BASC WORKING PAPER SERIES

GOVERNMENT AS FACILITATOR: HOW JAPAN IS BUILDING ITS CYBERSECURITY MARKET

Benjamin Bartlett

Working Paper 2018-06

BERKELEY APEC STUDY CENTER
552 Barrows Hall
University of California
Berkeley, California 94720-1950
September 2018

This paper is part of a project "Comparative Industrial Policy in the Cyber Security Industry: Policies, Drivers, and International Implications," organized by Vinod K. Aggarwal and Andrew Reddie of the Berkeley APEC Study Center and funded by the Center for Long-Term Cybersecurity at the University of California, Berkeley. I'd like to thank the Center for Japanese Studies for research support as well as the Center for Long-Term Cybersecurity, the Institute on Global Conflict and Cooperation, and BASC for convening this project. My thanks also to Prof. Vinod Aggarwal, Prof. Steve Vogel, Prof. Barry Naughton, and Andrew Reddie for comments on previous drafts.

Government as Facilitator: How Japan is Building its Cybersecurity Market
Benjamin Bartlett
BASC Working Paper 2018-06

Benjamin Bartlett[1]
University of California, Berkeley
Department of Political Science
210 Barrows Hall
Berkeley, CA 94720
bartlbe@berkeley.edu

[1] Benjamin Bartlett is a Ph.D. candidate in the Charles & Louise Travers Department of Political Science at the University of California, Berkeley.He specializes in East Asian security, particularly Japanese security policy.He has been a fellow of the Japan Society for the Promotion of Science, and a Waseda University Visiting Junior Research Fellow. He holds a B.A. in computer science from Earlham College, and an M.Sc. in computer science from the University of Toronto.

1. Introduction

Japan is a country with a long history of active industrial policy and a heavy focus on high-technology sectors. Though its industrial policy efforts have slowed in recent years, both due to economic stagnation and the fact that it has "caught up" to other advanced industrial economies, its recent efforts in building up its space sector demonstrates that the government is still capable of bringing forth industrial policy.[2] Nevertheless, it has been surprisingly inactive in building a domestic cyber security sector. This is not to say, however, that it has no industrial policy aimed toward cyber security. Instead, its industrial policy is aimed primarily at improving the cyber security of related sectors, such as telecommunications and manufacturing, the latter having become a related sector with the development of the "Internet of Things".

While geopolitical factors, such as the rising threat of cyber-attacks from abroad, have been a driver for the Japanese government's increased focus on cyber security, the particular measures used to promote cyber security have been primarily determined by domestic factors. Because the Ministry of Internal Affairs and Communications and the Ministry of Economy, Trade and Industry have played large roles in developing cyber security policy in Japan, policies have been relatively business-friendly, aimed at creating a secure business environment and reassuring the public that the internet is a safe place to do business. Meanwhile, demand from the private sector is for more security, rather than for the promotion of Japanese cyber security products. The Japanese government has had to balance this demand to "do more" with its own desire to encourage private firms to invest more heavily in security themselves.

This paper explores Japan's industrial policy toward cyber security. I begin by describing the perceived market failures with regard to cyber security, and the Japanese government's rationales for intervention. Next, I briefly describe the institutions involved in Japan's cyber security policy-making. I follow by discussing three models of Japanese intervention: *government as provider*, *government as facilitator*, and *government as promoter*. Then, I examine the factors that have led to this particular constellation of measures. Finally, I look at the effectiveness of these measures as well as make some concluding remarks about likely future trends.

2. Market Failures

The primary market failure the Japanese government is concerned with is under-investment in cyber security by the private sector. While in one sense this is a similar problem to the one faced by the U.S.[3], the underlying causes are different. In the U.S., this under-investment in cyber security reflects the incentives of the IT market, which rewards rapid innovation and release of products over security.[4] In contrast, Japan's IT sector has and continues to focus on releasing "good" rather than "innovative" code. The U.S. has moved increasingly towards an agile approach to code-writing, where programs

[2] Pekkanen and Kallender-Umezu 2010.

[3] Aggarwal and Reddie 2018, US Chapter

[4] Cite Aggarwal and Reddie US Case

are released quickly with the expectation that problems will arise after release, and new versions that solve those problems will be rapidly created and released.. By contrast, the Japanese IT industry still relies heavily on the "waterfall" method, which places a heavy emphasis on planning and quality control before release.[5] Arguably this has been part of the explanation for Japan's relatively uncompetitive software industry[6], but has led to a lower rate of bugs.[7]

The problem is thus not a focus on rapid innovation and release of software. Instead, this trend of under-investment is driven by three factors. First, compared to firms in many other countries, Japanese firms have relatively low awareness of cyber security threats. According to the Risk Management Survey Report 2015, conducted by Tokio Marine Nichido, only 52.5% of firms viewed information security as a priority risk.[8] In contrast, a survey of American companies by Willis Towers Watson found that 85% of respondents answered that cyber security was a top priority for their firm.[9] Likewise, KPMG's Cybersecurity Surveys from 2013 to 2016 found that, while the ratio of Japanese companies that believe cyber security issues should be discussed at the board level had increased, it was still much lower than the rate overseas (68% versus 88% in 2016).[10] There are a number of possible reasons for this. Japanese is a relatively difficult language for non-native speakers and thus a less hospitable medium for phishing attacks, which could lead to less of a fear of such attacks. Alternatively, it could be because firms are situated within a high-trust society where the notion that there exist "bad actors" that would try to break into networks is still relatively foreign.[11] Regardless of the reason, the fact remains that awareness of cyber risks remains quite low.

Secondly, some tools that aid in improving cyber security, such as information sharing, open Japanese firms up to reputational risks. Information sharing involves some sort of arrangement whereby firms let other firms (and possibly the government) know when they have been attacked and the nature of that attack. The idea is that then the other firms can be better prepared for attacks of a similar nature. In some cases, information about how to prevent similar attacks may be included.

Of course, the problem is that in order to let other firms know about an attack, a firm reveals that it has been breached. This is not only potentially embarrassing, but can harm the stock value of the company, driving away investment. Though information sharing arrangements often include anonymization techniques, the firm must believe that these

---

[5]Author's interview with Hideki Matsuoka, Oracle Japan, formerly Maritime Self-Defense Forces, Tokyo, January 2017. All opinions expressed are Matsuoka's own, and do not reflect those of Oracle Japan or the Self-Defense Forces.

[6] Cole and Nakata 2014.

[7] Though the data is a little old, research by Michael Cusumano of MIT, released in 2004, showed that the average rate of bugs found per 1000 lines of code per year for Japanese software was 0.02; by contrast, for American software, the rate was 0.225, over ten times as many. Kibashiri 2007.

[8]Tokio Marine Nichido 2015.

[9]Willis Towers Watson 2017.

[10]Kriz and Matsubara 2016.

[11]Interview with NISC official, Tokyo, July 2017.

techniques work. Furthermore, even if the techniques do work, within the information sharing institution there will be those who know the firm's true identity, individuals who must be trusted not to leak the information.

In short, information sharing is a classic collective action problem. Though all firms would be better off if they shared information, any given firm increases its risks of harming its reputation by doing so. It has thus been very difficult to get Japanese firms to agree to information-sharing schemes, particularly since they are worried that the institution in charge of information-sharing will leak that they have been the victim of a cyber attack.[12]

Third, it is difficult for firms to know what the risk of cyber attack is, or to understand to what degree an investment in cyber security ameliorates that risk. In short, cyber risk management is hard, and it is difficult for firms to know where to invest their money; at the same time, firms cannot simply invest endlessly in cyber security.[13] Since the upfront costs are obvious and the potential risks are not, there is a tendency for firms to under-invest.

The firms themselves are aware of this problem. As a result, one of their major demands is for the government to provide a fixed set of cyber security requirements that would allow firms to know when they were "doing enough". For reasons that will be explained later in this paper, the government has been unwilling to meet this demand.[14]

Another area of market failure relates to adjustment failure. In particular, there is a large gap between the number of cyber security jobs and the available workforce: in 2015, there were 80 thousand unfilled information security jobs. Even worse is the fact that the existing labor force is under-skilled; out of 265 thousand information security employees, 160 thousand (60%) lacked the appropriate skills for their position.[15] In an earlier survey, 73% of firms reported that they did not have enough specialists in research and development.[16]

3. Japan's Rationales for Government Intervention

The Japanese government's rationales for intervention include the risks it poses to economic and public security created by the market failures described above. We can see this rationale echoed in the first three basic principles listed in the third act of the Cybersecurity Basic Law, passed in 2014. Along with establishing the Cyber Security

---

[12] Author's interviews with employee of JPCERT/CC, METI official, employee of Tokio Marine Nichido, Tokyo, Summer 2017.

[13] Author's interviews with Masaki Ishiguro, Mitsubishi Research Institute, Tokyo, January 2017, and with Tokio Marine Nichido employee, Tokyo, August 2017.

[14] Author's interviews with Masaki Ishiguro, Mitsubishi Research Institute, Tokyo, January 2017, and with METI official, Tokyo, August 2017.

[15] Roth 2016.

[16] IPA 2011, 29.

Strategic Headquarters, and re-establishing NISC as the CSSHQ's secretariat, the Basic Law sets the legal basis for Japan's industrial policy.

Article 3 (1) Given that ensuring the free flow of information through maintaining the Internet and other advanced information and telecommunications networks, the utilization of information and telecommunications technologies are critical to enjoying benefits through the freedom of expression, enabling the creation of innovation, improving economic and social vitality, and so forth, the promotion of the Cybersecurity policy must be carried out with the intent to produce active responses to threats against Cybersecurity through coordination among multiple stakeholders, including the national government, local governments, and critical information infrastructure CII Operators (referring to operators of businesses that provide infrastructure which is the foundation of the people's living conditions and economic activities and the functional failure or deterioration of which would risk enormous impacts to them; hereinafter, the same is to apply).

(2) The promotion of the Cybersecurity policy must be carried out with the intent to raise awareness to each member of the public about Cybersecurity and encourage each member of the public to take voluntary actions to prevent any damage caused by threats against Cybersecurity, and to positively promote actions to establish resilient systems which can quickly recover from damage or failure.

(3) The policy to promote Cybersecurity must proactively be carried out with the intent to implement on maintaining the Internet and other advanced information, telecommunications networks and actions toward the establishment of a vital economy and society through the utilization of information and telecommunications technologies.[17]

Several specific concerns underlie these basic rationales. The first major concern is the security and economic threat posed by cyber-attacks on critical infrastructure, concern over which has heightened in anticipation of the 2020 Olympics. Thirteen sectors are classified as "critical infrastructure": telecommunications, finance, aviation, rail, electricity, gas, government/administrative services (including regional services), medical services, water, transport, chemicals, credit, and oil.[18]

[17] "Japanese Law Translation - [Law Text] - the Basic Act on Cybersecurity" 2015.

