Institutional Determinants of Cyber Security Promotion Policies: Lessons from Japan, the U.S., and South Korea

by

Benjamin Gosnell Bartlett

A dissertation submitted in partial satisfaction of the

requirements for the degree of

Doctor of Philosophy

in

Political Science

in the

Graduate Division

of the

University of California, Berkeley

Committee in charge:

Professor Vinod Aggarwal, Chair
Professor T.J. Pempel
Professor Steve Vogel
Professor Steve Weber
Professor Dana Buntrock

Fall 2018

Institutional Determinants of Cyber Security Promotion Policies: Lessons from Japan, the U.S., and South Korea

Abstract

Institutional Determinants of Cyber Security Promotion Policies: Lessons from Japan, the U.S., and South Korea

by

Benjamin Gosnell Bartlett

Doctor of Philosophy in Political Science

University of California, Berkeley

Professor Vinod Aggarwal, Chair

Ensuring the cyber security of the private sector requires both the production of and consumption of cyber security technology. States vary in the degree to which they promote production and consumption. Taking an institutionalist approach, I argue that the difference between states can be explained as the result of two policy legacies. States with a policy legacy of maintaining strong traditional national security capabilities have the instruments necessary to promote production of cyber security technology, as well as actors—the military and intelligence agencies—who are motivated to do so. States with a policy legacy of economic guidance have the instruments to promote the consumption of cyber security technology, and economically-oriented bureaucratic actors who see it as their responsibility to do so.

To provide evidence for my hypotheses, I do a comparative case study of Japan, the U.S., and South Korea. Japan, with a policy legacy of restrained traditional security capabilities and a legacy of economic guidance, does little to promote production but is active in promoting consumption. The U.S., with a legacy of maintaining strong traditional security capabilities but without a legacy of economic guidance, is active in promoting production but does little to promote consumption. South Korea, which has a policy legacy of maintaining strong traditional security capabilities and a legacy of economic guidance, promotes both.

The key implication of this research is that a state's ability to promote cyber security in the private sector is heavily determined not only by past policies, but past policies that were unrelated to cyber security. States without the proper policy legacies will have to find ways to build substituting institutions in order to promote both production and consumption of cyber security.

To My Father, David Lyon Bartlett

The kindest, sweetest, gentlest man I have ever known.

Contents

List of Figures

Acknowledgments

I want to thank my chair, Vinod Aggarwal, and my committee members. I would also like to thank the Japanese Society for the Promotion of Science, Keio University, Waseda University, and the Center for Japanese Studies at the University of California, Berkeley, for their funding and support. Thanks as well to the many people in Japan who kindly gave me their time and helped to make this dissertation possible. Finally, I would like to thank my family, without whose unwavering support I could not have done this.

Chapter 1

Introduction

Though once known for its strong industrial policies, Japan has fallen behind other countries, including South Korea and the U.S., in supporting its cyber security sector, despite the obvious security benefits. At the same time, the Japanese government has been quite active in promoting the adoption of cyber security technology within the private sector. Using an institutionalist approach, I argue that this is the result of two factors: a policy legacy of maintaining minimal traditional security capabilities, and a policy legacy of economic guidance.

By *traditional security capabilities*, I mean those capabilities that bear either on the ability to wage or to deter militarized conflict, including war.[1] *Economic guidance* is a somewhat trickier concept. All governments play a role in shaping their economies; the difference is in how they play that role.[2] Economic guidance, refers to policies for promoting specific sectors, or for influencing the behavior of specific firms in particular ways, rather than by setting broader "rules of the road".[3]

The reason for looking at sector promotion and the promotion of technology adoption is that ensuring cyber security requires both the production of and consumption of cyber security technology. Anti-virus software, firewall software, encryption tools, and other cyber security products and services mean little if they are not properly used. Whether and how a

[1]This roughly corresponds to Walt's definition of "security" as it related to the field of security studies. See Stephen M. Walt, "The Renaissance of Security Studies," *International Studies Quarterly* 35, no. 2 (1991): 212–213.

[2]For a thorough discussion of this point, see Steven K. Vogel, *Marketcraft: How Governments Make Markets Work* (Oxford University Press, February 2018).

[3]Johnson's developmental state remains the archtypical example of a state providing guidance, but note that "guidance" does not have to be as top-down as depicted in Johnson's work; it can be the "reciprocal consent" described by Samuels, where the private sector acquiesces to the expansion of state jurisdiction in return for institutionalized access to public goods, or anything in-between. The key is that the government plays some type of "guiding" role, not that its role is absolute. See Chalmers Johnson, *MITI and the Japanese Miracle: The Growth of Industrial Policy : 1925-1975* (Stanford University Press, 1982); Richard J. Samuels, *The business of the Japanese state: energy markets in comparative and historical perspective* (Cornell University Press, 1987).

government promotes the adoption of cyber security technology in the private sector is thus as important as whether and how it promotes the production of that technology. Indeed, there is an argument to made that the latter is more important for the strengthening of cyber security, since cyber security technology can be purchased from abroad.

That having been said, there is a strong national security argument to be made for indigenous production of cyber security technology. There is no guarantee that security products developed in another country will not have backdoors or other flaws introduced into it by a foreign government. Perhaps ironically, cyber security products are a particularly tempting target for such backdoors because they require administrative access to a computer to function. Administrative access allows the program to access any file on the computer, to alter the configuration of the computer, and to install and run programs. As a result, a backdoor included in one of these programs would give the foreign government complete access to any computer on which they were installed.[4] Using foreign cyber security products for military or government systems risks giving foreign governments access to those systems.

As importantly, having a strong indigenous cyber security sector also makes it easier for governments to develop customized cyber tools, both for offensive and defensive purposes. Cyber tools are far more effective when other states are unaware of them; if they have access to a tool, they can figure out how to defend against it or overcome it, depending on whether it is offensive or defensive. Having a foreign firm develop customized cyber tools thus has obvious disadvantages. Best of all for the government to develop the tool itself; second-best is to have a domestic firm develop it. In either case, the human capital made available by a strong cyber security sector provides a clear advantage to governments.

There are also potential economic benefits to an indigenous cyber security sector. The sector is growing rapidly: it is projected to grow with a compound interest rate of 9.8% between 2015 and 2020; worldwide enterprise security spending is expected to be $96 billion in 2018.[5] Because cyber security products have large fixed up-front costs, but small and decreasing costs for duplication and distribution, firms which entered this sector early have an advantage over late arrivals.[6] If a country has no early movers, the government may wish to help its indigenous companies in order to help them catch up with the early movers in other countries.

However, in order to promote an indigenous cyber security sector, the government must

[4]Andrew Desiderio and Kevin Poulsen, "Exclusive: U.S. Government Can't Get Controversial Kaspersky Lab Software Off Its Networks," *The Daily Beast*, May 2018, accessed July 18, 2018, `https://www.thedailybeast.com/exclusive-us-government-cant-get-controversial-kaspersky-lab-software-off-its-networks`.

[5]Steve Morgan, *Cybersecurity Market Reaches $75 Billion In 2015; Expected To Reach $170 Billion By 2020*, December 2015, accessed July 25, 2018, `https://www.forbes.com/sites/stevemorgan/2015/12/20/cybersecurity%E2%80%8B-%E2%80%8Bmarket-reaches-75-billion-in-2015%E2%80%8B%E2%80%8B-%E2%80%8Bexpected-to-reach-170-billion-by-2020/`; Gartner, *Gartner Forecasts Worldwide Security Spending Will Reach $96 Billion in 2018, Up 8 Percent from 2017*, December 2017, accessed July 18, 2018, `https://www.gartner.com/newsroom/id/3836563`.

[6]Klaus M. Schmidt and Monika Schnitzer, "Public Subsidies for Open Source - Some Economic Policy Issues of the Software Market," *Harvard Journal of Law & Technology* 16 (2002): 477–478.

Country	Policy Legacies		Policy Outcomes	
	Security Capabilities Maintenance	Economic Guidance	Sector Promotion	Cyber Security Promotion
Japan	Weak	Strong	No	Yes
U.S.	Strong	Weak	Yes	No
South Korea	Strong	Strong	Yes	Yes

Figure 1.1: Basic argument.

create demand for indigenous products and services. In practice, this means the government purchasing the products and services, and/or encouraging firms and individuals within the private sector to purchase these products and services. Because the indigenous cyber security sector is not yet developed, this creates a trade-off between short-term security and potential long-term benefits. In the short term, relying on indigenous technology will leave consumers with weaker cyber security than if they used foreign technology. And while this may pay off in the long run if the indigenous cyber sector takes off, there is no guarantee that this will happen. The short-term costs are certain, while the long-term benefits are not.

Because firms are consumers of cyber security technology, these short-terms costs are in part economic. Relying on weaker cyber security products and services not only risks the cyber security of the firm, but the cyber security of its products and services in turn. Weaker cyber security can both impose direct costs, through losses by cyber crime, and indirect costs, since consumers may not wish to use products and services that have a reputation for poor cyber security.

The basic argument is that, from the perspective of maintaining strong traditional security capabilities, the case for promoting an indigenous cyber security sector is quite strong, while the economic case is not. Thus, states with a policy legacy of maintaining strong traditional security capabilities promote their sector, such as the U.S. and South Korea, promote their cyber security sectors. States without such a legacy, such as Japan, do not. In truth, the outcome is not quite this binary—Japan does take some small steps to promote cyber security technology—but as will be seen in Chapter 3, these are quite small, and are primarily aimed at building technologies and human capital that will improve cyber security in other key sectors.

