmillan 2015), 28–57, 65–70.

Disclosure Statement

No potential conflict of interest was reported by the author.

Notes on contributors

Paul Kallender (MA, Columbia; Ph.D candidate, Keio University) is coauthor of *In Defense of Japan: From the Market to the Military in Space Policy* (Stanford University Press, 2010). He is an associate researcher at the Global Security Research Institute.

Christopher W. Hughes (Ph.D, University of Sheffield) is Professor of International Politics and Japanese Studies, University of Warwick, and author of *Japan's Re-emergence as a Normal Military Power* (Oxford, 2004), *Japan's Remilitarisation* (Routledge 2009), and *Japan's Foreign and Security Policy Under the 'Abe Doctrine'* (Palgrave 2015).

Bibliography

Berger, Thomas U., *Cultures of Antimilitarism: National Security in Germany and Japan* (Baltimore MD: Johns Hopkins University Press 1998).

Bōeichō, 'Bōeichō, Jietiai ni Okeru Jōhō Tsūshin Gijutsu Kakumei e no Taio Sōgō-teki Shisaku no Suishin Gaiyō: Jōhō Yūetsu no Tame no Kiban Kōchiku o Mezashite' (Dec. 2000), <http://www.mod.go.jp/j/approach/others/security/it/youkou/index.html>.

Bōeishō, 'Nichbei Saibā Bōei Seisaku Wākingu Gurūpu no Gaiyō Honnen Hachigatsu no Nichbei Bōei Kaidan ni Okeru ni Motozuki, Jieitai to Beigun no Saibā, Kyōryoku o Shinka suru Nichbei Bōei Tōkyoku de Giron o Okonau Tame no Wakugumi toshite Secchi' (3 Oct. 2013, <http://www.mod.go.jp/j/press/youjin/2013/10/03_cdpwg_gaiyou.html>.

Bōeichō, 'Nihon Bōeichō to Beikoku Kokubōshō no Jōhō Hoshō to Konpyūtā Nettowāku Bōgyō ni Okeru Kyōryoku ni Kansuru Ryōkai Obegaki (MOU) no Teiketsu ni Tsuite' (18 Apr. 2006), <http://www.mod.go.jp/j/press/news/2006/04/18a.html>.

Bōeishō, 'Heisei 17nen ikō ni Kakawaru Bōeikeikaku no Taikō ni Tsuite' (10 Dec. 2004), <http://www.mod.go.jp/j/approach/agenda/guideline/2005/taiko.pdf>.

Bōeishō, 'Kaisetsu: Jieitai Shiki Tsūshin Shisutemutai Kashō no Shinhen' (2007), <http://www.clearing.mod.go.jp/hakusho_data/2007/2007/html/j22c1000.html>.

Bōeishō, 'Heisei 23nen ikō ni Kakawaru Bōeikeikaku no Taikō ni Tsuite' (17 Dec. 2010), <http://www.mod.go.jp/j/approach/agenda/guideline/2011/taikou.pdfpp>.

Bōeishō, *Heisei 24nendo Bōei Yosanan no Gaisan no Gaiyō* (Dec. 2012), <http://www.mod.go.jp/j/yosan/2012/kankei.pdf>.

Bōeishō, 'Heisei 26nen ikō ni Kakawaru Bōeikeikaku no Taikō ni Tsuite' (17 Dec. 2013), <http://www.mod.go.jp/j/approach/agenda/guideline/2014/pdf/20131217.pdf>.

Bōeishō, *Waga Kuni no Bōei to Yosan: Heisei 28nendo Yosan no Gaiyō* (24 Dec. 2015), <http://www.mod.go.jp/j/yosan/2016/yosan.pdf>.

Bōeishōhen, *Bōei Hakusho 2010* (Tokyo: Zaimushō Insatsukyoku 2010).

Bōeishōhen, *Bōei Hakusho 2011* (Tokyo: Zaimushō Insatsukyoku 2011).

Bōeiryoku no Arikata Kentō no Tame no Iinkai, *'Bōeiryoku no Arikata Kentō ni Kansuru Chūkan Hōkoku* (26 Jul. 2012), <http://www.mod.go.jp/j/approach/agenda/guideline/2013_chukan/20130726.pdf>.