[18] NISC 2016b, 10. Author's interviews with Masaki Ishiguro, Mitsubishi Research Institute, and Kousuke Ito, Connected Consumer Device Security Council, Tokyo, January 2017.

A second major concern is protecting individual information. In part, this is a genuine concern over citizen safety, but it is also partly driven by the worry that should the public come to see the internet as "unsafe", they would refuse to use internet-based services, and this would hurt Japan's competitiveness.[19]

A third major concern is securing products created by internet-adjacent firms, such as self-driving cars and internet-connected consumer devices from attack.[20] The government fears that compromises of these devices could turn consumers away from Japanese products; in contrast, a good safety record could provide Japan with a competitive advantage. This also, of course, receives a lot of attention because it touches on a number of sectors in Japan's economy, rather than just the software sector. One measure of how important this particular area is to the government is that MIC and METI have created a joint working group to write security guidelines for IoT, along with the IoT Acceleration Consortium.[21]

Though Japan has not yet acted upon it (for the most part), the Cybersecurity Basic Law provides justification for more traditional sector-promoting industrial policy as well:

Article 19　Given that it is critical for Japan to have self-reliant capabilities to ensure Cybersecurity, and in order to create new business opportunities, develop sound businesses, and improve international competitiveness, and so as to make the Cybersecurity sector a "growth industry" which is able to create employment opportunities, the national government is to provide necessary measures related to Cybersecurity, including the promotion of advanced research and development, technological advancements, the development and recruitment of human resources, the strengthening of the market environment and the development of new businesses through the improvement of competitive conditions, and the internationalization of technological safety and reliability standards and the participation in such frameworks on the basis of mutual recognition.

Article 20　Given that it is critical for Japan to maintain self-reliant technological Cybersecurity capabilities, in order to promote research and development for Cybersecurity as well as the technological and other relevant demonstrations of Cybersecurity, and to expand the distribution of relevant Cybersecurity outcomes, the national government is to provide necessary measures related to Cybersecurity for: the improvement of the environment of Cybersecurity research; the promotion of basic research on technological safety and reliability as well as the promotion of research and development for core technologies; the development of skilled researchers and engineers; the strengthening of

[19] Author's interview with former METI official, Tokyo, June 2017.

[20] NISC 2016b. Author's interview with Kousuke Ito, Connected Consumer Device Security Council, Tokyo, January 2017.

[21] "IoT Security Guidelines Ver. 1.0 Formulated（METI）" 2017.

coordination among national research institutes, universities, the private sector, and other relevant parties; and international coordination for research and development.

Article 21 (1) In close coordination and cooperation with universities, colleges of technology, technical schools, private enterprises, and other relevant entities, the national government is to provide necessary measures to ensure appropriate assignments and employment conditions or treatment of the workforce in the field of Cybersecurity, thereby enabling their functions and work environments to become attractive enough to meet their professional values. (2) In close coordination and cooperation with universities, technical schools, specialized training colleges, private enterprises, and other relevant entities, for the purposes of recruitment, development, and quality improvement of Cybersecurity-related human resources, the national government is to provide necessary measures, including the utilization of a qualification scheme and training of young technical experts.[22]

This suggests that while we do not see a particularly strong effort to promote the cyber security sector at the present time, this could change in the future.

4. Institutions Involved in Cyber Security Policy-making

[22] "Japanese Law Translation - [Law Text] - the Basic Act on Cybersecurity" 2015.

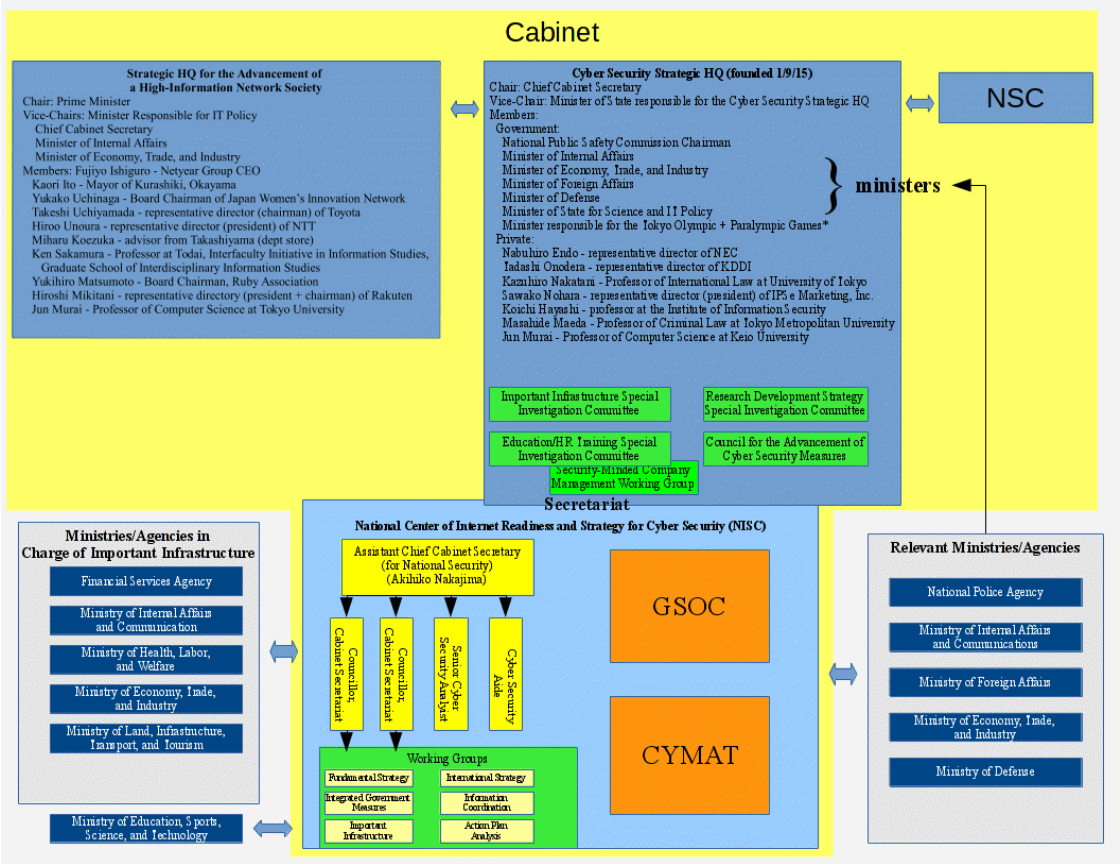

Figure 1: Japan's governmental cyber security policy-making structure

Though I will discuss how government preferences affect Japan's cyber security industrial policy later in the paper, for the benefit of the reader I will briefly describe the government bodies involved in the creation of cyber security policy in Japan. The most important institutions are the Cyber Security Strategic Headquarters, National center of Incident readiness and Strategy for Cybersecurity (NISC), the Ministry of Internal Affairs and Communications (MIC), the Ministry of Economy, Trade and Industry (METI), the National Police Agency (NPA), and the Ministry of Defense (MOD).

Along with discussing their role in developing Japan's cyber security policy, I will also mention the role each actor has to play in implementing those non-tariff measures identified by UNCTAD.[23] In truth, Japan only pursues one of these types of measures with regard to cyber security: subsidies. Along with the actors mentioned above, this requires the introduction of the Ministry of Finance (MOF), which is in charge of fiscal policy for the government, and the Ministry of Education, Culture, Sports, Science and Technology (MEXT) which provides research and development funding.

4.1 Cyber Security Strategic HQ and NISC

[23] UNCTAD 2012.

The Cyber Security Strategic Headquarters, founded on January 9th, 2015, sits within the Cabinet Office and first met on February 2, 2015.[24] It replaced the Information Security Policy Council, which was located under the Strategic Headquarters for the Advancement of a High-Information Network Society. It is chaired by the Chief Cabinet Secretary, with the Minister of State responsible for the Cyber Security Strategic Headquarters serving as vice-chair. It has the heads of four ministries as members, along with the National Public Safety Commission Chairman, who heads the National Police Agency: the Minister of Internal Affairs; the Minister of Economy, Trade, and Industry; the Minister of Defense; and, in a change from the Information Security Policy Council, the Minister of Foreign Affairs. Two other ministers not associated with a particular ministry or agency are also members: the Minister of State for Science and IT Policy (who also serves as one of the Vice-Chairs for the Strategic Headquarters for the Advancement of a High-Information Society) and the Minister responsible for the Tokyo Olympic and Paralympic Games[25]. There are also seven members from academia and industry, one more than had been on the Information Security Policy Council.[26]

According to the Basic Cyber Security Law, the Cyber Security Strategic Headquarters has several responsibilities. It oversees creating and promoting the implementation of cyber security strategies. It is responsible for evaluating cyber security plans regarding government bodies, independent administrative agencies, and designated corporations, based on standards it has developed as well as other appropriate standards, and for promoting policy implementation based on these other appropriate standards. It evaluates measures taken by administrative bodies, independent administrative organizations, and designated corporations to respond to major cyber security incidents, including investigating to determine the cause of such incidents. Additionally, the Cyber Security Strategic Headquarters is responsible for developing plans for and evaluating the implementation of policies for estimating the cyber-security-related expenses of related administrative organizations and is responsible for promoting the implementation and coordination of other appropriate policy measures.[27]

Among its other duties, the Cyber Security Strategic Headquarters prepares the Cyber Security Strategy Plan for the Japanese government, though it does so in consultation with the Strategic Headquarters for the Advancement of a High-Information Network Society and the National Security Council. In other areas as well, the Cyber Security Strategic Headquarters works closely with these other two cabinet bodies.[28]

Though founded in April 2005, much earlier than the Cyber Security Strategic Headquarters, the National center of Internet readiness and Strategy for Cybersecurity (NISC) currently serves as its secretariat. NISC has several duties assigned to it by the

[24]NISC 2016b; “サイバーセキュリティ戦略本部　第1回会合　議事概要” 2015.

[25]Although this has consistently been the same person as the Minister of State responsible for the Cyber Security Strategic Headquarters, which means there is one less member than one would expect.

[26] NISC 2016a; Masuoka and Ishino 2012.

[27] “サイバーセキュリティ基本法” 2016.

[28]“サイバーセキュリティ基本法” 2016.

Cabinet Secretariat. First, it is to monitor and analyze any illegal activities targeting information transmission networks as well as the information systems of any administrative organs which transmit data via electromagnetic storage media. Second, it is to investigate the causes of any major hindrances or potential hindrances to the cyber security of administrative organs, with the exception of those organs managed by the Cabinet Information Research Division. Third, it is to provide necessary advice related to ensuring the cyber security of administrative organs, as well as offering information and other forms of support. Fourth, it is to provide any audits necessary to ensuring the cyber security of administrative organs. Finally, it is responsible for activities involving plans or strategies necessary to maintaining integrated planning and implementation for administrative organs, as well as integrated regulation regarding cyber security, excluding those activities already managed by the National Security Council, the Cabinet Public Relations Office, and the Cabinet Information Research Office.[29]

Although most of its duties apply to the maintenance of the Japanese government's cyber security system, it is through this last duty that NISC plays a role in cyber security policy-making. It contains a number of working groups which bring together relevant actors from both inside and outside government in order to make policy decisions relevant to cyber security.