There are both national security and economic reasons to promote the adoption of cyber security technology as well, although here the national security case is less clear-cut. Malware that infects public networks can spread to government networks; compromised networked devices can be used to launch DDOS and other attacks on government servers; and government officials use private-sector services, from which their personal data can be stolen. Firms can be targeted by foreign governments, who have resources with which they cannot compete. Stolen technology may have national security as well as economic implications, particularly if it is defense technology. However, how much of a threat this is to national

security in the traditional sense is difficult to gauge.

The economic case is much clearer. The cost of cybercrime was as much as $600 billion worldwide in 2017.[7] Stolen technology can reduce a company's competitiveness. Leaks of personal information can not only harm users financially through identity theft, but may make individuals unwilling to use internet services. DDOS attacks can make network services unavailable. On the positive side, if a country has a reputation for cyber secure products and services, this could provide a competitive advantage.

In practice, Japan and South Korea are active in promoting the adoption of cyber security technology, while the U.S. is not.[8] Because Japan and South Korea have strong legacies of economic guidance, there exist government actors in both of these countries that see promoting the adoption of cyber security as a natural extension of their responsibilities to protect and strengthen the economy. As importantly, private sector actors view government involvement as normal and legitimate, even if they do not always agree on what the specific nature of that involvement should be. Essentially, promoting the adoption of cyber security technology is a natural extension of the usual role of government.

By contrast, while the U.S. government certainly shapes its economy no less than Japan or South Korea, it does so via rule-setting rather than via guidance mechanisms. There do not exist actors within government who see promoting cyber security in the private sector as a major part of their duties, and promoting the adoption of cyber security technology is not seen as a natural extension of government's existing duties, but at best an area for debate. Moreover, firms are suspicious of government taking a role in promoting the adoption of cyber security, preferring to be left to their own devices.

This simple model is incomplete. While the economic argument is not as straightforward as the security argument, there is an economic argument to be made for sector promotion. In theory, even without a legacy of strong national security, Japan might still promote the cyber security sector for economic reasons. Thus, the question still needs to be answered: *why* does the Japanese government not find the economic case compelling? In Chapter 3, I will complicate this model, arguing that Japan does not find this case convincing due to previous experience in trying to promote software.

This model also ignores the fact that the national security argument for promoting the adoption of cyber security technology is not the same across sectors. In particular, the case for critical infrastructure sectors, such as electricity and transport, is much clearer than for other types of firms. The government and the military both rely on this infrastructure, making cyber attacks on those sectors closer to a traditional national security concern. Of course, other firms and the general public rely on this infrastructure as well, meaning attacks on these firms are potentially more damaging than for other types of firms. As I will discuss in Chapter 4, this means that all of the states, including the U.S., take actions to promote the adoption of cyber security technology in these sectors, regardless of whether they have

[7]Lynette Lau, *Cybercrime 'pandemic' may have cost the world $600 billion last year*, February 2018, accessed August 8, 2018, `https://www.cnbc.com/2018/02/22/cybercrime-pandemic-may-have-cost-the-world-600-billion-last-year.html`.

[8]With the notable exception of critical infrastructure, a point to which I will return shortly.

legacies of economic guidance. However, states with those institutions do have an advantage over states that do not, in that the instruments they use for guidance can easily be adapted to promoting the adoption of cyber security technology in critical infrastructure sectors. By contrast, states without these institutions have to develop these instruments.

1.1 Policy Outcomes

Sector Promotion

The first policy outcome, sector promotion, refers to the government using *selective policy instruments* to promote the cyber security sector. Policy instruments aimed at strengthening the economy can either be horizontal or selective. Horizontal policies are aimed at improving the general business environment, rather than on encouraging the growth of a particular sector. This includes instruments such as changing interest rates, reductions in corporate tax rates, R&D subsidies, labor training subsidies, and reforms to intellectual property laws. Selective policies include instruments such as public procurement, export promotion, strategic investment funds, and sector-specific tax breaks.[9] While horizontal policies may strengthen the cyber security sector, by *sector promotion* I mean only those instruments used specifically to strengthen the cyber security sector: R&D funding for cyber security projects, tax breaks aimed at cyber security firms, procurement of indigenous cyber security technology, and so forth.

In deciding whether a policy or instruments counts as promoting the cyber security sector, the important factor is intent. Policies created with the sole intent of boosting the cyber security sector of course count, but instruments designed for strengthening high technology sectors more broadly may count assuming there is a decision-making process involved. For example, a government-funded venture capital firm that invests in multiple types of technology firms included cyber security firms would count, because there is a conscious decision by the VC firm to invest in cyber security. By contrast, a program that offered subsidized loans to technology companies would not count, even if cyber security firms benefit, because the locus of decision-making is the firms themselves. In short, programs that firms select into do not count, *unless* the program is aimed at cyber security in particular (e.g., subsidized loans for cyber security firms).

There is a large literature on sector promotion, much of which looks at the economic reasons a government might choose to promote a particular sector.[10] It should be noted that sector promotion can be used both *strategically*, to promote a new industry (either truly new, or new to the particular country), or *defensively*, to protect existing sectors from

[9]Ken Warwick, *Beyond Industrial Policy*, OECD Science, Technology and Industry Policy Papers 2 (April 2013), 26–28, accessed February 9, 2017, `http://www.oecd-ilibrary.org/science-and-technology/beyond-industrial-policy_5k4869clw0xp-en`.

[10]Indeed, Prof. Vinod Aggarwal at the University of California at Berkeley has been heading a project on comparative industrial cyber security policy, in which participating authors describe industrial policies in a variety of countries. Publications forthcoming.

emerging competitive pressures, either long-term or through a period of adjustment, and the explanations for why a government would pursue sector promotion is naturally different depending on which of these two types of promotion is being discussed.[11] Because cyber security is clearly a new industry, I only discuss possible reasons a state might strategically promote a sector here.

One reason a government might choose to use sector-specific instruments would be to fix sector-specific *market failures*.[12] According to the welfare economics, there are three conditions under which markets are the most efficient allocators of resources. One, all goods and services are traded at publicly known prices. Two, all consumers and producers behave competitively. Three, an equilibrium exists. Leaving aside the last condition, a market failure occurs when either the first or second condition does not hold.[13] In this case, the government may step in to provide what the market cannot on its own. Research and development is a good example of this: because there is uncertainty over whether R&D will be successful and how long it will take, and because firms that invest in R&D not be able to capture the benefits entirely for themselves, firms tend to underinvest in R&D.[14] Thus, it may be necessary for the government to take measures to see that there is a proper level of investment in R&D, for example through funding it directly or by encouraging firms in a particular sector to form a consortium.

A second possible reason a state might want to promote a particular sector is due to spill-over effects such as inter-industry knowledge diffusion.[15] The argument is that certain sectors may be particularly likely sources of new manufacturing techniques or other process innovations, which will then spread to other sectors. As a result, developing the sector has a stronger positive effect on the overall economy than one would anticipate if considering the sector in isolation.

A third possible reason has to do with international trade and competition. Some sectors, due to economies of scale, advantages of experience, and innovation potential create high barriers to entry, advantaging first-mover states over late-comers.[16] Key is that while late-

[11] Warwick, *Beyond Industrial Policy*, 28–29.

[12] One could make the argument that in such a case the government is not truly promoting the sector, since it is simply making certain that the market is functioning properly. Since the resultant behavior is to take actions meant to aid firms in a specific sector, however, and because including government intent as part of the dependent variable risks begging the question, I include this behavior as sector promotion.

[13] John O. Ledyard, *Market Failure*, ed. Steven N. Durlauf and Lawrence E. Blume, London, 2008; Mariana Mazzucato and Caetano CR Penna, "Beyond Market Failures: The Market Creating and Shaping Roles of State Investment Banks," *SSRN Electronic Journal*, 2015, 9, accessed March 15, 2018, `http://www.ssrn.com/abstract=2559873`.

[14] Damiano Bruno Silipo and Avi Weiss, "Cooperation and competition in an R&D market with spillovers," *Research in Economics* 59, no. 1 (March 2005): 42; Daniel I. Okimoto, *Between MITI and the Market: Japanese Industrial Policy for High Technology* (Stanford University Press, 1989), 58–60.

[15] Patricia Succar, "The Need for Industrial Policy in LDC's-A Re-Statement of the Infant Industry Argument," *International Economic Review* 28, no. 2 (1987): 521–534; Howard Saggi Pack Kamal, *The Case For Industrial Policy : A Critical Survey*, Policy Research Working Papers (The World Bank, February 2006), 10–11, accessed July 26, 2018, `https://elibrary.worldbank.org/doi/abs/10.1596/1813-9450-3839`.

[16] Another way of thinking about this is that countries have different *technological capabilities*, which

comers will at first be under a competitive disadvantage, if they have the proper endowment structure, they can successfully promote this industry by protecting it from foreign competition until it becomes profitable through increasing returns and learning-by-doing.[17] These same barriers make the sector unusually profitable, which is what motivates late-comers to promote the sector.[18] Alternatively, a government may choose to subsidize a profit-earning imperfectly competitive sector in order to capture a larger share of the market versus a rival country.[19]

Much of the theoretical work assumes that policy-makers are rational actors: actors that not only have well-ordered preferences, but, within the limits of the information they have available to them, are able to pick the strategy (in this case, what sectors to promote) that will best achieve their desired outcome. Even theoretical critiques challenging whether governments can actually successfully pursue industrial policy tend to assume that governments act rationally, and that the problem is one of incomplete information.[20]

By contrast, much of the empirical work on industrial policy finds that policy-makers picked sectors based on some heuristic or a "logic of appropriateness" in which they chose those sectors they felt a country needed in order to be considered an advanced industrial economy. These findings fit with the expectation that policymakers are boundedly rational: their policy preferences are ultimately determined by their interests, but because of cognitive limitations and the complexity of the environment they face, they are forced to rely on heuristics and other cognitive short-cuts in order to make decisions.[21]

Komiya notes, for example, that both prior to WWII and during the post-War catch-up period, Japanese policy-makers used two criteria for deciding which industries to promote: they had to be symbols of industrial might that had already been pursued by countries more advanced than Japan, and they had to be large enough that they could capture public attention.[22] This is closer to a "logic of appropriateness" explanation, in which Japanese policy-

include not only the possession of particular technologies but also the ability to use those technologies effectively. See Ha-Joon Chang's argument in Justin Lin and Ha-Joon Chang, "Should Industrial Policy in Developing Countries Conform to Comparative Advantage or Defy it? A Debate Between Justin Lin and Ha-Joon Chang," *Development Policy Review* 27, no. 5 (2009): 483–502.