Buzan, Barry, Ole Wæver, and Jaap de Wilde, *Security: A New Framework for Analysis* (Boulder CO: Lynne Rienner Publishers 1998), 25.

Cabinet Secretariat, 'Overview of the Act on the Protection of Specially Designated Secrets' (2013) <http://www.cas.go.jp/jp/tokuteihimitsu/gaiyou_en.pdf>.

Department of Defense, *Quadrennial Defense Report* (Feb. 2010), <http://www.defense.gov/Portals/1/features/defenseReviews/QDR/QDR_as_of_29JAN10_1600.pdf>.

Department of Defense, *The DoD Cyber Strategy* (Apr. 2015), <http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf>.

Executive Office of the President of the U.S., *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications* (May 2009), <https://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf>.

Executive Office of the President of the U.S., *International Strategy for Cyberspace Prosperity, Security, and Openness in a Networked World* (May 2011), <https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf>.

Government of Japan, *Cybersecurity Strategy* (4 Sep. 2015), <http://www.nisc.go.jp/eng/pdf/cs-strategy-en.pdf>.

Hughes, Christopher W., *Japan's Reemergence as a "Normal" Military Power* (Oxford: Oxford University Press 2004).

Hughes, Christopher W., *Japan's Remilitarization* (London: Routledge 2009).

Hughes, Christopher W., *Japan's Foreign and Security Policy Under the "Abe Doctrine"* (New York: Palgrave Macmillan 2015).

Information Security Policy Council, *The First National Strategy on Information Security: Toward the Realization of a Trustworthy Society* (2 Feb. 2006), <http://www.nisc.go.jp/eng/pdf/national_strategy_001_eng.pdf>.

Information Security Policy Council, 'Information Security Strategy for Protecting the Nation' (11 May 2010), <http://www.nisc.go.jp/eng/pdf/New_Strategy_English.pdf>.

Information Security Policy Council, 'Information Security 2012' (4 Jul. 2012), <http://www.nisc.go.jp/eng/pdf/is2012_eng.pdf>.

Information Security Policy Council, *Cybersecurity Strategy: Towards a World-Leading, Resilient and Vigorous Cyberspace* (10 Jun. 2013), <http://www.nisc.go.jp/eng/pdf/cybersecuritystrategy-en.pdf>.

Information Security Policy Council Japan, *International Strategy on Cybersecurity Cooperation – j-Initiative for Cybersecurity* (2 Oct. 2013), <http://www.nisc.go.jp/eng/pdf/InternationalStrategyonCybersecurityCooperation_e.pdf>.

IT Strategy Headquarters, 'e-Japan Strategy' (22 Jan. 2001), <http://www.kantei.go.jp/foreign/it/network/0122full_e.html>.

Japan Ministry of Defense, *Defense of Japan 2010* (Tokyo: Urban Connections 2010).

Japan Ministry of Defense, 'Mid-Term Defense Program (FY2011–FY2015)' (17 Dec. 2010), <http://www.mod.go.jp/e/d_act/d_policy/pdf/mid_termFY2011-15.pdf>.

Japan Ministry of Defense, *Toward Stable and Effective Use of Cyberspace* (Sep. 2012), <http://www.mod.go.jp/e/d_act/others/pdf/stable_and_effective_use_cyberspace.pdf>.

Japan Ministry of Defense, *Defense of Japan 2013* (Tokyo: Midiamu Shuppansha 2013).

Japan Ministry of Defense, 'National Program Guidelines for FY2014 and Beyond' (17 Dec. 2013), <http://www.mod.go.jp/j/approach/agenda/guideline/2014/pdf/20131217_e2.pdf>.

Japan Ministry of Defense, 'Medium Term Defense Program (FY2014-FY2018)' (17 Dec. 2013), <http://www.mod.go.jp/j/approach/agenda/guideline/2014/pdf/Defense_Program.pdf>.

Japan Ministry of Defense, 'Joint Statement of the U.S.-Japan Cyber Defense Policy Working Group' (30 May 2015), <http://www.mod.go.jp/j/press/news/2015/05/30a_1.pdf>.