4.2 MIC and NICT

The Ministry of Internal Affairs and Communications (MIC) has roughly three major spheres of responsibility: (1) it is in charge of administration, particularly local administration; (2) it is in charge of information and communications technology; and (3) it is responsible for producing statistics related to socioeconomic and civic life in Japan.[30] Its involvement in cyber security policy-making primarily derives from the second of these responsibilities[31], but it is also involved through its role in administration and local administration, particularly in terms of securing critical infrastructure. Recently, the Minister of Internal Affairs and Communications announced plans to establish a bureau dedicated to cyber security within the ministry.[32]

The National Institute of Information and Communications Technology (NICT) is an incorporated administrative agency associated with the MIC. It promotes research in information technology and forms ties with and between academia and businesses.[33] NICT contains a number of research institutes involved with research and development of information and communications technology. Particularly relevant is the Cybersecurity Research Institute. This institute conducts research and development on cyber attack monitoring, automatic cyber attack counter-measures, security test bed development[34],

---

[29] 内閣官房 2017.

[30] "Ministry of Internal Affairs and Communications" 2017.

[31] Author's interview with Masaki Ishiguro, Mitsubishi Research Institute, Tokyo, January 2017.

[32] Nikkei 2017.

[33] "About NICT NICT Charter NICT-National Institute of Information and Communications Technology" 2017.

[34] That is, creating environments in which cyber-attacks can be safely replicated and counter-measures tested.

cryptographic technologies, and privacy protection technologies.[35] NICT also runs the Cryptographic Protocol Verification Portal, which publishes the results of verification tests on various cryptographic protocols, so that engineers can quickly check to make certain a given protocol does not have any known vulnerabilities.[36] MIC subsidizes cyber security R&D through NICT, and has also lobbied MOF for tax measures to help subsidize cyber security.

4.3 METI and IPA

As the name would suggest, the Ministry of Economy, Trade and Industry is responsible for policies regarding most Japanese firms as well as for trade policy. Its responsibilities touch on the cyber security sector in both direct and indirect ways: direct through its role in making industrial technology and information policy, and indirect through its role in promoting small and medium enterprises.[37] It is also in charge of utilities, such as gas and electricity, and thus has a large role to play in the securing of important infrastructure.[38]

METI oversees and provides funds for a number of projects both directly or indirectly related to cyber security. One of its projects is to build cyber security economic infrastructure which it funded in FY 2016 for 2.16 billion yen. Under the 2015 supplementary budget, it also spent 0.45 billion yen on a project for accelerating cyber security measures for citizens and enterprises, and another 0.4 billion yen on strengthening cyber security measures for critical infrastructure.[39]

Much like MIC has NICT, METI also has its own incorporated administrative agency that deals with cyber security (among other issues): the Information-Technology Promotion Association (IPA). IPA is responsible for certifying that products meet cyber security standards, as well as for verifying the security of cryptographic products. It is also responsible for collecting and sharing information related to cyber security trends and threats; it shares this information with government, business, and the public. METI's FY2016 budget included 4.25 billion yen in operational grants for IPA.[40] METI subsidizes R&D through IPA and other institutions, and also has lobbied MOF for tax measures aimed at subsidizing cyber security.

4.4 Ministry of Defense

Despite being involved in negotiations which led to the first Information Security Strategy,the establishment of NISC and the Information Security Policy Council, and its ongoing role in NISC and the Cyber Security Strategic Headquarters, the Ministry of Defense has not played much of a role in industrial policy. This may change, however, as the Ministry of Defense has recently been given funding to deal with cyber security.[41] In

---

[35] "Cybersecurity Research Institute NICT-National Institute of Information and Communications Technology" 2017.
[36] "Cryptographic Protocol Verification Portal (CPVP)" 2017.
[37] "Organization Chart/METI Ministry of Economy, Trade and Industry" 2017.
[38] Author's interview with Masaki Ishiguro, Mitsubishi Research Institute, Tokyo, January 2017.
[39] METI 2016.
[40] METI 2016.
[41] Author's interview with Masaki Ishiguro, Mitsubishi Research Institute, January 2017.

2014, the Ministry of Defense established the Cyber Defense Unit, which monitors the networks of the Ministry of Defense and the Self-Defense Forces, as well as conducts research on cyber threat information.[42] Potentially, this could lead to more procurement of domestic cyber security technology in the future.

4.5 National Police Agency

Like the MOD, the National Police Agency has not been especially involved in industrial policy. It has, however, clashed with MIC over its preferred policies with regard to traffic data storage requirements for ISPs and telecommunications carriers. The NPA wishes for the data to be stored by the ISPs and carriers so that it can be used to track down cyber criminals. Along with legal concerns, MIC worries that this would pose an undue burden on ISPs and carriers.[43]

Again, like the MOD, the NPA has recently been improving its cyber security capabilities. For example, it recently created the Cyber Force in order to support criminal investigations into cyber terrorism and related crimes.[44] This could lead it to become more heavily involved in industrial policy in the future, particularly through procurement policies.

4.6 MOF

Though not as directly involved in cyber security policy-making as the actors listed above, the Ministry of Finance does play a role in subsidizing cyber security through its Tax Bureau, which drafts Japan's national tax policies. It also determines the budgets of other ministries through its Budget Bureau, and is thus indirectly responsible for R&D funds.[45]

4.7 MEXT

Perhaps surprisingly, given its title, the Ministry of Education, Sports, Science and Technology does not play a direct role in setting cyber security policy. It is, however, in charge of universities, university-industry cooperation, and science and technology promotion, and so plays a role in subsidizing research and development for cyber security.[46]

5. Japan's Cyber Security Industrial Policy

Tokyo uses a variety of measures to overcome the aforementioned market failures. These measures can be grouped under three models, each representing a different general approach to dealing with the problem. The first model is *government as provider*. Under

[42] Ministry of Defense 2014.

[43] Author's interview with MIC official, Tokyo, July 2017.

[44] National Police Agency 2017.

[45] MOF n.d. It is also worth noting that MOF is the responsible authority for the financial system, and so banks and other financial firms report cyber security attacks to it.

[46] MEXT n.d.

this model, the Japanese government directly invests in and promotes cyber security. The second model is *government as facilitator*. With this set of measures, the government seeks to help firms overcome information and coordination problems by providing a variety of institutions to promote cooperation and information-sharing between firms. The third model is *government as promoter*. With this set of measures, the government provides guidance and incentives to encourage private investment in cyber security.

Following Harris and Carman, interventions can fall into five categories: *market creating*, *market facilitating*, *market modifying*, *market substituting*, and *market proscribing*. Market-creating policies establish rights, incentives, and opportunities for exchange. Market-facilitating policies improve the operation of markets by reducing transaction costs, strengthening incentives, or internalizing benefits and costs. Market-modifying policies seek to produce outcomes different from those that would be otherwise produced by the market. Market-substituting policies replace the function of the market with instruments of political authority. Market-proscribing policies prohibit exchanges by particular actors or of particular objects.[47]

5.1 Government as Provider

One of the Japanese government's responses to under-investment in cyber security has been to directly invest in Japan's cyber security capabilities. This includes programs to remove malware and bots from Japanese computers as well as raising public awareness campaigns in an effort to improve Japanese citizens' cyber security practices. The government has also created several training programs meant to increase the number of skilled cyber security workers.

5.1.1 Malware and Bot Removal Programs [Market Substituting]

The Japanese government has invested in technologies to remove malware and bots from Japanese users' computers. The most well-known of these efforts was the Cyber Clean Center. Running from December 2006 until March 2011, this was a joint effort by Telecom-ISAC Japan, the information and analysis center for Japan's telecommunications sector; JPCERT/CC, Japan's Computer Security and Incident Response Team; and IPA, with the support of the Ministry of Economy, Trade and Industry, and the Ministry of Internal Affairs and Communications. The Center would detect and analyze bots, then create tools to remove them from infected computers. It also monitored the Japanese internet, and upon detecting a bot coming from a certain IP address, would then send a notice to the appropriate Internet Service Provider (ISP). The ISP would then forward this notice to the user associated with the IP address, along with instructions to go to the Cyber Clean Center website and download the tool to remove the bot.[48]

The creation of the Cyber Clean Center came out of discussions between the government, groups like JPCERT/CC, and firms in the telecommunications sector. While the firms all agreed that bots were becoming a major problem for the functioning of Japan's internet, and that some sort of joint effort to remove the bots was called for, but in a classic

[47] Harris and Carman 1984.
[48] Telecom-ISAC 2017; Arimura 2008; Brian Krebs 2010.

example of a collective action problem, none of the companies were willing to pay for it. In the end, the effort was funded entirely by the Japanese government.[49]

Along with the Cyber Clean Center, the Japanese government has also pursued more ad-hoc measures to deal with malware. For example, there was an incident in which malware was infecting Japanese users' computers and sending information from that computer to external servers. The Japanese police managed to take over one of these servers. When the malware attempted to send information from a user's computer to the server the police had taken over, the user would receive a notice that their computer had been infected, along with instructions as to how to remove the malware.[50]

Currently, the government is becoming increasingly concerned with the spread of bots across the Internet of Things. For example, the Mirai worm, which infected a large number of IoT devices and turned them into bots with which DDOS attacks could be launched, has alarmed the government. As a result, there are plans to create something akin to the Cyber Clean Center, this time with a focus on removing bots from IoT devices.[51]

5.1.2 Public Awareness Campaigns [Market Creating; Market Facilitating]

[49] Author's interview with employee of JPCERT/CC, Tokyo, August 2017.
[50] Author's interview with National Police Agency official, Tokyo, July 2017.
[51] Author's interviews with employee of JPCERT/CC, Tokyo, August 2017, and NISC official, January 2018.

Figure 2: Photo of a cyber-security-awareness poster in Harajuku, Tokyo. Text: "Such a simple password... does not suit you."