[17]Nicholas Crafts, "Overview and Policy Implications," in *Learning From Some of Britain's Successful Sectors: An Historical Analysis of the Role of Government*, BIS Economics Paper 6 (March 2010), 3–4.

[18]Saadia M. Pekkanen, *Picking Winners?: From Technology Catch-up to the Space Race in Japan* (Stanford University Press, 2003), 11.

[19]James A. Brander and Barbara J. Spencer, "Export subsidies and international market share rivalry," *Journal of International Economics* 18, no. 1 (February 1985): 83–100; Crafts, "Overview and Policy Implications," 4.

[20]See Pack, *The Case For Industrial Policy* for an overview of some of these critiques.

[21]James G. March, "Bounded Rationality, Ambiguity, and the Engineering of Choice," *The Bell Journal of Economics* 9, no. 2 (1978): 587–608; Herbert A. Simon, "Human Nature in Politics: The Dialogue of Psychology with Political Science," *American Political Science Review* 79, no. 2 (June 1985): 293–304; James G. March, *A Primer on Decision-Making* (New York: Free Press, 1994); Bryan D. Jones, "Bounded Rationality and Political Science: Lessons from Public Administration and Public Policy," *Journal of Public Administration Research and Theory* 13, no. 4 (October 2003): 395–412.

[22]Ryutaro Komiya, "Introduction," in *Industrial Policy of Japan*, ed. Ryutaro Komiya, Masahiro Okuno,

makers are promoting those industries they believe an advanced economy *should* have, rather than an economically rational one. Having now caught up with other economies, Japan's decisions in terms of what sectors to promote have become more difficult, but Pekkanen has found that Japanese government officials still favor promoting cutting-edge technology, seeing it as key for the future economic survival of Japan.[23] As I will discuss in Chapter 3, past experience and its effects on policy-makers' beliefs about the probability of success can also affect whether they choose to promote a sector.

Governments may also promote certain sectors or technologies not for purely economic reasons, but to fulfill some other goal. Probably the most common goal is defense: states worry about being dependent on other countries for technologies necessary to their national security.[24] But addressing other societal challenges, for example improving environmental conditions, may also provide motivation for government support of particular technologies.[25]

This dissertation also seeks to better understand how policy-makers consider trade-offs when deciding whether to promote a particular technology. There are clearly potential security and economic advantages to promoting an indigenous cyber security sector, yet the Japanese government has decided not to do so. I argue that what is puzzling in isolation is understandable when considered within the context of broader economic goals: there are trade-offs between strengthening the cyber security sector, and strengthening the cyber security of the broader economy, and without a strong national security apparatus to push for the former, Japan has decided on the latter. These effects of these trade-offs, particularly when considering capital goods rather than consumer goods, is something to which more attention could be paid in the literature.

Cyber Security Promotion

The policy outcome variable, promotion of adoption, refers to government efforts to encourage firms and individuals to consume or adopt cyber security technologies. *Technologies* refers not only to cyber security products or services, but also to practices. The latter are critically important in ensuring cyber security—anti-virus software does one little good if one does not make certain to keep it updated, and even the most sophisticated server defenses do one little good if employees use obvious passwords. A wide range of instruments fall under this category, from regulations to ad campaigns.

and Kotaro Suzumura (San Diego, CA: Academic Press, 1988), 8.

[23]Pekkanen, *Picking Winners?*, 7–8.

[24]Ethan Barnaby Kapstein, "International Collaboration in Armaments Production: A Second-Best Solution," *Political Science Quarterly* 106, no. 4 (1991): 657–675; Richard J. Samuels, *"Rich Nation, Strong Army": National Security and the Technological Transformation of Japan* (Cornell University Press, 1994); Richard A. Bitzinger, "Reforming China's defense industry," *Journal of Strategic Studies* 39, nos. 5-6 (September 2016): 762–789; Marc R. Devore, "Arms Production in the Global Village: Options for Adapting to Defense-Industrial Globalization," *Security Studies* 22, no. 3 (July 2013): 532–572.

[25]Jong-Tsong Chiang, "From 'mission-oriented' to 'diffusion-oriented' paradigm: the new trend of U.S. industrial technology policy," *Technovation* 11, no. 6 (September 1991): 339–356; Mazzucato and Penna, "Beyond Market Failures," 22–24.

While a clear literature speaks to sector promotion, the applicable literature here is less clear. The literature on market failures, which can be used to explain under-consumption of goods, are clearly relevant, but are better for explaining the cause of the problem and why government action can help, rather than why a government would actually choose to intervene.[26] There is also a recent policy literature on government actions aimed at the demand side to promote technological diffusion, but which focuses primarily on the design and effectiveness of these activities rather than on why governments choose to pursue them.[27] This dissertation should help shed some light on what is clearly a rising trend, though there are of course differences between cyber security technology and ICT technology more broadly.

While not addressing this specific outcome, on why states adopt different policy responses to similar (or to the same) problems applies here. Roughly speaking, there are three sets of explanations: resources/material capabilities; domestic societal explanations; and domestic institutional explanations.

Resources/Material Capabilities

The classic example of a capabilities-based explanation is the neo-realist explanation for state strategies for ensuring their own security. According to neo-realism, states all face the same security concerns: they are in constant danger of being attacked by another state. In order to defend themselves, they have one of three options: to build up their own military capabilities to the point where they can match any possible threat (internal balancing); to ally with other states who have similar military capabilities against more powerful states or groups of states (external balancing); or to ally with a far more powerful state (bandwagoning). All states would prefer to internally balance, because they cannot trust other states; but in the case where they do not have the capabilities to do so, they are forced to externally balance or to bandwagon.[28]

Resource-based approaches can be used to explain economic policies as well. Though it is not his primary explanation, Ikenberry mentions that different resource conditions could explain the different responses of states to oil shocks. States which produce much of their own required energy are better insulated from oil shocks than those which do not, and so do not need to pursue as drastic adjustment policies.[29]

[26]See Robert G. Harris and James M. Carman, "Public Regulation of Marketing Activity: Part I: Institutional Typologies of Market Failure," *Journal of Macromarketing* 3, no. 1 (June 1983): 49–58 for a good description of possible market failures and their consequences. I discuss this further in Chapter 4.

[27]J. Edler et al., "Evaluating the demand side: New challenges for evaluation," *Research Evaluation* 21, no. 1 (March 2012): 33–47; Janice A Hauge and James E. Prieger, "Demand-Side Programs to Stimulate Adoption of Broadband: What Works?," *Review of Network Economics* 9, no. 3 (January 2010).

[28]Kenneth Neal Waltz, *Theory of International Politics* (McGraw-Hill, January 1979); Robert Owen Keohane, *Neorealism and Its Critics* (Columbia University Press, 1986); Colin Elman, "Horses for courses: Why nor neorealist theories of foreign policy?," *Security Studies* 6, no. 1 (September 1996): 7–53.

[29]G. John Ikenberry, "The Irony of State Strength: Comparative Responses to the Oil Shocks in the 1970s," *International Organization* 40, no. 1 (1986): 119–120.

In this particular case, a resource-based explanation does not hold. For one, the state which does not promote the adoption of cyber security technology, the U.S., is the wealthiest of the three. For another, there are any number of inexpensive instruments for promoting the adoption of cyber security technology. It is difficult to imagine a lack of resources being a reason for any advanced industrial country to choose not to pursue this policy.

Societal Explanations

Societal explanations point at differences in interest groups and social coalitions as the reason for differences in policy responses. Generally, these explanations rely on a combination of differences in the strength of particular groups (for example, industry versus agriculture) or the differences in the interests of the same types of groups (industry that benefits from free trade versus industry that benefits from protectionism).

A good example of this is Peter Gourevitch's study of state responses to the Great Depression. He argues that while all states began with an "orthodox" policy of deflation, each eventually broke with this policy. However, the degree to which they broke with orthodoxy, and the policies they adopted in its place, depended upon the strength and interests of particular social groups in each state.[30]

Another example is Snyder's work on great power over-expansion. Though all great powers have to be concerned with their security, some respond with expansion, while other do not. He argues that states choose expansion due to domestic coalitions that have their own reasons for wanting military expansion and economic autarky.[31]

An more recent example is Heiginbotham's argument about the decisions states in East Asia make about whether to invest in land or naval forces. He argues that the former have reason to make common cause with more autocratic, nationalistic civilian leaders, while the latter have reason to make common cause with liberal, democratic civilian leaders.[32] Thus he argues that the rise in maritime force-building in East Asia since the 1980s can be better explained by the rise of more liberal political leaders than by changes to the security environment.[33]

While interest groups certainly do play a role in determining policy for promoting the adoption of cyber security technology, in this case there are not clear, systematic differences in strength or interests of social groups that would explain the differences in outcome. Indeed, arguably the state that has a strong social group that would clearly benefit from policies promoting the adoption of cyber security technology is the U.S.: the U.S. has a number of large cyber security firms, and these would profit from other actors investing

[30]Peter Alexis Gourevitch, "Breaking with Orthodoxy: The Politics of Economic Policy Responses to the Depression of the 1930s," *International Organization* 38, no. 1 (1984): 95–129.