Japanese Ministry of Internal Affairs and Communications, 'Joint Ministerial Statement of the ASEAN-Japan Ministerial Policy Meeting on Cybersecurity Cooperation, Tokyo' (13 Sep. 2013), <http://www.soumu.go.jp/main_content/000249127.pdf>.

Jiyū Minshutō Seisaku Chōkai IT Senryaku Tokubestu Iinkai, *Jōhō Sekyuritī Taisaku ni Kansuru Mōshiire* (28 Oct. 2011), <http://www.jimin.jp/policy/policy_topics/pdf/seisaku-088.pdf>.

Jiyū Minshutō, *Jōhō Sekyuritī ni Kansuru Teigen* (24 Feb. 2012), <https://www.jimin.jp/policy/policy_topics/pdf/seisaku-096.pdf>.

Kallender-Umezu, Paul, 'Japan Takes Action Against Complex Cyber Threats', *Defense News*, 9 Oct. 2012, <http://archive.defensenews.com/article/20121009/C4ISR01/310090010/Japan-Takes-Action-Against-ComplexCyber-Threats>.

Kallender-Umezu, Paul, 'Experts: Japan's new cyber unit understaffed, lacks skills', *Defense News*, 9 Jul. 2013, p. 10.

Kallender, Paul, 'Japan, The Ministry of Defense and Cyber-Security', *The RUSI Journal* 151/1 (2014), 94–103. doi:10.1080/03071847.2014.895264.

Karendā, Pōru, 'Bōeishō to Saibā Sekyuritī ni Kansuru Shinten to Otoshiana', SFC Kenkyūjo Nihon Kenkyū Purattofōm, *Rabowākingu Pēpa Shirīzu*, 8, Dec. 2013, 1–16, <http://jsp.sfc.keio.ac.jp/pdf/wp/jsp-wp_8_Paul%20Kallender.pdf>.

Kawaguchi, Hiroshi, 'Cybersecurity Strategy in Japan, Japan Security Operation Centre' (21 Jan. 2015), <http://staff.cs.kyushu-u.ac.jp/en/event/2015/01/data/17%20kawaguchi.pdf>.

Kawahara, Jumpei, Director for Counter Cyber Attacks, Security Planning Division, Security Bureau, NPA, 'Cyber Attacks Situation and Police Measures,' Presentation to the International Cybersecurity Symposium – Critical Infrastructure Protection towards 2020', Tokyo, 29 Feb. 2016.

Kyodo News, 'At least 2 million sets of personal data feared leaked after cyberattacks in 2015', *The Japan Times*, 3 Jan. 2016, <http://www.japantimes.co.jp/news/2016/01/03/national/least-2-million-sets-personal-data-feared-leaked-cyberattacks-2015/#.VoIMYoR8zzI">.

Lewis, James Andrew, *U.S.-Japan Cooperation in Cybersecurity: A Report of the CSIS Strategic Technologies Program*, CSIS, Washington DC (Nov. 2015), <http://csis.org/files/publication/151105_Lewis_USJapanCyber_Web.pdf>.

Liff, Adam P., 'Japan's Defense Policy: Abe the Evolutionary', *The Washington Quarterly* 38/2 (2015), 79–99. doi:10.1080/0163660X.2015.1064711.

Lind, Jennifer, 'Pacifism or Passing the Buck? Testing Theories of Japanese Security Policy', *International Security* 29/1 (2004), 92–121. doi:10.1162/0162288041762968.

Maslow, Sebastian, 'A Blueprint for a Strong Japan? Abe Shinzō and Japan's Evolving Security System', *Asian Survey* 55/4 (2015), 739–65. doi:10.1525/as.2015.55.4.739.

METI, *Cybersecurity and Economy Study Group Report of August 2011* (Tokyo: Ministry of Economy, Trade and Industry 2011).

Midford, Paul, *Rethinking Japanese Public Opinion and Security: From Pacifism to Realism?* (Stanford, CA: Stanford University Press 2011).