The Japanese government does not just pursue technical approaches to improving Japan's cyber security. Rather, in recognition of the poor security practices on the part of users leaving Japan's networks vulnerable, Tokyo has applied a great deal of effort into raising public awareness and education about cyber security issues. This is done through a variety of programs, such as advertisements on billboards and on the web, as well as school programs meant to teach children basic cyber security skills. Though several agencies now play a role in this, initial efforts to better educate the public were spearheaded by the Ministry of Internal Affairs and Communications. This policy's implementation stemmed from the ministry's worry that Japanese consumers were hesitant to use the internet due to concerns that it was unsafe. This would hurt the Japanese economy relative to other countries whose firms could take advantage of the efficiencies created by the internet. Thus, MIC hoped that by better educating the public about how to be safe while using the internet, Japanese consumers would become more willing to use internet-based services.[52]

One of the government's major efforts to promote cyber security awareness among the public is its "Information Security Month"[53], established in 2009. Taking place in February, during this month the government distributes stickers, posters, and web banners about cyber security. Government websites are also altered to include the government's message about cyber security, and messages about cyber security are also broadcast over its streaming station.[54]

Various government bodies have also set up web sites aimed at improving public awareness of cyber security issues and teaching them about effective cyber security measures. For example, NISC has created the "Information Security Site for the Protection of Citizens"[55], on which it publishes teaching materials. MIC also publishes information about cyber security through its site, "Information Security Site for

[52]Author's interview with former METI official, Tokyo, June 2017.
[53]情報セキュリティ月間
[54]情報セキュリティ政策会議 (Information Security Policy Council) 2014, 13.
[55]国民を守る情報セキュリティサイト

Citizens"[56]. Likewise, IPA publishes easy-to-understand materials on cyber security and offers teaching materials on its (more-creatively-named) site, "From Here, Security!"[57] As part of these initiatives, the government has been encouraging cooperation between the various agencies hosting these sites to cross-link between each other's' sites.[58]

The government has also been working with creators of pop media, such as music and comics, to promote cyber security.[59] It has had several cross-promotional efforts with anime series: *Ghost in the Shell*, *Sword Art Online*, and *Beatless*, all of which have sci-fi themes with a heavy focus on information technology. These efforts have included not just posters featuring the characters and cyber-security safety messages, but also events with directors, voice actors, and costumed characters. The government has also used more traditional methods for getting its message across to the public, such as ads in magazines and video ads on trains.[60]

The government also works to educate the public specifically on cybercrime. Efforts have included short courses mixing information about cybercrime in general with information about specific cases; information about common cybercrime tactics and counter-measures posted to government websites; and plans to encourage "cyber-crime prevention volunteers". The government has also released pamphlets on cybercrime, including pamphlets aimed specifically at middle and high school students warning of crimes involving dating sites.[61]

Beyond efforts aimed at the general public, there have been a number of measures aimed specifically at improving cyber education for primary and secondary school students. Some of these measures, such as education in "information morals" and cyber security poster or slogan competitions, are targeted primarily at students. Others, such as symposia on cyber security and the posting of educational materials from the government, academia, and private industry on NISC's information security site are aimed at educators and guardians.[62]

Though the primary aim of these efforts is to improve public security, these efforts help Japanese firms as well since they help teach both their employees and their customers better security practices. Weak passwords and unprepared employees are as much of a threat to a company as is unpatched or misconfigured software.

5.1.3 Training Programs [Market Facilitating]

[56]国民のための情報セキュリティサイト
[57]これからセキュリティ！
[58]情報セキュリティ政策会議 (Information Security Policy Council) 2014, 16.
[59]情報セキュリティ政策会議 (Information Security Policy Council) 2014, 17.
[60]情報セキュリティ政策会議 (Information Security Policy Council) 2014, 17.
[61]情報セキュリティ政策会議 (Information Security Policy Council) 2014, 17.
[62]情報セキュリティ政策会議 (Information Security Policy Council) 2014, 18–19.

Beyond directly investing in the public provision of cyber security, the government also has many initiatives meant to increase the number of cyber security workers. Two of these programs are run by the Information-Technology Promotion Association: the Exploratory IT Human Resources Project, which seeks to find and train potential innovators in the IT field; and the Security Camp, a training program that teaches students about cyber security tools and techniques, and encourages them to enter the field of cyber security.[63]

The Ministry of Internal Affairs and Communications has requested 3.51 billion yen in 2017 to build a National Cyber Training Center. This training center would focus on training national and local administrative personnel, as well as those personnel associated with important infrastructure, to deal with cyber-attacks. It would also generate human resources specifically to deal with cyber issues surrounding the 2020 Olympics, as well as train young people in cyber security more generally.[64] Additionally, the Ministry of Education, Culture, Sports, Science and Technology (MEXT) which has requested 450 million yen for funds to grant to universities and technical schools to promote cyber security education, and the National Police Agency has requested 870 million yen for its own cyber security human resources development program.[65] These three programs accounted for about 8% of the proposed 2017 cyber security budget.[66]

5.2 Government as Facilitator

The government acts as a facilitator between firms (and between firms and academia) in three ways. First, it includes firms in various policy advisory councils and working groups within the government. Second, it works with semi-public and private organizations to promote information sharing between firms. Finally, through semi-public organizations, it helps to fund and coordinate joint research and development efforts.

5.2.1 Policy Consultation [Market Facilitating]

As can be seen in Figure 1, the Cabinet Office contains a number of bodies and working groups devoted to various aspects of cyber security. Each of these bodies and working groups have as members representatives from the private sector. For example, the Cyber Security Strategic Headquarters includes as members the representative directors of NEC, a provider of information technology products and services; KDDI, a telecommunications operator; and IPSe Marketing, Inc., an IT consulting company.[67] While the main purpose of these bodies and working groups is to provide advice and input to the government, it also allows the government to coordinate policy with and between the firms belonging to these bodies. Informal coordination between industries and their responsible ministries (for example, between the telecommunications industry and MIC) also occurs.

---

[63] "IPA Information-Technology Promotion Agency, Japan: IPA: Business Outline" 2017.

[64] NISC 2017, 4.

[65] NISC 2017, 1.

[66] NISC 2017, 9. The Ministry of Health, Labor and Welfare also has a program for developing human resources related to cyber security, but it is not clear how much money is budgeted to this.

[67] NISC 2016a.

5.2.2 Information-Sharing Promotion [Market Substituting]

Along with receiving input on cyber security policy, the government has also invested a great deal of effort into promoting information sharing between firms. For some types of firms this is a requirement: firms that fall under critical infrastructure sectors are required to report any cyber security incidents to their responsible ministries. There is currently a debate over whether this should be further centralized, with the information from all critical sector firms going to NISC.[68]

To further encourage information sharing about cyber threats between those firms for which it is not a requirement, the Japanese government works with semi-public and private organizations to promote information sharing between firms. Though a number of such organizations exist, two of the most important are JPCERT/CC, which works with METI, and ICT-ISAC, which works with MIC.

JPCERT/CC is an association of network security providers and security vendors. Founded in 1996 as a volunteer organization, it now has around 80 permanent staff. It joined the global Forum of Incident Response and Security Teams (FIRST) in 1998.[69] Though JPCERT/CC receives funding from METI, it is a private organization.[70] JPCERT/CC serves several functions. It actively monitors the internet for threats. After analyzing any threats it may detect, it transmits this information to its constituents. It functions as a Computer Security Incident Response Team (CSIRT). Constituents who believe they have been the victim of a cyber-attack can contact JPCERT/CC. JPCERT/CC then analyzes the attack and investigates its source, works to limit the damage caused by the attack, and provides information on preventive counter-measures. It may request patches from vendors if necessary. It also shares information about these incidents with its constituents in weekly and quarterly reports, as well as on its portal site, JVN. It also coordinates with other CSIRTs, both within Japan (where it acts as the "CSIRT of CSIRTs") and internationally.[71] While in some sense JPCERT/CC is directly providing security, its incident response activities serve as an incentive for companies to actually report when they have been the victim of a cyber-attack. Information about the attack can then be shared with other firms, to the benefit of all.

ICT-ISAC (Information and Communications Technology Information Sharing and Analysis Center) Japan is one of a number of ISACs in Japan, each serving a different sector. ICT-ISAC is arguably the most important, however, since the ICT sector is the most directly affected by cyber security concerns. A private organization, it was founded in 2002 as Telecom-ISAC, in order to collect and analyze data about cyber-attacks on telecommunications and internet service providers. It was reorganized in March 2016 as ICT-ISAC Japan, to include broadcasting and other ICT firms. ICT-ISAC contains several working groups dedicated to sharing and analyzing information about various

---

[68] Author's interview with METI official, Tokyo, August 2017.

[69] JPCERT/CC 2017b. Author's interviews with Masaki Ishiguro, Mitsubishi Research Institute, January 2017, and with JPCERT/CC employee, Tokyo, July 2017.

[70] Author's interview with JPCERT/CC employee, Tokyo, July 2017. Equivalent organizations in other countries, such as US-CERT in the United States and KrCERT/CC in South Korea, are usually government-run.

[71] JPCERT/CC 2017b, 2018, 2017a.

cyber security issues relevant to the ICT sector. MIC has observer status at ICT-ISAC, and ICT-ISAC implements various cyber security projects headed by MIC.[72] Thus, while METI funds JPCERT/CC but takes an otherwise hands-off approach, MIC has a closer working relationship with ICT-ISAC Japan.

5.2.3 Research-and-Development Promotion [Market Facilitating]

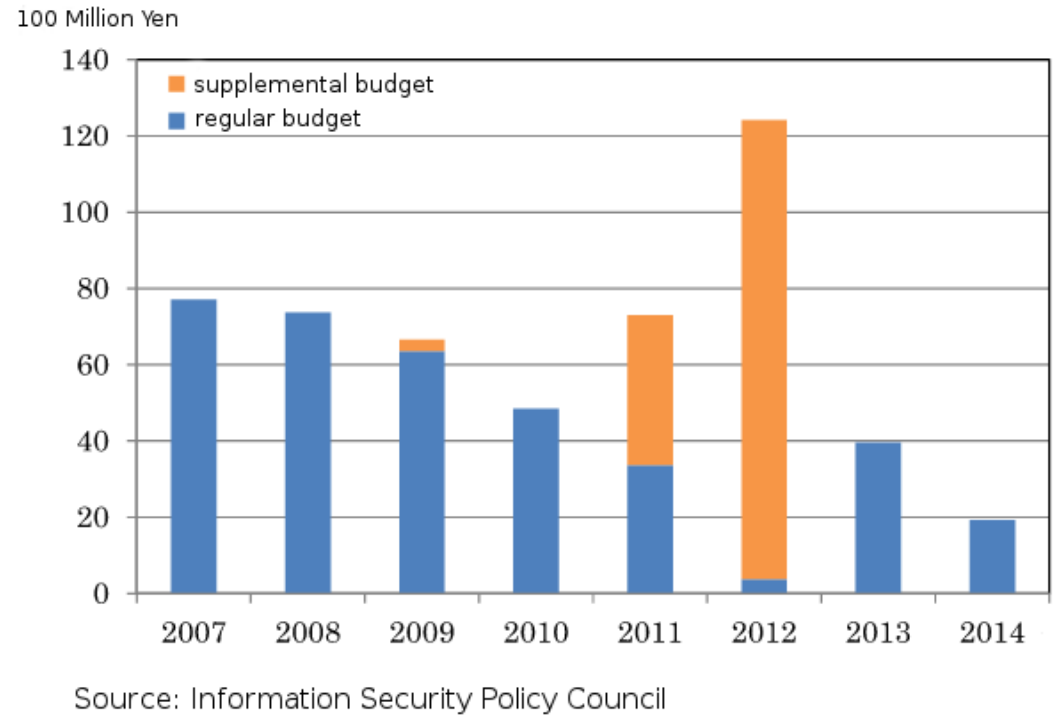

Figure 3: The Japanese government's research and development spending, 2009–2014.