[31]Jack Snyder, *Myths of Empire: Domestic Politics and International Ambition* (Cornell University Press, 1991).

[32]The reasons why are in part materialistic, and in part for organizational sociological reasons, which gives a sense of how these different approaches can be mixed.

[33]Eric Heginbotham, "The Fall and Rise of Navies in East Asia: Military Organizations, Domestic Politics, and Grand Strategy," *International Security* 27, no. 2 (October 2002): 86–125.

more heavily in cyber security. Yet it is the U.S. that does not pursue these policies, while Japan and South Korea, which do not have strong cyber security sectors, do. While there are differences in firm preferences between states—Japanese firms are more welcoming of government involvement than U.S. firms—these are a result of differing policy legacies, which provide a better explanation for the differences in outcomes than differences in interests.

Institutional Explanations

Institutional explanations point to differences in formal or informal procedures, routines, norms, and conventions as the cause of differences in policy outcomes. This covers a wide range of explanations, and I will not attempt to make an exhaustive list.[34] Instead, I will cover two of the major themes: that institutions affect outcomes via the capacities they make available to states, and that they affect outcomes via ideas, which in turn shape actor preferences.

Explanations involving capacities can be roughly divided into two sets. One set of explanations claim that all states would prefer to have the same policy response, but that institutions affect how well or quickly they can do so. For example, Taliaferro argues that states that face high external vulnerability would like to emulate the military, governing, and technological practices of the most successful states in the international system. Whether or not a state can actually do so, however, is determined by whether the state has institutions that allow it to effectively extract and mobilize domestic resources.[35] Dyson similarly argues that while international conditions shape state security policy over the long run, the level of executive autonomy in military matters determines how quickly adjustment occurs. In particular, low autonomy can lead to policy stasis over the medium term.[36]

A second set claims that different institutions give states different sets of policy instruments, and states formulate different policy responses depending on the tools available to them. The difference between this and the previous set of explanations is that in this case, there is no assumption that states will eventually converge on a policy. An example of this is Ikenberry's argument that France, Japan and Germany, and the U.S. developed different policy responses to the oil shocks of the 1970s because each had different sets of instruments that could be applied to the solution: France had institutions for central planning and government-owned energy enterprises; Japan and Germany had institutions for corporatist bargaining and financial and guidance mechanisms; and the U.S. had little government planning structures, but could use regulatory decontrol and budget expenditures. As a re-

[34]For broader coverage of institutional theory, see Peter A. Hall and Rosemary C. R. Taylor, "Political Science and the Three New Institutionalisms," *Political Studies* 44, no. 5 (December 1996): 936–957; Edwin Amenta and Kelly M. Ramsey, "Institutional Theory," in *The Handbook of Politics: State and Civil Society in Global Perspective*, ed. Kevin T. Leicht and J. Craig Jenkins (New York: Spring, 2010), 15–39.

[35]Jeffrey W. Taliaferro, "State Building for Future Wars: Neoclassical Realism and the Resource-Extractive State," *Security Studies* 15, no. 3 (September 2006): 464–495.

[36]Tom Dyson, "Convergence and Divergence in Post-Cold War British, French, and German Military Reforms: Between International Structure and Executive Autonomy," *Security Studies* 17, no. 4 (December 2008): 725–774.

sult, the French government took control of the production of energy, both domestically and by negotiating state-to-state contracts; Germany and Japan encouraged energy efficiency and phased out industries that relied heavily on oil (such as petrochemicals); and the U.S. reduced government control over energy, allowing the price to better reflect supply.[37] Similarly, Weir and Skocpol's argument that the difference between the responses of the Social Democratic government in Sweden and the Labour Party government in U.K. to unemployment caused by the Great Depression can be explained by the existing policies of each for dealing with unemployment also falls under this category. In essence, because the Labour Party had established unemployment insurance prior to the Depression, it relied on this to deal with unemployment during the Depression, while the Social Democratic government, which did not have an established unemployment insurance program available, relied instead on public works programs.[38]

Turning to ideas, I again discuss two sets of explanations: that institutions affect what ideas find their way into the policy-making system, and that institutions shape the ideas that actors themselves hold. The former set of explanations takes as a given that certain actors have certain ideas. Institutions affect the policy outcome by determining which actors are able to insert their ideas into the policy-making system. Again, Weir and Skocpol provide an example, arguing that the reason Sweden established a social Keynesian policy after the Great Depression was because they had institutional mechanisms that allowed economic experts to participate in public policy making.[39]

The second set of explanations does not take ideas as a given, but instead explain those ideas as a result of learning and socialization. These ideas then shape actor preferences, which in turn affect policy outcomes. "Ideas" run a fairly wide gamut. On the one extreme, they can be as simple as heuristics developed in response to some earlier experience, and then maintained through socialization. Goldstein, for example, argues that U.S. defense of free trade developed as a reaction to the experience of the Great Depression, from which policy-makers took the lesson that high trade barriers would lead to negative economic consequences. Though the lowering of trade barriers was originally a short-term measure, intellectuals and others interpreted the following recovery as due to the lowering of trade barriers. This built support for continued free trade, and it eventually became a norm.[40] On the other extreme, ideas can refer to actors' self-conceptions and their conceptions of others. An example is Katzenstein's argument that Germany and Japan's differing conceptions of the strength of their own societies and the nature of the international order led them to taking different approaches when dealing with terrorism.[41] This shaping of ideas does not

[37]Ikenberry, "The Irony of State Strength."

[38]Margaret Weir and Theda Skocpol, "State Structures and the Possibilities for "Keynesian" Responses to the Great Depression in Sweden, Britain, and the United States," in *Bringing the State Back In*, ed. Peter B. Evans, Dietrich Rueschemeyer, and Theda Skocpol (Cambridge: Cambridge University Press, 1985), 120–125.

[39]Ibid., 120,125–132.

[40]Judith Goldstein, "The Political Economy of Trade: Institutions of Protection," *The American Political Science Review* 80, no. 1 (1986): 161–184.

[41]Peter J. Katzenstein, "Same War: Different Views: Germany, Japan, and Counterterrorism," *Interna-*

have to take place on the level of the state; sub-state institutions can shape the ideas of actors within those institutions as well.[42]

Many institutional arguments include more than one of these mechanisms, and my own argument is no exception. My own argument draws both on the idea that policy legacies make certain policy instruments available, and that it is easier to adapt these existing instruments to new uses than to invent completely new instruments; and on the idea that past policy decisions form norms about appropriate policy responses. In the latter case, my argument falls somewhere in between the two extremes listed above. I argue that the policy legacy does not simply create heuristics for the government to follow, but also that it creates norms among the wider population about what counts as "appropriate" or "normal" government behavior.

1.2 Policy Legacies

Policy legacies affects policy outcomes in a two main ways. Most obviously, they create certain administrative capacities, which cannot be easily shifted to other purposes, due to the costs involved. This in turn helps to shape policy-makers' ideas about what policies are feasible. New policies which rely on existing instruments are relatively easy to devise and implement, while those which require new instruments are more difficult.[43]

Policy legacies also create ideas among policy-makers about what types of problems they should be looking to solve. If a state has a legacy of maintaining strong traditional security capabilities, then government actors will be conditioned to be looking for potential national security weaknesses that require a response. If a state has a legacy of economic guidance, then government actors will be conditioned to look for economic risks that must be ameliorated, or economic opportunities that must be ceased. Thus, policy legacies provide both problems and likely solutions.

These factors are reinforced when policy legacies include the creation of bureaucratic organizations to implement the policy. Because bureaucratic organizations justify their budget and autonomy through their activities, they are especially likely to look for and generate solutions to problems of the type they were created to solve.[44] They also have available to them an existing set of instruments for solving those particular types of problems. Thus,

tional Organization 57, no. 4 (2003): 731–760.

[42]For a good overview of ideas and institutions more broadly, see John L. Campbell, "Institutional Analysis and the Role of Ideas in Political Economy," *Theory and Society* 27, no. 3 (1998): 377–409.

[43]In the main, this draws from Weir and Skocpol, "State Structures and the Possibilities for "Keynesian" Responses to the Great Depression in Sweden, Britain, and the United States," 120–125, though is only one of the institutional factors they discuss in this work; the other, state structure and its effects on the adoption of new ideas by the government, is not an important part of my explanation. Ikenberry, "The Irony of State Strength"; Katzenstein, "Same War" also discuss how available policy instruments shape policy.

[44]For a discussion of bureaucratic motives for problem-seeking, see E. Kawabata, "Dual Governance: The Contemporary Politics of Posts and Telecommunications in Japan," *Social Science Japan Journal* 7, no. 1 (April 2004): 21–39.

bureaucratic actors are particularly likely to develop problems and their solutions along the lines of the policy legacy which created them.

Beyond these main factors, policies that substantially follow an existing policy legacy are more likely to be successfully implemented because they are less likely to draw opposition from social groups. There are two reasons for this. One, policy legacies often create entrenched interests, and substantial deviation these legacies potentially harms these interests. Two, policies that reflect long-standing policy legacies are less likely to be questioned simply because over time they come to be taken as a "given" by most actors.[45]

Capability Maintenance

The key policy legacy that determines whether a state promotes its cyber security sector is whether or not it has sought to maintain strong traditional national security capabilities. One reason is that policy-makers are more likely to consider the national security advantages of promoting a strong cyber sector. Because policy-makers are in the habit of considering what technologies are necessary for the maintenance of strong national security capabilities, they are inclined to consider this question for cyber security technology as well. This does not mean, of course, that they always support indigenous technological development over purchasing technology from abroad, but it does mean they will consider the question.