Ministry of Defense Japan, 'Second Japan-U.K. Foreign and Defence Ministerial Meeting 8 January 2016 Joint Statement', 2016 <http://www.mod.go.jp/j/press/youjin/2016/01/08_js_e.pdf>.

Ministry of External Affairs, 'Fact Sheet: India and Japan, Working Together for Peace and Prosperity,' (12 Dec. 2015), <http://www.mea.gov.in/bilateral-documents.htm?dtl/26179/Fact_Sheet_India_and_Japan_Working_Together_for_Peace_and_Prosperity>.

Ministry of Foreign Affairs Japan, 'Japan-EU Relations February 2016', (2016), 3–4, <http://www.mofa.go.jp/files/000033265.pdf>.

Ministry of Foreign Affairs Japan, 'Joint Statement of the Security Consultative Committee. Alliance Transformation: Advancing United States-Japan Security and Defense Cooperation' (1 May 2007), <http://www.mofa.go.jp/region/n-america/us/security/scc/joint0705.html>.

Ministry of Foreign Affairs Japan, 'Joint Statement of the Security Consultative Committee. Toward a Deeper and Broader U.S.-Japan Alliance: Building on Fifty Years of Partnership' (21 Jun. 2011), <http://www.mofa.go.jp/region/n-america/us/security/pdfs/joint1106_01.pdf>.

Ministry of Foreign Affairs Japan, 'Press Conference by Minister for Foreign Affairs Koichiro Gemba' (14 Feb. 2012), <http://www.mofa.go.jp/announce/fm_press/2012/2/0214_01.html>.

Ministry of Foreign Affairs Japan, 'Fact Sheet: U.S.-Japan Cooperative Initiatives' (Apr. 2012), <http://www.mofa.go.jp/region/n-america/us/pmv1204/pdfs/Fact_Sheet_en.pdf>.

Ministry of Foreign Affairs Japan, 'Joint Statement by the Prime Minister of the UK and Japan: A Leading Strategic Partnership for Global Prosperity and Security' (10 Apr. 2012), <http://www.mofa.go.jp/region/europe/uk/joint1204.html>.

Ministry of Foreign Affairs Japan, 'Joint Statement of the Security Consultative Committee. Toward a More Robust Alliance and Greater Shared Responsibilities' (3 Oct. 2013), <http://www.mofa.go.jp/mofaj/files/000016028.pdf>.

Ministry of Foreign Affairs Japan, 'Joint Statement of the Security Consultative Committee. A Stronger Alliance for a Dynamic Security Environment: The New Guidelines for Japan-U.S. Defense Cooperation' (27 Apr. 2015), <http://www.mofa.go.jp/mofaj/files/000078186.pdf>.

Ministry of Foreign Affairs Japan, 'The Guidelines for Japan-U.S. Defense Cooperation' (27 Apr. 2015), <http://www.mofa.go.jp/mofaj/files/000078188.pdf>.

Ministry of Foreign Affairs Japan, 'Japan and India Vision 2025 Special Strategic and Global Partnership: Working Together for Peace and Prosperity of the Indo-Pacific Region and the World' (12 Dec. 2015), <http://www.mofa.go.jp/s_sa/sw/in/page3e_000432.html>.

Ministry of Foreign Affairs Japan, 'Prime Minister Abe and Prime Minister Turnbull Joint Statement "Next Steps of the Special Strategic Partnership: Asia, Pacific and Beyond"' (18 Dec. 2015), <http://www.mofa.go.jp/a_o/ocn/au/page4e_000362.html>.

Nakao, Koji 'Toward Proactive Response Against Cyber-Attacks Based on Global Monitoring and Analysis: PRACTICE Project (Research Part)', 2013 <https://sicherheit.eco.de/wp-content/blogs.dir/27/files/1145_nakao2.pdf>.

Naikaku Kanbō, *Kokka Anzen Hoshō ni Tsuite* (15 Dec. 2013), <http://www.cas.go.jp/jp/siryou/131217anzenhoshou/nss-j.pdf>.

Nakayama, Shozo, 'Govt. Claims Cyberdefense Right/Says International Laws Should be Applied to Computer Infiltration', *Yomiuri Shimbun*, 17 May 2012, <http://news.asiaone.com/print/News/AsiaOne%2BNews/Asia/Story/A1Story20120518-346660.html>.