As can be seen in Figure 3, the Japanese government's spending on research and development has been inconsistent. That having been said, the government does have several vehicles through which it funds research and development efforts. One of these, NICT, was discussed in Section 4. As of 2017, MIC was funding several projects through NICT. These included the maintenance of an internal network real-time analysis environment and large-scale storage environment; development and testing of an active observation system for cyber-attacks; development of technology to analyze and perform calculations on encrypted data while leaving it encrypted; and lightweight encryption and certification technology for IoT devices.[73]

Other vehicles for research and development funding include the National Institute of

[72] Omori 2016, 16–17; ICT-ISAC Japan 2018.
[73] サイバーセキュリティ戦略本部 (Cybersecurity Strategic Headquarters) 2017, 30.

Advanced Industrial Science and Technology (AIST), the Control System Security Center (CSSC), the National Institute of Informatics (NII), and the New Energy and Industrial Technology Development Organization (NEDO). AIST is one of the largest public research organizations in Japan, with a number of research bases around Japan. Reorganized in April 2001 as an incorporated administrative agency, it is supervised by METI. Its purpose is to generate technologies useful for Japanese industry and society, and in particular to move technology from the initial research stage to the commercialization stage.[74] Along with conducting its own cyber security research and development, it cooperatively manages the SEI-AIST Cyber Security Cooperative Research Laboratory along with Sumitomo Electric Industries.[75] As of 2017, METI was funding a project through AIST to develop large-scale software analysis tools for verifying the validity of embedded systems for automobiles, and a project to develop technology for new systems allowing for high-speed processing of encrypted data, as well as the generation of the "world's smallest cipher."[76]

Incorporated in 2012, CSSC is also supervised by METI. Its membership is primarily made up of corporations, as some trade associations, IPA, and Tohoku University. It conducts research and development aimed at the cyber security of control systems.[77] As of 2017, METI was funding a project through CSSC to develop technology to detect cyber-attacks by analyzing system behavior.[78]

NII is an inter-university research institute under the supervision of the Ministry of Education, Culture, Sports, Science and Technology (MEXT). Though its focus is more on academic research than the other research institutions mentioned here, it also promotes cooperation between academia, industry, and government. Among its several centers is the Center for Cyber Security Research and Development.[79] As of 2017, through NII, MEXT was funding the construction of a system to collect and share communications data about cyber-attacks related to machine-to-machine functions.[80]

NEDO was originally established in 1980 to promote the development of new energy technologies, in response to the two oil crises of the 1970s. Its mission was later expanded to include research and development of industrial technologies. Unlike AIST or NII, NEDO does not have its own researchers, but instead coordinates between private and academic researchers. Its mission is specifically to develop technologies that will ultimately be useful for industry, but where the risk is high enough, and the long-term payoff unclear enough, that private industry would not develop the technologies on its own. Like AIST and CSSC, NEDO is supervised by METI.[81]

---

[74] AIST 2018a, 2018b.
[75] AIST 2018c; Sumitomo Electric Industries, Ltd. 2018.
[76] サイバーセキュリティ戦略本部 (Cybersecurity Strategic Headquarters) 2017, 30.
[77] CSSC 2018b, 2018a.
[78] サイバーセキュリティ戦略本部 (Cybersecurity Strategic Headquarters) 2017, 30.
[79] National Institute of Infomatics 2018a, 2018b.
[80] サイバーセキュリティ戦略本部 (Cybersecurity Strategic Headquarters) 2017, 30.
[81] NEDO 2018a, 2018c, 2018b.

NEDO is managing a major project initiated under NISC's Strategic Innovation Creation Program (SIP) with a focus on ensuring the cyber security of critical infrastructure. Part of the goal of this project is to develop technologies that can be used not only in Japan, but also sold overseas.[82] For 2017, this project was given an estimated budget of 2.62 billion yen (about 24.68 million dollars), 1.79 billion of which is being used for research and development.[83] Participating in this project are a number of firms, including NTT, NTT Communications, Hitachi, Fujitsu, Mitsubishi Electric, Renesas Electronics Corporation, and Panasonic.[84] Technologies being developed by this project include technology for verifying the security of control and telecommunications equipment; technology for monitoring and analysis of control and telecommunications equipment and control network operations; technology for the protection of control and telecommunications technology and systems protection; IoT security verification technology; and platform technology for the evaluation and verification of IoT equipment.[85]

5.3 Government as Promoter

The government also encourages companies to invest more in cyber security. It does so through two mechanisms: regulatory powers and tax policy.

5.3.1 Regulatory Power [Market Facilitating]

This set of interventions consists of the provision of standards and regulations about cyber security to firms by government.

Discussing all of these interventions would take far too much space, but it is possible to mention a few recent examples. In December 2015, the Japanese Ministry of Economy, Trade, and Industry and the Information-Technology Promotion Agency, which is overseen by the Ministry, released *Cybersecurity Guidelines for Business Leadership Version 1.0*, aimed at Japanese business executives.[86] In August 2016, NISC released the *General Framework for Secured IoT Systems*, which lays out an initial plan for helping to ensure the security of devices connected to the Internet, including consumer devices. It lays out a two-stage approach, first focusing on the creation and operation of IoT systems, and then on their use by different sectors.[87]

Finally, in December 2016, METI and IPA released a revised version of their cyber security guidelines for businesses, appropriately titled *Cybersecurity Guidelines for Business Leadership ver. 1.1*. There were two major changes from version 1. One, the revised guidelines increase the emphasis that business leaders have a responsibility to

[82]サイバーセキュリティ戦略本部 (Cybersecurity Strategic Headquarters) 2017, 30; 内閣　政策統括官（科学技術・イノベーション担当） (Cabinet Office Policy Unification Service (In Charge of Science and Technology Innovation)) 2017, 8.
[83]NEDO 2017a; 内閣　政策統括官（科学技術・イノベーション担当） (Cabinet Office Policy Unification Service (In Charge of Science and Technology Innovation)) 2017, 12.
[84]NEDO 2017b.
[85]内閣　政策統括官（科学技術・イノベーション担当） (Cabinet Office Policy Unification Service (In Charge of Science and Technology Innovation)) 2017, 10–12.
[86]Matsubara and Kriz 2016.
[87]Matsubara 2016.

invest in cyber security as part of their business strategies. As support for this, it points out that cyber-attacks have become unavoidable. Two, it includes a 128-page supplementary *Guidebook for the Cybersecurity Guidelines ver. 1.0*, which is published by IPA. This supplements the original guidelines by giving specific actions that can be taken by business leaders and others involved in a company's cyber security; the original guidelines had principles but lacked concrete examples.[88]

While the government has hard regulations involving its own reporting on cyber security and reporting from critical infrastructure firms, these guidelines released by the government are for the most part "soft", meant to encourage best practices rather than to enforce them.

5.3.2 Tax Policies [Market Facilitating]

Another set of interventions the Japanese government has often pursued in the past is the use of favorable tax policies to bolster a particular sector or technology. There have been some measures taken regarding cyber security as well.

From FY 2006–2010, the government instituted a set of tax measures called the "Information Base Strengthening Tax System" (情報基盤強化税制). These were a set of tax incentives aimed at encouraging small- and medium-sized enterprises to acquire or replace four types of software and systems: servers and server-oriented operating systems; database management software and related application software; coordination software; and firewall software and equipment. While firewall software and equipment improves cyber security in obvious ways, the incentives for servers, operating systems, and database management software also aimed at improving security by requiring these systems and software to meet the ISO/IEC 15408 criteria for internet technology security.[89] Specifically, a company could apply a depreciation worth 50% of the standard value (70% of the actual value) of the equipment/software, or a tax credit worth 10% of the standard value. Though deductions could at most reach 20% of the current financial year's taxes, deductions in excess of this limit could be brought forward to the next financial year.[90]

Though the Information Base Strengthening Tax System was abolished in FY2010, a new set of provisions were implemented regarding information technology for small- and medium-sized enterprises. Even more than the previous set of incentives, these were aimed explicitly at improving the cyber security of these companies; the provisions were added "based on the circumstances that progress in the computerization of small- and

[88] Kriz and Matsubara 2016.
[89] MOF 2010, 369–70.
[90] MOF 2010, 369.

medium-sized industries, including dealing with unauthorized access and system faults, has certainly not been sufficient."[91]

The new tax provisions included several changes. First, while servers and server operating systems could still be depreciated assuming they met ISO/IEC 15408 certification as before, server virtualization software could now be depreciated as well. Server virtualization software allows two or more virtual servers, possibly running different operating systems, to run on the same machine. The actual machine hardware and operating system are invisible to those services running on the virtual server. The reason given for this tax incentives was to improve the efficiency of small- and medium-sized businesses' use of information technology hardware.[92] Virtualization certainly does this, but it has advantages for cyber security as well: virtual servers protect the real server from being accessed and attacked; compromised virtual servers can easily be replaced with backup images made prior to the attack; and virtual servers can be monitored from "outside" the system by the real server—monitoring which is impossible to detect from within the virtual server. Additionally, along with database management software, software that processes information organized by a database was included, again assuming it met ISO/IEC 15408 certification.[93]

Two other changes were more explicitly aimed at improving cyber security. One change was that while coordination software (defined in the new provision as "software that receives commands from data processing systems, and performs commands on systems other than data processing systems."[94] was still included, new requirements were placed upon it. Previously, there had been no mention of requiring ISO/IEC 15408 certification; under the new provisions, this requirement was included. The provision also included requirements for message-passing set by Japan Industrial Standards.[95]

The other change was that, in recognition that there were increasingly cyber-attacks that could pass through firewalls, as well as other ingenious attacks that small- and medium-sized enterprises must be able to respond to, the tax incentives were expanded beyond firewalls to include all software and equipment meant to block unauthorized access. This included equipment supporting data protocols for establishing communication channels, for determining communication methods, and for providing application services.[96]

Currently, the Ministry of Economy, Trade and Industry, with the support of the Ministry of Internal Affairs and Communications, is pushing for the government to create a set of tax measures aimed at promoting cyber security as part of its "Connected Industries" initiative. The main purpose of this initiative is to overcome coordination failures and

---

[91]"中小企業については、不正アクセス・システム障害への対応を含めた情報化の進展がまだ必ずしも十分ではないと考えられている状況を踏まえ" MOF 2010, 366

[92]MOF 2010, 366–67.