Beyond being more likely to seriously consider the security advantages of indigenous technologies in general, countries with this policy legacy are more likely to have actors who are specifically familiar with the potential risks of relying on foreign cyber security technology. They may be involved in offensive operations themselves, or at the very least will have received training about such operations, and therefore are more likely to be familiar with the risks involved in purchasing security products and services from abroad. Moreover, they are likely to be more worried about foreign access to their own networks, which are key to national defense, than other actors would be.

The national security organizations that result from this legacy are also more likely to need specialized cyber security tools than are other actors. They may wish to develop these tools themselves, or to hire a firm in order to create the tools for them. Given that many of these tools become less effective if an adversary learns of or acquires them, there is a clear incentive to maintain a strong indigenous work force that can build these tools under conditions of secrecy.

Finally, as a practical matter, this policy legacy creates a set of instruments that can be used to provide a source of funding and support for the indigenous cyber security sector: those same instruments for supporting other indigenous technologies necessary for defense. Procurement by the military or intelligence agencies is one such instrument, but R&D and other instruments may have been developed as well. This can be especially helpful in the

[45]Campbell's concept of "ideas as public sentiments" perhaps comes closest, but it is not always the public that matters—it could be firms or some other actor, depending on the issue. See Campbell, "Institutional Analysis and the Role of Ideas in Political Economy," 392–394.

early stages of a particular technology, when it may be promising or useful for national security purposes, but not yet ready for the market.[46]

Though I will not go into a detailed comparison of the three countries' policy legacies here, it is possible to get a sense of the differences simply by looking at defense spending. The U.S. spends more on defense than any other country in the world, between 3.1–4.7% of GDP from 2003–2017. While South Korea does not come close to the United States in terms of spending, it still spent between 2.3–2.6% of GDP on defense during that time period. By contrast, Japan's defense spending was at most 1% of GDP during that time.[47]

Beyond these differences in spending, Japan's policy legacy has primarily restricted its ability to maintain traditional security capabilities. Until relatively recently, Japan did not even have a Ministry of Defense; instead, its armed forces were overseen by the Japan Defense Agency, which was staffed by bureaucrats from other ministries. Article 9 of the Japanese Constitution strictly limits the role of the Japanese Self-Defense Forces. Moreover, legally the Self-Defense Forces are strictly limited in terms of what they can do on Japan's own soil. While Japan does have intelligence agencies, they are relatively small (as importantly for this dissertation, they also play no role in cyber security policy).

It should be noted that, ever so slowly, these policies have been changing. In 2007, the JDA was reformed into the Ministry of Defense and given its own Cabinet position. In 2013, the position of the MOD was strengthened further when Prime Minister Abe established the National Security Council in the Cabinet Office; its 60 staff members are partly made up of bureaucrats from the MOD (the others come from the Ministry of Foreign Affairs). The government also passed a law allowing the JSDF to participate in collective defense, albeit in a limited fashion.[48] It is possible that we will look back and see these changes as having set the foundation for a different policy legacy, one focused on maintaining strong traditional security capabilities, but we are far from that point yet.

[46]Because it deals with a different set of problems than individuals or firms, technologies that are often not yet useful for the market can be very useful for the government. An example of this is machine translation, of which the U.S. government, especially the military and intelligence agencies, was an early supporter. For companies, machine translation was not particularly useful unless it produced near-perfect translations, because the goal was to translate user manuals and similar documents for customers. By contrast, what the U.S. government needed to do was take a huge number of documents it had acquired from overseas and figure out which ones it should spend its intelligence resources on. Being able to take a large number of documents in Farsi that might be about a uranium program, translate them enough for a "first glance" to see whether they actually seemed to actually be about the topic of interest, and then pass those that were on to analysts that could actually read Farsi was of enormous advantage to the government, and did not require the machine translation to be anywhere near perfect. Similarly, one can imagine an AI-based cyber security program that successfully detects intrusion 65% of the time might not be a worthwhile investment for a company, but might well be useful as one more layer of defense for military networks.

[47]Stockholm International Peace Research Institute, *SIPRI Military Expenditure Database*, 2018, accessed July 30, 2018, `https://www.sipri.org/sites/default/files/3_Data%20for%20all%20countries%20from%201988%E2%80%932017%20as%20a%20share%20of%20GDP.pdf`.

[48]See Andrew L. Oros, *Japan's Security Renaissance: New Policies and Politics for the Twenty-First Century* (Columbia University Press, March 2017) for a good overview of the ways in which Japan's national security institutions have been strengthening.

Economic Guidance

Japan is is many ways the paradigm of economic guidance. Post-WII, the Ministry of International Trade and Industry (MITI) and the Ministry of Finance (MOF), along with other ministries, played a strong role in regulating market behavior and promoting particular industries. They promoted savings and investment, encouraged banks to provide loans to favored sectors, managed competition between firms, and diffused technological knowledge and promoted research collaboration. The ministries also worked with industry associations, which both lobbied the government and made certain industry complied with government directives.[49] While increasing openness to trade and investment, the "catching up" of Japan's economy, and the financial crisis and "lost decade" have all changed the government's role over time, it continues to play a guiding role in the economy, promoting technological upgrades, joint ventures meant to encourage innovation, and so forth.[50]

The government role in guiding the economy in South Korea had been, if anything, even stronger than Japan's, relying more on a top-down approach rather than the intermediary associations that Japan has used. Its main form of control had been through the allocation of capital.[51] Though structural reforms imposed by the IMF after the 1997 financial crisis liberalized the financial sector in South Korea and removed this particular tool from the government's toolbox, it has continued to play a strong guiding role in the economy, in part balancing against business interests by coordinating with labor.[52]

By contrast, the U.S. is the arch-typical example of a liberal market economy.[53] This is not to say that the U.S. government does not shape the economy, but it does so primarily by "setting the rules" and then letting market mechanisms take over, rather than by coordinating directly with firms.[54] There is no American equivalent of MITI/METI. This trend has only increased since the 1980s, when market fundamentalism became a motivating ideology of the Republican party.[55]

Why does this lead to differences in the promotion of cyber security? For one, when there

[49]Vogel, *Marketcraft*, 78–79. See also Johnson, *Miti and the Japanese Miracle*; Okimoto, *Between MITI and the Market*.

[50]Steven K. Vogel, *Japan Remodeled: How Government and Industry are Reforming Japanese Capitalism* (Cornell University Press, 2006), 217–218; Sébastien Lechevalier, *The Great Transformation of Japanese Capitalism*, trans. J.A.A. Stockwin, Nissan Institute/Routledge Japanese Studies Series (New York, NY: Routledge, 2014), 81.

[51]Peter B. Evans, *Embedded Autonomy: States and Industrial Transformation* (Princeton University Press, March 1995), 53.

[52]Dong-Myeon Shin, *Social and Economic Policies in Korea: Ideas, Networks and Linkages* (Abingdon, Oxon: Routledge, 2003), 177–179,188–191.

[53]See, for example, Peter A. Hall and David Soskice, "Introduction," in *Varieties of Capitalism: The Institutional Foundations of Comparative Advantage*, ed. Peter A. Hall and David Soskice (New York: Oxford University Press, Inc., 2001), 27–33.

[54]See Vogel, *Marketcraft*, 43–76 for an overview of how the U.S. shapes the market.

[55]Fred Block, "Innovation and the Invisible Hand of Government," in *State of Innovation: The U.S. Government's Role in Technology Development*, ed. Fred Block and Matthew R. Keller (Boulder, CO: Paradigm Publishers, 2011), 1–30.

is a policy legacy of economic guidance, there are governmental actors who see promoting cyber security in the private sector as part of their responsibilities. Cyber security is not simply an issue of traditional, national security, but has economic consequences as well. Fears that their data may be stolen may make consumers less likely to use internet services, reducing efficiency and harming competitiveness. Other countries may steal technology from domestic firms, reducing a country's overall competitive edge. Most obviously, attacks on critical infrastructure could cause enormous economic harm. If a government takes a "hands off" approach to the economy, then it is likely to see this a problem for the private sector to solve. But for a government used to guiding economic policy, this problem is similar to technological diffusion and other similar issues of economic coordination. Thus, we would expect the government to play a similar role here.

Not only is the government of a country with a legacy of economic guidance more likely to act, but firms are more likely to accept the government's role in promoting cyber security in the private sector. After all, such firms are already used to the government playing a coordinating role in other areas of the economy. This is not to say, of course, that the interests of firms and government will necessarily align, but that firms will not simply reject government action out of hand. By contrast, in countries where the government does not play a strong role in coordinating the economy, firms are much more likely to be opposed to government action, since this deviates from existing norms.

Finally, a government that is already involved in economic guidance has on hand the tools and capacities required to promote cyber security. The same mechanisms that allow it to coordinate and influence firms for purely economic reasons can be turned to diffusing cyber security technology and best practices. This includes networks between government and firms, which can be used both to gather information and advice from firms, and in return educate or pressure them. By contrast, a government which takes a "hands off" approach to the economy does not have such tools readily available. Even were it to build such tools specifically for cyber security, it would take some time before they reached the efficiency of those tools used by governments in which economic guidance is commonplace; moreover, the government may not feel as though building such tools *solely* for cyber security is worth the cost, assuming it could even be managed.

The rest of the dissertation proceeds as follows: in Chapter 2, I discuss how the policy legacies of each country have been embedded in particular bureaucratic organizations, which are in large part responsible for the ultimate policy outcomes. In Chapter 3, I discuss the sector promotion policies of each country in more detail, and argue that it is not just Japan's lack of national security institutions that have led to its lack of sector promotion, but also an earlier failed experience in promoting the software sector. In Chapter 4, I discuss the cyber security promotion policies of each country in more detail, and explain why despite the differences in policy legacies, there is convergence in one key area: all three countries have policies to promote cyber security in critical infrastructure sectors. Finally, in Chapter 5 I review the argument, discuss the implications of this dissertation, and consider some future avenues of research.