National Information Security Center, 'Japanese Government Efforts to Address Information Security Issues: Focusing on the Cabinet Secretariat's Efforts' (Nov. 2007), <http://www.nisc.go.jp/eng/pdf/overview_eng.pdf>.

National Information Security Policy Council, *The Second National Strategy on Information Security, Aiming for Strong 'Individual' and 'Society' in IT Age* (3 Feb. 2009), <http://www.nisc.go.jp/eng/pdf/national_strategy_002_eng.pdf>.

National Institute for Defense Studies, *NIDS China Security Report 2014: Diversification of Roles in the People's Liberation Army and People's Armed Police* (Tokyo: National Institute for Defense Studies 2014).

NISC, *Saiba Sekuritī Kihon Hōan no Gaiyō*, 10 Aug 2014, <http://www.nisc.go.jp/conference/seisaku/dai40/pdf/40shiryou0102.pdf>.

OECD, 'Country Statistical Profile: Japan', *OECDi Library*, 28 Feb 2013, <http://www.oecd-ilibrary.org/economics/country-statistical-profile-japan_20752288-table-jpn>.

Oros, Andrew L., *Normalizing Japan: Politics, Identity, and the Evolution of Security Practice* (Stanford CA: Stanford University Press 2008).

Pyle, Kenneth B., *Japan Rising: The Resurgence of Japanese Power and Purpose* (New York: Public Affairs 2007).

Samuels, Richard J., *Securing Japan: Tokyo's Grand Strategy and the Future of East Asia* (Ithaca NY: Cornell University Press 2007).

Subcommittee on Asia and the Pacific of the Committee on Foreign Affairs House of Representatives, *Asia: The Cyber Security Battleground* (Washington DC: Committee on Foreign Affairs House of Representatives 2013), <http://docs.house.gov/meetings/FA/FA05/20130723/101186/HHRG-113-FA05-20130723-SD002.pdf>.

Taipei Times, 'Japanese Navy Officer Arrested for Leaking Secret Data: Police', *AFP*, 13 Dec. 2007, <http://www.taipeitimes.com/News/world/archives/2007/12/14/2003392484>.

Taipei Times, 'Japan Probes Website Attacks Amid Anonymous Claims', *AFP*, 27 Jun. 2012, <http://www.taipeitimes.com/News/world/archives/2012/06/29/2003536553>.

Takahashi, Takeshi, Fujiwara, Hiroyuki and Kadobayashi, Youki, 'Building Ontology of Cybersecurity Operational Information', Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research, Oakridge, TN, 21–23 Apr 2010, 79.

Taniwaki, Yasu, 'Cybersecurity Strategy in Japan', Deputy Director-General NISC (9 Oct. 2014), <http://www.nisc.go.jp/security-site/campaign/ajsympo/pdf/keynotelecture.pdf>.

Tsuchiya, Motohiro, 'Cybersecurity in East Asia: Japan and the 2009 Attacks on South Korea and the United States', in Kim Andreasson (ed.), *Cybersecurity: Public Threats and Responses* (Boca Raton, FL: CRC Press 2012), 55–76.

United States Joint Forces Command, *The Joint Operating Environment (JOE) 2010* (18 Feb. 2010), <http://fas.org/man/eprint/joe2010.pdf>.

U.S. Department of State, 'Joint Statement on U.S.-Japan Cyber Dialogue' (10 May 2013), <http://www.state.gov/r/pa/prs/ps/2013/05/209238.htm>.

U.S. Department of State, 'The 4th U.S.-Japan Bilateral Cyber Dialogue' (27 Jul. 2016), <http://www.state.gov/r/pa/prs/ps/2016/07/260572.htm>.

Yamada, Yasuhide, Yamagishi, Atsuhiro and Katsumi, Ben T., 'Comparative Study of the Information Security Policies of Japan and the United States', *Journal of National Security Law & Policy* 4 (2010), 217–32, <http://jnslp.com/wp-content/uploads/2010/08/14_Yamada.pdf>.