[93]MOF 2010, 367.

[94]MOF 2010, 367. "Data processing system" was defined in article 20, clause 1, item 5 of the Law Concerning the Promotion of Data Processing, as "an assembly of computers and programs composed in order to carry out data processing functions in an integrated manner". Government of Japan 2017

[95]MOF 2010, 367.

[96]MOF 2010, 366–67.

incomplete information problems between various high-technology companies, particularly those involved with data (such as IoT and artificial intelligence). METI gives the example of cooperation between a robotics firm and a venture company working on deep learning to create an IoT platform for the manufacturing industry, that, among other things, can automate machines based on data from manufacturing facilities.[97] METI recognizes, however, that in order for this initiative to succeed, strong cyber security is also necessary.[98] Specifically, METI and MIC are calling for 26,092 million yen in tax breaks (approximately 234.5 million U.S. dollars) in order to support these "Connected Industries" for the next two years.[99] Though it is not clear exactly what percentage of that will go to cyber security, the increase in cyber security forms an important part of the justification for these measures: "At the same time, as shared data is expanded and connected beyond current frameworks (such as companies), in order to deal with the threat of increasing cyber-attacks, [these tax incentives] will promote things such as the facilities necessary to constructing security systems able to withstand various cyber-attacks, and will also promote the introduction of further security measures."[100]

6. Drivers of Intervention Measures

While geopolitical factors have been a driving factor in the Japanese government's increased focus on cyber security, the particular measures used to promote cyber security have been primarily determined by domestic factors. Concerns about foreign hacking, and in particular, attacks on government sites (in the early 2000s) and the pension system (in 2015) were major drivers for changes in Japan's cyber security policy and policy-making structure. Because the Ministry of Internal Affairs and Communications and the Ministry of Economy, Trade and Industry have played large roles in developing cyber security policy, policies have been relatively business-friendly, aimed at creating a secure business environment and reassuring the public that the internet is a safe place to do business. That these two ministries have not focused more on the promotion of a cyber security sector, but instead on the promotion of cyber security in adjacent sectors, is due the fact Japan has few cyber security firms, but many firms for which cyber security is an issue: demand from the private sector is for more security, rather than for the promotion of Japanese cyber security products. The Japanese government has had to balance this demand to "do more" with its own desire to encourage private firms to invest more heavily in security themselves.

6.1 Geopolitical Context

There are a number of geopolitical reasons why Japan should be worried about improving its cyber security. Japan's relations with China have been becoming increasingly tense over the last several years. Though the proximate cause has been the dispute over control of the Senkaku/Diaoyu Islands and other maritime issues, there is no guarantee that this

[97] METI 2018.
[98] METI 2017b, 2017a.
[99] METI 2017a; MIC 2017.
[100] METI 2017a, 128.

conflict will not spill over into cyber space. What is more, China has quite formidable capabilities in this regard. As mentioned earlier, the cyber forces of the People's Liberation Army number in the few thousands.[101] What is more, China is considered a trend-setter in cybercrime innovation, developing a number of hacking tools that then become widespread both in China and beyond.[102]

North Korea has become more belligerent as well, and as the world saw in the hacking of Sony Pictures, has the capability to steal and distribute information via the internet. And while relations with Russia have perhaps grown slightly warmer, the two countries still have a territorial dispute between them, and recent events in the United States have demonstrated Russia's ability to use hacking to create difficulties for those it perceives as opposing its interests.

There have been several incidents that highlight these threats. One incident involved the Wi-Fi at the G-7 Ise-Shima summit being tampered with, infecting users' machines with a computer virus originating in Russia.[103] More directly related to traditional security concerns, Japan's defense industry has also been targeted. In 2007, an officer of the Marine Self-Defense Forces accidentally exposed classified data on the Aegis weapons system to the outside world when he shared pornography on a peer-to-peer network. More troubling, in 2011, Japan's largest defense contractor, Mitsubishi Heavy Industries Ltd., was breached by Chinese hackers. They were able to access classified submarine, missile, fighter jet, and nuclear power plant data.[104]

Two particular incidents have strongly impacted Japanese cyber security policy-making. The first was a series of hacks of government websites in the early 2000s by Chinese "patriotic hackers". Prior to this, the Japanese government had no unified cyber security policy. These hacks, however, forced the government to take cyber security more seriously, resulting in a series of policy discussions between MIC, METI, MOD, and NPA that would eventually lead to the creation of NISC and the Information Security Policy Council (ISPC), the precursor to the Cyber Security Strategic Headquarters. The ISPC would in turn release the "First National Strategy on Information Security" in 2006.[105]

There were two major differences between the policy-making structure at the time and the current policy-making structure, described earlier. For one, while the Cyber Security Strategic Headquarters is placed directly underneath the Chief Cabinet Secretary in the Cabinet Office, the ISPC was situated underneath another committee, the Information Technology Strategic Headquarters (ITSH). Thus, there was no direct line between the ISPC and the Prime Minister; it was the Chief of the ITSH that established the ISPC, not the cabinet itself.[106]

---

[101] 三菱総合研究所 2015, 58.

[102] Kingston 2016.

[103] Kingston 2016.

[104] Kingston 2016.

[105] Author's interview with MIC official, Tokyo, July 2017. Nitta 2014; Tsuchiya 2016

[106] Tsuchiya 2016.

Additionally, NISC at the time had very little authority over government bodies. It could receive information related to cyber security from government ministries, agencies, and local governments, but only on a voluntary basis. It had no authority to request this information, or to make recommendations without being asked for them.[107]

The second incident was the breach of the Japan Pension Service in 2015. Already by this time, LDP politicians had pushed for and ultimately passed the Cyber Security Basic Law in 2014. This restructured cyber security policy-making into its current form. Under this law, NISC was also granted authority to actively monitor the security of government bodies and independent administrative agencies.[108] However, the breach of the Japan Pension Service demonstrated that this new authority had not gone far enough: the Japan Pension Service had been organized in 2010 as a special public corporation, and thus had not been under the authority of NISC.[109] An amendment to the Basic Law in 2016 brought these entities under the authority of NISC as well.[110]

Thus, it can be clearly seen that these geo-political concerns have caused the Japanese government to take the issue of cyber security more seriously. The specific constellation of measures it has used to deal with the market failures surrounding cyber security, however, has been primarily determined by its domestic structure.

6.2 State-Level Preferences

Though politicians have occasionally intervened in cyber security policy-making, such as with the passage of the Basic Law, cyber security policy is mainly a result of negotiations between bureaucrats. Each of the main three ministries and one agency involved in cyber security policy-making has its own interests. MIC's main interest is in network security; that is, it is interested in protecting the network itself, rather than individual companies. One example of this is DDOS attacks, which slows down the network as a whole and forces internet service providers to spend a lot of money on facilities. This problem is likely to become worse as the Internet of Things becomes a more widespread phenomenon, creating more opportunities for bad actors to take over networked devices and turn them into bots. MIC therefore has an interest in making sure malware does not spread among these devices.[111] MIC is responsible for telecommunications companies and internet service providers, and so to some degree represents their interests within the government. It wants to improve cyber security, but not place undue burdens on ISPs.

METI's main interest is in promoting competitiveness and creating a "sound business environment". In terms of cyber security, this means METI is interested in reducing the number of cyber security incidents for Japanese companies.[112] METI oversees much of Japanese industry, and so to a certain extent represents their interests within the government. It is also responsible for a number of sectors that fall under "critical

[107]Interview with NISC official, Tokyo, January 2018. Tsuchiya 2016
[108]Tsuchiya 2016.
[109]Ironically, it had been created to replace the Social Insurance Agency after the latter had lost millions of pension records in a database merger.
[110]Interview with NISC official, Tokyo, January 2018.
[111]Author's interview with NISC official, Tokyo, July 2017.
[112]Author's interview with NISC official, Tokyo, July 2017.

infrastructure". That having been said, METI clearly wants industry to take on more responsibility for its cyber security.

MOD's main interest is in defending their own facilities and those of the Japanese Self-Defense Forces. The latter in particular has a large communications system that has suffered from cyber-attacks. MOD thus focuses heavily on security and resilience of defense-related networks and facilities.[113]

NPA's main interest is in preventing cybercrimes and catching and prosecuting criminals. Of the four ministries and agencies described here, it is NPA that cares about attribution of cyber-attacks.[114] This sometimes places them at odds with MIC, which places a higher emphasis on user privacy than on catching cyber criminals.[115]

Negotiations between these ministries and agency take place primarily in NISC or the Cyber Security Strategic Headquarters. MIC and METI have several advantages in these negotiations. Relative to other actors, they have strong connections to networks of cyber security experts, particularly through IPA and NICT, and to industry.

Additionally, while traditionally MIC and METI have been competitors, particularly regarding control over jurisdiction of information technology and the internet, they have been able to form an alliance over cyber security policy. In part, this is because their interests are aligned: while both want to improve cyber security, they both worry that policies favored by MOD or NPA may place undue burdens on firms and harm the economy. They also worry that MOD and NPA may not be equipped to deal with the international cooperation that cyber security requires. The expert communities with which both MIC and METI have ties also played a large role in bringing the two bureaucracies together.[116]

Thanks to these first two conditions, when NISC was originally created, MIC and METI were able to place their own bureaucrats in key positions, further strengthening them. NISC does not have its own staff; instead, its staff is seconded to it by MIC, METI, MOD, and NPA. Thus, the NISC serves less as an independent actor making policy, and more as an arena in which the three ministries and one agency can work out their policy differences. Though the director of NISC is seconded from the Ministry of Defense, it is one of the deputy directors that runs the day-to-day operations of NISC and represents NISC at meetings. This deputy director is alternately seconded from MIC and METI, giving the two ministries a great deal of power to set the agenda.[117]

Thus, while the interests of MOD and NPA are not irrelevant, government preferences largely reflect those of MIC and METI: the maintenance of a well-functioning network and a sound business environment, and the desire for private industry to do more while simultaneously not burdening them with too-costly or innovation-stifling regulations.

---

[113] Author's interview with NISC official, Tokyo, July 2017.

[114] Author's interview with NISC official, Tokyo, July 2017.

[115] Author's interviews with NPA official and MIC official, Tokyo, July 2017.

[116] Author's interview with MIC official, Tokyo, July 2017.

[117] Tsuchiya 2016.

6.3 State-Society Relations

The final factor in determining the shape of Japan's industrial policy toward cyber security is the nature and preference of its cyber-security-related firms. Part of what drives Japan's industrial policy toward cyber security is the relative sizes of its cyber-security-related sectors. Following Aggarwal and Reddie's framework, Japan's cyber-security-related industries can be split into three sectors: cyber security firms, internet technology firms, and internet-adjacent firms.[118] Cyber security firms work on cyber security issues directly. We can think of these firms as *producers* of security. Internet technology firms do not work on cyber security issues directly, but their operations and products rely on cyber security. Internet-adjacent firms create products which rely on some networked components, but do not fall within the information technology sector. Both internet technology firms and internet-adjacent firms can be considered *consumers* of cyber security, though they may also produce cyber security for internal use.