Chapter 2

Bureaucratic Organizations

In this chapter, I further lay the grounds for the argument introduced in the introduction. In Japan, a legacy of post-war anti-militarism and "developmental state" economic policies has led to a situation in which economic bureaucratic organizations have a stronger role in cyber security policy-making than national security institutions. In the U.S., the situation is the opposite: a history of strong national defense and intelligence capabilities give the national security organizations a strong role, while the fact that it is a liberal market economy means that there are no strong advocates for the promotion of cyber security in the private sector. Finally, South Korea has both a legacy of maintaining strong traditional security capabilities and a history of economic guidance, providing it with both the motives and instruments for strong sector promotion and cyber security promotion.

2.1 Japan

In Japan, four bureaucratic actors play a particularly strong role in cyber security policy-making: the Ministry of Defense (MOD), the National Police Agency (NPA), the Ministry of Internal Affairs and Communications (MIC), and the Ministry of Economy, Trade and Industry (METI). MOD is, of course, part of Japan's national security apparatus, while MIC and especially METI play a strong role in economic guidance. NPA does not fit into either category: it has some national security concerns, particularly in terms of cyber terrorism, but for the most part is concerned with cyber crime.

These four bureaucratic actors shape policy both within their own jurisdictions, and, more broadly, through a pair of bodies within the Cabinet Office. Until the Cybersecurity Basic Law was passed in 2015, these two bodies were the Information Security Policy Council (ISPC) and its Cabinet Secretariat, the National Information Security Center (NISC). The ISPC was established by the order of the Prime Minister in May 2005. It was located under the Information Technology Strategic Headquarters (ITSH) in the Cabinet Office. Chaired by the Chief Cabinet Secretary, its members included the Minister of Internal Affairs and Communications; the Minister of Economy, Trade and Industry; the Chairman of the Na-

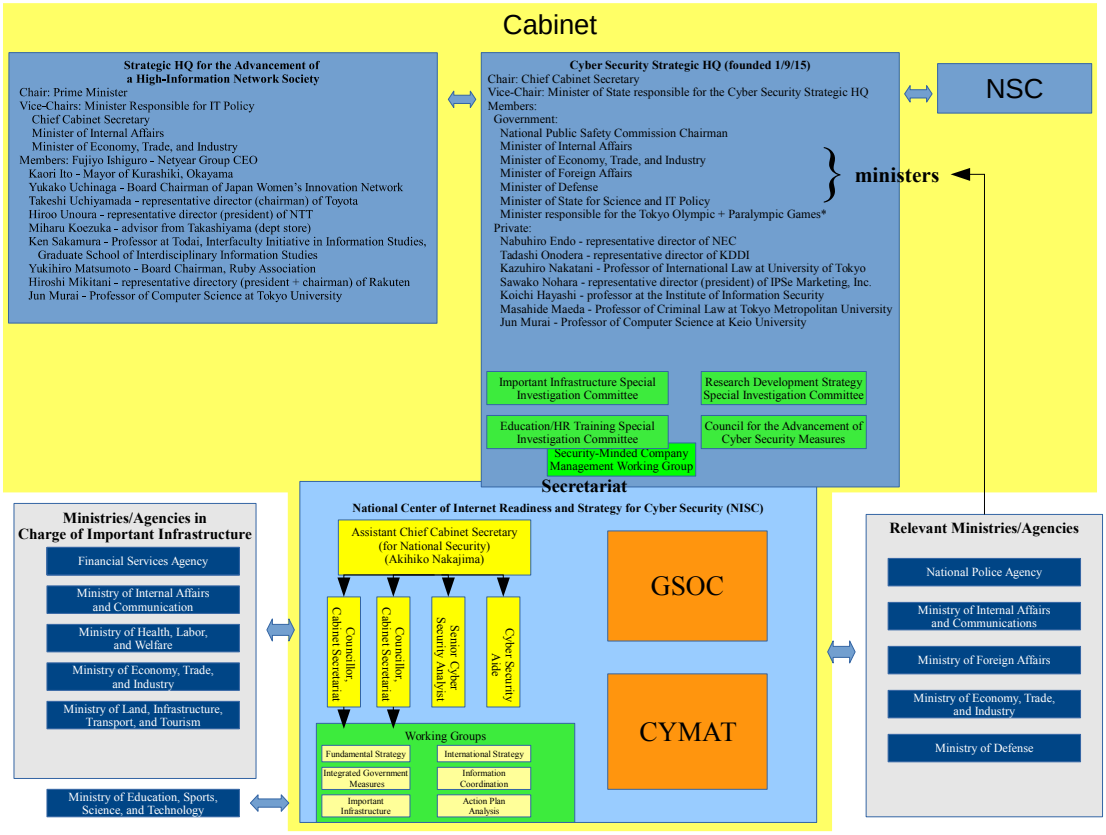

Figure 2.1: Japan's cyber security policy-making system

tional Public Safety Commission (who is in charge of the NPA); the Minister of Defense; and the Minister of State for Science and Technology Policy, who served as vice chair. It also included six experts from the private sector. In 2012, the Minister of Foreign Affairs was added as well, though the Ministry of Foreign Affairs mainly deals with international negotiations involving cyber security, and so does not play a major role in the issues discussed in this dissertation.[1] In 2015, ISPC was replaced with the Cyber Security Strategic Headquarters (CSSH), which has its own Minister of State and is directly under the authority of the Prime Minister rather than under the ITSH. One more outside expert was added, but the CSSH is otherwise similar in composition and role to the ISPC.[2]

[1]Motohiro Tsuchiya, "Cyber Security Governance in Japan: Two Strategies and a Basic Law," in *Information Governance in Japan: Towards a New Comparative Paradigm*, ed. Kenji E. Kushida, Yuko Kasuya, and Eiji Kawabata (Silicon Valley New Japan Project, 2016).

[2]National center of Incident readiness and Strategy for Cybersecurity, 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 *[About Support for Strenghtening Cyber Security Measures]* [in Japanese], technical

The National Information Security Center (NISC), which served as the secretariat for ISPC, was founded slightly earlier, in April 2005; it was renamed to the National center of Incident readiness and Strategy for Cybersecurity in 2015, when the CSSH was created, but continues to serve in much the same role. While major policy decisions are made in ISPC/CSSH, much of the ground-work and the details of implementation are left to NISC. Though it may appear to be its own agency, with the exception of some of the technical staff it is staffed by bureaucrats from MIC, METI, MOD, and NPA. Thus, it too serves as an arena in which these four organizations can collectively make policy decisions. NISC also 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.

Beyond being involved in policy-making, NISC has several duties assigned to it by the 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.[3]

The drafting of the cyber security strategies which form the core of Japanese cyber security policy is done by the bureaucrats staffing NISC, with input from outside experts. Drafting has sometimes been done in working groups set up for that express purpose, and more recently by the expert members of the ISPC/CSSH themselves.[4] The relevant ministers and the Chief Cabinet Secretary have input as well, but because of their limited time and divided attention, the details are mainly left to the bureaucrats and experts. Decisions are

report 9 (November 2016), accessed November 21, 2016, http://www.kantei.go.jp/jp/singi/keizaisaisei/miraitoshikaigi/4th_sangyokakumei_dai2/siryou9.pdf; Cyber Security Strategic Headquarters, サイバーセキュリティ戦略本部　第 *1* 回会合　議事概要 *[Cyber Security Strategic Headquarters, First Meeting, Summary of Proceedings]* [in Japanese], February 2015, accessed March 24, 2017, http://www.nisc.go.jp/conference/cs/dai01/pdf/01gijigaiyou.pdf; National center of Incident readiness and Strategy for Cybersecurity, サイバーセキュリティ戦略本部　名簿 *[Cyber Security Strategic Headquarters, Register of Names]* [in Japanese], April 2016, accessed March 24, 2017, http://www.nisc.go.jp/conference/cs/pdf/meibo.pdf; Ryusuke Masuoka and Tsutomu Ishino, *Cyber Security in Japan (v.2)*, technical report (Center for International Public Policy Studies, December 2012), accessed November 20, 2016, http://www.cipps.org/group/cyber_memo/003_121204.pdf.

[3]Cabinet Secretariat of Japan, 内閣官房組織令（抄）*[Order for the Organization of the Cabinet Secretariat (Excerpt)]* [in Japanese], accessed March 23, 2017, http://www.nisc.go.jp/law/pdf/soshikirei.pdf.

[4]Tsuchiya, "Cyber Security Governance in Japan: Two Strategies and a Basic Law."

made by consensus between these actors.

Each of the four bureaucratic actors has its own interests vis-a-vis cyber security. MOD views cyber security primarily through the lens of national security. Due to constitutional constraints, this has not meant the development of offensive cyber weapons.[5] Instead, MOD's main interest is in defending the networks of its own facilities, and those of the Japan Self-Defense Forces. This is no small task, since the JSDF in particular has a large communications system that has suffered from cyber attacks.[6] MOD has also identified cyber security as a technological base necessary for the defense of Japan, and so has an interest in supporting indigenous cyber security technology.[7] Protecting critical infrastructure is also a priority for MOD, since the JSDF relies on this infrastructure.

The NPA sees cyber security through the lens of criminal justice; it is mainly concerned with identifying, catching, and prosecuting cyber criminals. While the other three bureaucratic organizations focus primarily on strengthening the security of networks and devices to prevent attacks, NPA is interested in being able to identify and prosecute attackers. Thus, it favors policies that make it easier to collect information about cyber attacks.[8]

MIC has jurisdiction over telecommunications, and as such its main interest is in improving the cyber security of Japan's network. Thus, it is less concerned with attacks on specific companies, than on distributed-denial-of-service attacks, malware, bots, and other cyber security threats that slow down the network as a whole. These types of threats are only becoming worse as the Internet of Things becomes a more widespread phenomenon, increasing the number of devices that can be infected by malware or bots.[9]

MIC is also interested in maintaining individual privacy. The Supreme Court has ruled that Article 13 of the Japanese Constitution, which guarantees the right to life, liberty, and happiness, includes the protection of personal information[10], and MIC sees itself as the protector of this right. Conveniently, protecting this right has often coincided with another one of MIC's interests, making certain that internet service providers (ISPs) are not unduly burdened with regulations forcing them to store and keep large amounts of data.[11]

METI's main interest is in promoting competitiveness and creating a "sound business environment". In terms of cyber security, "sound business environment" means reducing the number of cyber security incidents for Japanese companies. It is also interested in improving the security of Japan's products and services, since it believes this will provide Japanese

[5]Though there has been some recent debate about this. See Mihoko Matsubara, *How Japan's Pacifist Constitution Shapes Its Approach to Cyberspace*, May 2018, accessed July 15, 2018, `https://www.cfr.org/blog/how-japans-pacifist-constitution-shapes-its-approach-cyberspace`.

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

[7]Ministry of Defense, *Strategy on Defense Production and Technological Bases: Toward strengthening the bases to support defense forces and 'Proactive Contribution to Peace'*, June 2014, 30, accessed June 20, 2018, `http://www.mod.go.jp/atla/soubiseisaku/soubiseisakuseisan/2606honbuneigo.pdf`.

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

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

[10]*Judgment concerning the constitutionality of Kyoto City Ordinance No. 10 of 1954 on Assembly, Marching, and Demonstration*, December 1969, 162.

[11]Interviews with MIC official and NPA official, Tokyo, July 2017.

firms with a competitive edge over foreign firms.[12] METI sees itself as different from the other ministries, focusing on the "national interest" rather than particularistic interests. As Ito Hiroshi, Deputy Direct-General for Cybersecurity and Information Technology at METI writes, "Other ministries and agencies distribute the national interest, METI exists to promote it..."[13] As industrial promotion has become less important, due to the maturity of Japan's industry and the end of the period of high growth, METI has looked for new areas in which it can play a role.[14] Cyber security provides METI a particularly good opportunity, since the need to coordinate between different firms plays to one of its major strengths: the networks it has within Japan's private sector.

Though MOD has reason to want an indigenous cyber security, it has difficulty in turning its preferences into policy. This is for two reasons: one, it is at a disadvantage to the other actors, especially METI and MIC, in terms of determining national policy (though this disadvantage has been somewhat lessening over time); two, it is extremely limited in its ability to implement policy on its own.

One of the disadvantages MOD has versus METI and MIC is it that it is still relatively new as a ministry. When ISPC and NISC were first formed, MOD did not yet exist. Instead, what would become MOD was called the Japan Defense Agency (JDA). Because it was not a ministry, it was not represented in the Cabinet. Moreover, it was primarily staffed with bureaucrats from other ministries, which greatly reduced its political power. In 2007, however, the Diet passed legislation establishing MOD as a cabinet ministry.[15] This, along with the establishment of the National Security Council (NSC) in 2013, has strengthened its position vis-a-vis the other ministries. Nevertheless, it is not nearly as experienced a bureaucratic actor as the other ministries.

MOD also does not have a strong network of experts to draw upon. By and large, outside experts have been allied with and tied to METI and MIC.[16] This means that while MIC and METI can point to expert opinion to support their positions, MOD lacks similar support. This makes it more difficult to convince others of its preferred positions.

More than its weaknesses in influencing policy, however, it is the restrictions on MOD's ability to implement policies, which derive from the legacy of Japan's post-WWII demilitarization, that limit its influence. Because Japan's national security policy is entirely defensive, the Self-Defense Forces (SDF) cannot easily be deployed to deal with cyber security attacks. Without clear orders, MOD and the SDF cannot protect cyber systems outside of their own. At the same time, it is not clear what conditions would call for such orders. It is one thing to mobilize the SDF in response to an imminent physical attack; it is diffi-

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

[13] 経産省は他の省庁と異なり国益を配分するのではなく増進させるための役所だ...

[14] Ulrike Schaede, "From developmental state to the 'New Japan': the strategic inflection point in Japanese business," *Asia Pacific Business Review* 18, no. 2 (April 2012): 167–185.

[15] Yuki Tatsumi, *Japan's National Security Policy Infrastructure: Can Tokyo Meet Washington's Expectation?* (Washington, DC: Henry L. Stimson Center, 2008).

[16] Interview with MIC official, Tokyo, July 2017.

cult to imagine an obvious analogous situation for cyber attacks.[17] Indeed, since most cyber operations are below the threshold of an armed attack, the SDF has little leeway to act.[18]

Moreover, MOD's budget is quite limited; though there is no legal restriction on its budget, by tradition it is kept under 1% of GDP. Given that it has to divide this budget between a number of priorities, including maritime security and missile defense, this leaves it with few resources to deal with cyber security. Moreover, until recently, the Ministry of Finance was reluctant to fund its proposed cyber security programs.[19] It was not until 2014 that the Ministry of Defense was finally given funding to establish 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.[20] Even now, this unit has only 110 members.[21] This lack of funding means that it cannot effectively serve as a source of funds for the cyber security sector, be it through procurement or R&D.

Beyond the specific weaknesses of the Ministry of Defense, the Japanese government's approach to cyber security is particularly notable for the lack of involvement of the intelligence agencies. This is both true for policy-making and implementation of cyber security policy. While in both the U.S. and South Korea, the intelligence agencies play a large role in dealing with cyber attacks, the intelligence agencies in Japan cannot share intelligence with NISC, which limits their usefulness in this regard. They are further limited by Japanese law, which only allows monitoring of communication in response to crimes, not for prevention of future crime or attacks. Their extreme secrecy also limits the role they can play in policy-making.[22] Moreover, the intelligence agencies lack the funding and work force of intelligence agencies in other countries. For example, the Directorate for Signals Intelligence, which is under the MOD and is the Japanese equivalent of the National Security Agency, employs about 1,700 people; by contrast, the NSA has a workforce of over 30,000, and the U.K.'s signals intelligence agency has a workforce of more than 6,000.[23] They are thus an even less likely source of funding for the cyber security sector than the Self-Defense Forces.

By contrast to the national security organizations, those bureaucratic organizations involved in economic guidance—METI and MIC—are quite strong, both in terms of their ability to affect policy and in their capacity to implement it. One of the major strengths METI and MIC have is each other: worried about the possible policy recommendations of MOD and NPA, the two have formed an alliance to make certain their own policy preferences

[17]Tsuchiya, "Cyber Security Governance in Japan: Two Strategies and a Basic Law."

[18]Matsubara, *How Japan's Pacifist Constitution Shapes Its Approach to Cyberspace.*

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

[20]Ministry of Defense, "Establishment of the Cyber Defense Unit," *Japan Defense Focus*, no. 52 (May 2014), accessed April 16, 2017, `http://www.mod.go.jp/e/jdf/sp/no52/sp_activities.html#article03`.

[21]Franz-Stefan Gady, "Japan's Defense Ministry Plans to Boost Number of Cyber Warriors," *The Diplomat*, July 2017, accessed August 2, 2018, `https://thediplomat.com/2017/07/japans-defense-ministry-plans-to-boost-number-of-cyber-warriors/`.

[22]Tsuchiya, "Cyber Security Governance in Japan: Two Strategies and a Basic Law"; Ryan Gallagher, *The Untold Story of Japan's Secret Spy Agency*, May 2018, accessed August 2, 2018, `https://theintercept.com/2018/05/19/japan-dfs-surveillance-agency/`.

[23]Gallagher, *The Untold Story of Japan's Secret Spy Agency.*

win out, and so coordinate with one another on cyber security policy.[24]

Though MIC and METI were both created in 2001 as part of administrative reform, both are the successors to earlier ministries, the Ministry of Posts and Telecommunications (MPT) in the case of MIC, and the Ministry of International Trade and Industry (MITI) in the case of METI. As such, both are far more experienced bureaucratic actors than MOD. Though "bureaucratic experience" is a difficult thing to measure directly, one example of the results of this experience is the way in which the two ministries control a key position in NISC. The head of NISC is the Director-General; however, since the Director-General is also the Assistant Chief Cabinet Secretary for National Security, they are too busy to manage the day-to-day affairs of NISC. Instead, day-to-day management of NISC falls to one of two Deputy Director-Generals—who is always a bureaucrat seconded either from MIC or from METI.[25] This gives MIC and METI quite a bit of control over the affairs of NISC.

Another strength of MIC and METI is that both have strong connections with cyber security experts in academia in the private sector, due to their involvement in information and communications technology policy more broadly.[26] They can rely on the authority of these experts to reinforce their own policies.[27]

It is their ability to implement their preferred policies, however, that truly explains why Japan has an active cyber security promotion policy. MIC has jurisdiction over telecommunications policy. In this role it regularly confers and coordinates with telecommunications companies and internet service providers. METI is in charge of industry more broadly. As a result of such coordination, METI and MIC have formal and informal networks they can use to get advice from and provide advice and information to firms.

Both MIC and METI are further strengthened by overseeing incorporated administrative agencies which perform specific cyber-security-related functions. These agencies have two major advantages for MIC and METI. One, they are staffed with experts, providing a source of expertise for policy advice and for proper implementation of policy. Two, while MIC and METI have wide responsibilities, these agencies have narrower missions: in part, their very existence is justified by their role in cyber security. This means that they are highly motivated to find ways to strengthen Japan's cyber security without heavy oversight from MIC or METI.