Cyber security firms provide an obvious source of demand for promotion of the cyber security sector. However, Japan has few cyber security firms. Only four companies in Cybersecurity Ventures' list of the most innovative cyber security firms are headquartered in Japan, and one of these, TrendMicro, is not a Japanese company.[119] Likewise, Japanese vendors account for only 0.16% of the number of vendors in The Cyber Research Databank.[120]

In contrast, Japan has a large number of internet technology and internet-adjacent firms. Internet technology firms include telecommunications equipment manufacturers such as NEC and OKI, telecommunications service providers such as NTT, KDDI, and Softbank, as well as their various subsidiaries, and internet technology service companies, such as Fujitsu and NTT Data. These are all major firms with large numbers of employees. They also include web-based service companies, such as Rakuten, one of the world's largest e-commerce sites. Thanks to the growth of automation and of the internet of things, internet-adjacent firms include not only financial firms such as banks, but also automobile manufacturers and manufacturers of consumer electronics, both of which play a large role in the Japanese economy. As power plants and other infrastructure components are increasingly becoming networked, firms providing critical infrastructure increasingly fall under this category as well.

In short, while Japan has few cyber security firms, it has many firms that rely on the internet, and thus that require cyber security. Unsurprisingly, then, the government's focus is more on improving cyber security for these firms than it is on promoting Japan's cyber security industry.

The preferences of Japanese firms with regard to government intervention are mixed. Firms have been reluctant to participate in some government-promoted efforts, such as information sharing, due to the reputational risks involved. However, in other areas, such

---

[118] Aggarwal and Reddie 2017.

[119] Cybersecurity Ventures 2017. By comparison, Israel, a far smaller country though also an acknowledged leader in this field, headquarters 34 of these companies; the UK headquarters 21; France, Germany, and Sweden each headquarter 7.

[120] The Cyber Research Databank 2017.

as regulation, firms want *more* government intervention; one of firms' main demands is for a set of firm guidelines on cyber security that they can follow.[121] This is because calculating risk is difficult for firms; they would prefer the government do the job for them. Firms have also shown willingness to participate in government-led joint research efforts, as detailed earlier. Arguably, then, the main dispute between the private sector and the government is that each side wants the other to take on more of the burden of improving Japan's cyber security, though overall the Japanese government seems to have a stronger awareness of the issue than does the private sector. Compared to the U.S., the private sector is far more welcoming of government involvement, though this may reflect the fact that policy in this area is being made by MIC and METI, which are already sensitive to business interests, rather than by the Japanese equivalents of the National Security Agency and the Department of Homeland Security.

7. Results of Interventions

Japan's approach has led to some successes, at least in terms of improving overall cyber security. In particular, Japan has a very "clean" internet. In relation to other countries in Asia, Japan does not have the same magntitude of problems with regard to illegal software, software that can contain malware or can leave systems open to exploitation due to an inability to update them. There is a high usage of anti-virus software, and companies and individuals patch their software regularly. In short, the Japanese do the basic things right.[122] This may help to explain why, for example, Japan was relatively unaffected by WannaCry, the ransomware that caused so many problems around the world.[123]

Some of the Japanese government's other efforts have had less of an effect. For example, despite its training programs, Japan continues to suffer from an under-supply of skilled cyber security workers. Part of the problem is that the government is limited in what it can do. Unlike countries such as the U.S. and Israel, Japan does not have a good way to cycle between the public and private sector—a particularly useful way both to improve the competency of government in this area and to build private-sector talent. There are two reasons for this. On the government side, the bureaucracy favors generalists over specialists, which means that for cyber security specialists there is not much opportunity for advancement within the government itself. However, government service might still be viewed as a sound option if it were an opportunity to build a skill set which could then lead to a good job in the private sector. Unfortunately, on the private sector side, firms prefer to hire permanent employees (the more desirable positions) directly out of college, rather than mid-career, which means that there is little payoff in government service for particularly talented workers.[124]

---

[121] Author's interview with METI official, Tokyo, August 2017.

[122] Author's interview with Professor Motohiro Tsuchiya, Keio University, August 2017.

[123] The fact that Japan was unaffected by WannaCry was mentioned to me by Professor Tsuchiya, but the speculation is my own.

[124] Author's interview with former IPA official, Japan, Summer 2017.

The government's efforts to encourage information sharing still have room for improvement as well. According to Japan Users Association of Information Systems' 2017 Survey of Business IT Trends, which surveyed the IT divisions of 1071 Japanese firms, 42.2% of respondents had not even heard of such information sharing systems; another 27.7% had heard of them but were not considering establishing them. Only 16% of respondents actually participated in such a scheme.[125]

For the government, there is a tricky balancing act between providing for Japan's cyber security and encouraging companies to invest in cyber security themselves. Government efforts such as the Cyber Clean Center have been extremely successful, but risk private firms growing complacent. Encouraging firms to invest in their own cyber security continues to be a major challenge for the government.

Though cyber security policy is increasingly important to the government, it would be difficult to say that intervention in this area has been particularly intense. Some of the market-substituting measures, such as the Cyber Clean Center and other efforts to remove malware, are quite strong relative to what we see in many countries, but otherwise the level of intervention is relatively low, and focused on coordination and voluntary measures. The goal seems to be to improve cyber security practices to provide an edge in related sectors where Japan is already competitive, rather than to promote the cyber security sector.

Accordingly, with the exception of R&D funding (which is targeted at Japanese firms), Japan's measures are non-discriminatory. The tax incentives, for example, are for the purchase of any cyber security technology that meets particular international standards, not for Japanese technology specifically. Likewise, while one could argue that market-substituting policies deprive cyber security companies of market opportunities, they do so indiscriminately. For example, one could argue that the Cyber Clean Center disadvantaged anti-malware software companies (since it did the same thing for free), but it did not specifically disadvantage *foreign* anti-malware software companies.

Conclusion

With the 2020 Summer Olympics coming to Japan, we are likely to see the Japanese government invest even more heavily in measures meant to improve critical infrastructure security. Another clear area of concern for the government is IoT devices. As mentioned earlier, the government is currently making an effort to build a new "Cyber Clean Center" aimed at removing bots and malware from internet-connected devices.[126] It is also clear that the Japanese government sees IoT as an area in which Japan can compete internationally, so we should anticipate that we will see more effort in building security into the manufacturing sector.

However, unless something changes drastically, we are unlikely to see strong promotion efforts in the cyber security sector in the near future. There is currently little demand

[125] 日本情報システム・ユーザー協会 (Japan Users Association of Information Systems) 2017, 94.

[126] Author's interview with NISC official, Tokyo, January 2018.

within Japan for native Japanese cyber security products: internet technology and internet-adjacent firms seem perfectly happy to purchase American products. The most likely purchaser of native Japanese cyber security products will be the government, but it feels it cannot do so as long as there are superior alternatives available — doing otherwise would reduce the government's own security.[127]

Instead of competing internationally in the cyber security sector, the Japanese government hopes that Japan can compete by offering products with strong built-in security. Further intervention will likely focus on encouraging "security by design" and other efforts to create and certify cyber-secure products. Convincing industry to cooperate will remain one of the major challenges for the government going forward.

[127] Author's interview with NISC official, Tokyo, July 2017.

References:

"About NICT | NICT Charter | NICT-National Institute of Information and Communications Technology." 2017. Accessed March 24. https://www.nict.go.jp/en/about/charter.html.

Aggarwal, Vinod and Reddie, Andrew (2018) "Comparative Industrial Policy and Cybersecurity: A Framework for Analysis," BASC Working Paper Series, 2018-01.

Aggarwal, Vinod K., and Andrew Reddie. 2017. "Comparative Industrial Policy and Cybersecurity: A Framework for Analysis and the U.S. Case."

AIST. 2018a. "AIST:About AIST." Accessed February 18. http://www.aist.go.jp/aist_e/about_aist/index.html.

———. 2018b. "AIST:History." Accessed February 18. http://www.aist.go.jp/aist_e/about_aist/history/history.html.

———. 2018c. "AIST:Information Technology and Human Factors." Accessed February 18. http://www.aist.go.jp/aist_e/dept/en_dithf.html.

Arimura, Kouichi. 2008. "Anti-Bot Countermeasures in Japan." http://www.nca.gr.jp/jws2008/WS1-ccc.pdf.

Brian Krebs. 2010. "Talking Bots with Japan's 'Cyber Clean Center' — Krebs on Security." https://krebsonsecurity.com/2010/03/talking-bots-with-japans-cyber-clean-center/.

Cole, Robert E., and Yoshifumi Nakata. 2014. "The Japanese Software Industry." *California Management Review* 57 (1): 16–43. http://cmr.ucpress.edu/content/57/1/16.abstract.

"Cryptographic Protocol Verification Portal (CPVP)." 2017. Accessed March 24. http://crypto-protocol.nict.go.jp/index_en.html.

CSSC. 2018a. "Control System Security Center -Backgrounds & Objectives-." Accessed February 18. http://www.css-center.or.jp/en/aboutus/purpose.html.

———. 2018b. "Control System Security Center -Overview-." Accessed February 18. http://www.css-center.or.jp/en/aboutus/.

"Cybersecurity Research Institute NICT-National Institute of Information and Communications Technology." 2017. Accessed March 24. https://www.nict.go.jp/en/csri/.

Cybersecurity Ventures. 2017. “Cybersecurity 500 List of Top Cybersecurity Companies.” https://cybersecurityventures.com/cybersecurity-500-list/.

Government of Japan. 2017. “情報処理の促進に関する法律,(略)情報処理促進法.” Accessed November 22. http://www.houko.com/00/01/S45/090.HTM.

Harris, Robert G., and James M. Carman. 1984. “Public Regulation of Marketing Activity: Part II: Regulatory Responses to Market Failures.” *Journal of Macromarketing* 4 (1): 41–52.

ICT-ISAC Japan. 2018. “ICT-ISAC Japan.” Accessed February 20. https://www.ict-isac.jp/english/index.html#Member.

“IoT Security Guidelines Ver. 1.0 Formulated（METI）.” 2017. Accessed March 24. http://www.meti.go.jp/english/press/2016/0705_01.html.

IPA. 2011. “情報セキュリティ産業の構造と活性化に関する調査　報告書.” https://www.ipa.go.jp/files/000024418.pdf.

“IPA Information-Technology Promotion Agency, Japan : IPA:Business Outline.” 2017. Accessed March 24. http://www.ipa.go.jp/english/about/outline.html.

“Japanese Law Translation - [Law Text] - the Basic Act on Cybersecurity.” 2015. http://www.japaneselawtranslation.go.jp/law/detail/?ft=1&re=02&dn=1&x=0&y=0&co=01&ia=03&ky=%E3%82%BB%E3%82%AD%E3%83%A5%E3%83%AA%E3%83%86%E3%82%A3&page=1.

JPCERT/CC. 2017a. “JPCERT Coordination Center Activities.” Accessed April 12. https://www.jpcert.or.jp/english/pr/index.html.

———. 2017b. “JPCERT コーディネーションセンター JPCERT/CCについて：JPCERT/CCのさまざまな活動.” Accessed April 16. http://www.jpcert.or.jp/about/05.html.

———. 2018. “JPCERT コーディネーションセンター インシデント対応とは？.” Accessed February 20. https://www.jpcert.or.jp/ir/.

Kibashiri, Masamizu. 2007. “日本のソフトウエア生産性と品質は世界最高水準～なぜ日本のソフトは国際競争力がないのか。 - 木走日記.” *はてなダイアリー*. http://d.hatena.ne.jp/kibashiri/20070323/1174629051.

Kingston, Jeff. 2016. “Japan’s Cybersecurity Upgrade — Too Little, Too Late?” *The Japan Times*. http://www.japantimes.co.jp/opinion/2016/05/21/commentary/japans-cybersecurity-upgrade-little-late/.

Kriz, Danielle, and Mihoko Matsubara. 2016. “Japanese Government Updates Cybersecurity Guidelines: Increased Focus on Cybersecurity Investments and SMBs.” *Palo Alto Networks Blog*. http://researchcenter.paloaltonetworks.com/2016/12/gov-

japanese-government-updates-cybersecurity-guidelines-increased-focus-cybersecurity-investments-smbs/.

Masuoka, Ryusuke, and Tsutomu Ishino. 2012. “Cyber Security in Japan (V.2).” Center for International Public Policy Studies. http://www.cipps.org/group/cyber_memo/003_121204.pdf.

Matsubara, Mihoko. 2016. “Assessing Japan’s Internet of Things (IoT) Security Strategy for Tokyo 2020.” *Palo Alto Networks Blog*. http://researchcenter.paloaltonetworks.com/2016/09/cso-assessing-japans-internet-of-things-iot-security-strategy-for-tokyo-2020/.

Matsubara, Mihoko, and Danielle Kriz. 2016. “Japan’s Cybersecurity Guidelines for Business Leadership.” *Palo Alto Networks Blog*. http://researchcenter.paloaltonetworks.com/2016/05/japans-cybersecurity-guidelines-for-business-leadership-changing-the-japanese-business-mindset-and-potentially-raising-the-global-bar/.

METI. 2016. “METI-Related FY 2016 Budget.” http://www.meti.go.jp/english/aboutmeti/policy/fy2016/pdf/160329related_budget.pdf.

METI. 2017a. “平成３０年度税制改正に関する経済産業省要望のポイント (METI’s 2018 Tax Reform Requests).” http://www.meti.go.jp/main/yosangaisan/fy2018/pdf/01_10.pdf.

———. 2017b. “「Connected Industries」東京イニシアティブ2017 ("Connected Industries" Tokyo Initiative 2017).” http://www.meti.go.jp/press/2017/10/20171002012/20171002012-1.pdf.

———. 2018. “Connected Industries（METI）.” Accessed February 18. http://www.meti.go.jp/english/policy/mono_info_service/connected_industries/index.html.

MEXT. n.d. “MEXT : Organization.” Accessed March 19, 2018. http://www.mext.go.jp/en/about/organization/index.htm.

MIC. 2017. “平成３０年度税制改正に関する総務省要望のポイント (MIC’s 2018 Tax Reform Requests).” http://www.mof.go.jp/tax_policy/tax_reform/outline/fy2018/request/soumu/30y_soumu_k.pdf.

Ministry of Defense. 2014. “Establishment of the Cyber Defense Unit.” *Japan Defense Focus*, no. 52 (May). http://www.mod.go.jp/e/jdf/sp/no52/sp_activities.html#article03.

“Ministry of Internal Affairs and Communications.” 2017. Accessed March 24. http://www.soumu.go.jp/english/.

MOF. n.d. “Functions.” Ministry of Finance. Accessed March 19, 2018. http://www.mof.go.jp/english/about_mof/functions/index.htm.

———. 2010. “租税特別措置法等（法人税関係）の改正 (Special Tax Measures Law, Etc. (Related to Business Taxes) Revision).” https://www.mof.go.jp/tax_policy/tax_reform/outline/fy2010/explanation/PDF/08_P350_420.pdf.

National Institute of Infomatics. 2018a. “Mission & Strategies - About NII - National Institute of Informatics.” Accessed February 18. http://www.nii.ac.jp/en/about/introduction/mission/.

———. 2018b. “研究施設（センター） - 研究.” Accessed February 18. http://www.nii.ac.jp/research/centers/.

National Police Agency. 2017. “@Police-the National Police Agency’s Commitment to Information Security.” Accessed April 16. https://www.npa.go.jp/cyberpolice/english/action02_e.html.

NEDO. 2017a. “NEDO:戦略的イノベーション創造プログラム（SIP）／重要インフラ等におけるサイバーセキュリティの確保.” http://www.nedo.go.jp/activities/ZZJP_100109.html.

———. 2017b. “研究開発内容（全体版）(Contents of Research and Development (Complete Version)).” http://www.nedo.go.jp/content/100862901.pdf.

———. 2018a. “NEDO:About NEDO.” Accessed February 18. http://www.nedo.go.jp/english/introducing_index.html.

———. 2018b. “NEDO:Background Information.” Accessed February 18. http://www.nedo.go.jp/english/introducing_profile.html.

———. 2018c. “NEDO:NEDO Project Activities (Budget: 1.27 Billion US Dollars).” Accessed February 18. http://www.nedo.go.jp/english/introducing_pja.html.

Nikkei. 2017. “Japan to Create Cyberdefense Bureau.” *Nikkei Asian Review*. https://asia.nikkei.com/Politics-Economy/Policy-Politics/Japan-to-create-cyberdefense-bureau.

NISC. 2016a. “サイバーセキュリティ戦略本部　名簿.” http://www.nisc.go.jp/conference/cs/pdf/meibo.pdf.

———. 2016b. “サイバーセキュリティ対策の強化に向けた対応に ついて.” 9. http://www.kantei.go.jp/jp/singi/keizaisaisei/miraitoshikaigi/4th_sangyokakumei_dai2/siryou9.pdf.

NISC. 2017. “政府のサイバーセキュリティに関する予算.” https://www.nisc.go.jp/active/kihon/pdf/yosan2017.pdf.

Nitta, Yoko. 2014. “National Cyber Security Strategy: Are We Making Progress? Japan’s Efforts and Challenges.” *Georgetown Journal of International Affairs*, 89–98. http://www.jstor.org/stable/43773652.

Omori, Kazuaki. 2016. “Cybersecurity Policy and Projects by Ministry of Internal Affairs and Communications (MIC).” Tokyo. https://www.oasis-open.org/events/sites/oasis-open.org.events/files/1.6%20MIC%20Kazuaki%20Omori.pdf.

“Organization Chart/METI Ministry of Economy, Trade and Industry.” 2017. Accessed March 24. http://www.meti.go.jp/english/aboutmeti/data/aOrganizatione/index.html.

Pekkanen, Saadia, and Paul Kallender-Umezu. 2010. *In Defense of Japan: From the Market to the Military in Space Policy*. Stanford University Press.

Roth, William. 2016. “Japan’s Cyber Security Market: Opportunities and Challenges.” http://spfusa.org/wp-content/uploads/2016/02/Japan-Cyber-Market-Feb2016.pdf.

Sumitomo Electric Industries, Ltd. 2018. “Cyber-Security R&D Office R&D Sumitomo Electric Industries, Ltd.” http://global-sei.com/technology/rd/cyber/.

Telecom-ISAC. 2017. “Cyber Clean Center / What Is Cyber Clean Center?” Accessed October 16. https://www.telecom-isac.jp/ccc/en_index.html.

The Cyber Research Databank. 2017. “Cyber Security Statistics CyberDB.” Accessed September 4. https://www.cyberdb.co/database/cyberdb-statistics/.

Tokio Marine Nichido. 2015. “リスクマネジメント動向調査2015 (Risk Management Survey Report 2015).”

Tsuchiya, Motohiro. 2016. “Information Governance in Japan.” In, edited by Kenji E. Kushida, Yuko Kasuya, and Eiji Kawabata. Stanford Silicon Valley New Japan Project.

UNCTAD. 2012. “International Classification of Non-Tariff Measures: 2012 Version.”
Willis Towers Watson. 2017. “Decoding Cyber Risk: 2017 Willis Towers Watson Cyber Risk Survey, US Results.” https://www.willistowerswatson.com/-/media/WTW/PDF/Insights/2017/06/WTW-Cyber-Risk-Survey-US-2017.pdf.

“サイバーセキュリティ基本法.” 2016. http://law.e-gov.go.jp/htmldata/H26/H26HO104.html.

サイバーセキュリティ戦略本部 (Cybersecurity Strategic Headquarters). 2017. “サイバーセキュリティ研究開発戦略 (Cybersecurity Research and Development Strategy).” https://www.nisc.go.jp/active/kihon/pdf/kenkyu2017.pdf.

“サイバーセキュリティ戦略本部　第1回会合　議事概要.” 2015. http://www.nisc.go.jp/conference/cs/dai01/pdf/01gijigaiyou.pdf.

三菱総合研究所. 2015. “サイバーセキュリティに関する法律及び制度：主要事項.” 日本: 国立国会図書館.

内閣官房. 2017. “内閣官房組織令（抄）.” Accessed March 23. http://www.nisc.go.jp/law/pdf/soshikirei.pdf.

内閣　政策統括官（科学技術・イノベーション担当） (Cabinet Office Policy Unification Service (In Charge of Science and Technology Innovation)). 2017. “戦略的イノベーション創造プログラム（ＳＩＰ） 重要インフラ等におけるサイバーセキュリティの確保 研究開発計画 (Strategic Innovation Creation Program (SIP) Ensuring Cyber Security for Important Infrastructure, Etc. Research and Development Plan).” http://www.nedo.go.jp/content/100767969.pdf.

情報セキュリティ政策会議 (Information Security Policy Council). 2014. “新・情報セキュリティ普及啓発プログラム (New Information Security Public Awareness Program).” http://www.nisc.go.jp/active/kihon/pdf/awareness2014.pdf.

日本情報システム・ユーザー協会 (Japan Users Association of Information Systems). 2017. “企業IT動向調査2017 (Survey of Business IT Trends 2017).” 23. http://www.juas.or.jp/cms/media/2017/04/it17_ppt.pdf.