MIC oversees the National Institute of Information and Communications Technology (NICT), an incorporated administrative agency. It promotes research in information technology and forms ties with and between academia and business.[28] NICT contains a number

[24]Interview with MIC official, Tokyo, July 2017.

[25]Tsuchiya, "Cyber Security Governance in Japan: Two Strategies and a Basic Law."

[26]Both MIC and METI are represented in the IT Strategic Headquarters, which fulfills the same function for ICT policy as the Cyber Security Strategic Headquarters does for cyber security policy.

[27]It helps, of course, that for the most part these experts have similar policy preferences to MIC and METI. Author's interview with MIC official, Tokyo, July 2017.

[28]National Institute of Information and Communications Technology, *About NICT | NICT Charter | NICT-National Institute of Information and Communications Technology*, accessed March 24, 2017, `https://www.nict.go.jp/en/about/charter.html`.

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[29], cryptographic technologies, and privacy protection technologies.[30] 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.[31]

METI oversees the Information-technology Promotion Agency (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 about cyber security trends and threats; it shares this information with government, business, and the public. It also runs other programs meant to improve Japan's cyber security.[32]

MIC and METI also work with cyber-security-related business organizations. These organizations also work to provide cyber-security-related services and information to their members. Two of the most important are ICT-ISAC, supported by MIC, and IPA, supported by METI.

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 a number of working groups dedicated to sharing and analyzing information about various 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.[33]

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

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

[30]National Institute of Information and Communications Technology, *Cybersecurity Research Institute | NICT-National Institute of Information and Communications Technology*, accessed March 24, 2017, `https://www.nict.go.jp/en/csri/`.

[31]National Institute of Information and Communications Technology, *Cryptographic Protocol Verification Portal (CPVP)*, accessed March 24, 2017, `http://crypto-protocol.nict.go.jp/index_en.html`.

[32]Information-technology Promotion Agency, *IPA Information-technology Promotion Agency, Japan : IPA:Business Outline*, accessed March 24, 2017, `http://www.ipa.go.jp/english/about/outline.html`.

[33]Kazuaki Omori, *Cybersecurity Policy and Projects by Ministry of Internal Affairs and Communications (MIC)*, Tokyo, November 2016, 16–17, accessed February 20, 2018, `https://www.oasis-open.org/events/sites/oasis-open.org.events/files/1.6%20MIC%20Kazuaki%20Omori.pdf`; ICT-ISAC Japan, *ICT-ISAC Japan*, accessed February 20, 2018, `https://www.ict-isac.jp/english/index.html#Member`.

the global Forum of Incident Response and Security Teams (FIRST) in 1998.[34] Though JPCERT/CC receives funding from METI, METI does not directly oversee its activities. JPCERT/CC's existence as an independent, private organization is a key selling point to the firms it encourages to join in its information sharing program.[35] JPCERT/CC serves several functions. First, it actively monitors the internet for threats. After analyzing any threats it may detect, it transmits this information to its constituents. Second, 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. Finally, it coordinates with other CSIRTs, both within Japan (where it acts as the "CSIRT of CSIRTs") and internationally.[36] JPCERT/CC's incident response activities serve as an incentive for companies to 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.

In summation, the relative weakness of Japan's national security organizations limit their influence over cyber security policy. By contrast, Japan's long tradition of public-private economic coordination has created organizations, MIC and METI, with a strong motivation to promote cyber security in the private sector, and the instruments to do so. I turn now to the U.S. case.

2.2 The U.S.

The U.S. has, since the end of World War II, had a policy of maintaining strong traditional security capabilities. National security is seen as a vital role of government and is a major subject of political rhetoric. As a result, while in Japan cyber security tends to be seen through the lens of public safety and economic stability, in the U.S. it is primarily seen as an

[34]JPCERT/CC, *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 [JPCERT Coordination Center, About JPCERT/CC: The Various Activities of JPCERT/CC]* [in Japanese], accessed April 16, 2017, `http://www.jpcert.or.jp/about/05.html`, Author's interviews with Masaki Ishiguro, Mitsubishi Research Institute, January 2017, and with JPCERT/CC employee, Tokyo, July 2017.

[35]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.

[36]JPCERT/CC, *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 [JPCERT Coordination Center, About JPCERT/CC: The Various Activities of JPCERT/CC]*; JPCERT/CC, *JPCERT コーディネーションセンターインシデント対応とは？[JPCERT Coordination Center: What is Incident Response?]* [In Japanese], accessed February 20, 2018, `https://www.jpcert.or.jp/ir/`; JPCERT/CC, *JPCERT Coordination Center Activities*, accessed April 12, 2017, `https://www.jpcert.or.jp/english/pr/index.html`.

issue of national security.[37] It is the national security organizations in the U.S. which have both the authority and capability to deal with the cyber security issue.

While in Japan the bureaucracy plays a strong role in creating national cyber security policy, in the U.S. this is left to Congress, at least in theory. In practice there is no overarching legislative framework; instead, there are a number of laws that touch on aspects of cyber security, the last of which was passed in 2009.[38] Nevertheless, bureaucratic organizations play a strong role in implementation of policy, and have some flexibility in how they do so.

Two of the most important bureaucratic actors in this area in the U.S. are the military and the intelligence agencies. As in Japan, both have to worry about maintaining the security of their own networks, but unlike Japan, both maintain offensive as well as defensive cyber capabilities. This means that they have a greater need for specialized tools than the Japanese Self-Defense Forces. As a result, they have a strong incentive to maintain a strong indigenous cyber security sector, both so they can have such tools developed by the private sector, and so that they have a source of human capital—people they can hire to build the tools internally.[39]

As important as their interests, the military and intelligence agencies have the resources to support the cyber security sector. The cyber security budget for the Department of Defense in 2017 alone was over $7 billion (not including the budget of the National Security Agency, which is kept secret); by contrast, the cyber security budget for the entire government of Japan was around $600 million.[40] Moreover, research and development funding for national security purposes receives consistent support from Congress, in contrast to funding for other purposes.[41] In short, the U.S. has a set of strong national security institutions, which has in turn created actors both motivated and enabled to promote the cyber security sector.

By contrast, because it does not share Japan's history of economic guidance, the U.S. lacks actors that are both willing and able to promote domestic cyber security. It is perhaps telling that the bureaucratic organization in charge of domestic cyber security is another national security organization: the Department of Homeland Security (DHS), which was made the official lead for cyber security in 2003. DHS is in charge of coordinating the

[37]For an in-depth discussion of the way in which the cyber security issue is framed within the U.S., see Myriam Dunn Cavelty, *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age* (Routledge, November 2007).

[38]Eric A Fischer, *Federal Laws Relating to Cybersecurity: Overview of Major Issues, Current Laws, and Proposed Legislation*, December 2014, 2–3,62–71 This last law was the Health Information Technology for Economic and Clinical Health Act; arguably the last major cyber-security-related law was the E-Government Act of 2002.

[39]It helps that, unlike in Japan, workers moving between government and the private sector is not unusual in the U.S.

[40]Office of Management and Budget, "21. Cyber Security Funding," in *An American Budget: Analytical Perspectives* (Washington, D.C.: U.S. Government Publishing Office, 2017), 273–287, accessed July 23, 2018, `https://www.whitehouse.gov/wp-content/uploads/2018/02/ap_21_cyber_security-fy2019.pdf`; National center of Incident readiness and Strategy for Cybersecurity, 政府のサイバーセキュリティに関する予算 *[Government Budget Related to Cyber Security]* [in Japanese], 2017, accessed April 22, 2017, `https://www.nisc.go.jp/active/kihon/pdf/yosan2017.pdf`.

[41]Block, "Innovation and the Invisible Hand of Government," 6–15.

security of civilian government networks, and of providing cyber security support to critical infrastructure sectors.[42]

A few factors keep DHS from playing a similar role in promoting cyber security that METI and MIC play in promoting cyber security in Japan. One problem is that DHS was created in 2002 as an integration of all or part of 22 different federal departments. As a result, it has a wide variety of duties, including, but not limited to, customs and immigration, emergency management, and transportation security. This wide range of competing responsibilities make it difficult for DHS to play a leading role in cyber security the way that METI or MIC does—much less NICT or IPA, with their even narrower missions. It also reduces the incentives for DHS to play this kind of role, since it can easily justify its continued existence based on its existing roles. Critical infrastructure firms have complained about a lack of communication from DHS, even when they were supposed to be working together to develop voluntary cyber security measures. These problems are exacerbated by a lack of cyber security expertise within the department.[43]

DHS is also weak for jurisdictional and budgetary reasons. Despite its responsibilities for protecting the cyber security of critical infrastructure, Congress has not granted DHS any regulatory power over critical infrastructure firms. Instead, regulatory powers fall to the respective regulatory agencies for each sector. This means that even if DHS wanted to push firms in critical infrastructures to improve their cyber security, it has very little leverage to do so. Its cyber security budget is also small, particularly relative to the Department of Defense.[44] Because it is not responsible for coordinating with the private sector the way MIC and METI are, it lacks the networks necessary to informally put pressure on firms to improve their cyber security.[45] In short, even if DHS wanted to promote cyber security in the private sector, it lacks a good set of tools for doing so.

There is one narrow area in which the U.S. government has been involved in economic guidance, and that is in standard-setting. The National Institute of Standards and Technology (NIST) is housed within the Department of Commerce. It was established in 1901 in order to formulate industrial measures and standards, and has a strong history of working with industry to develop these standards. Because of its small budget and lack of regulatory powers, it cannot play the same kind of role as METI or MIC, but to the degree that the U.S. has promoted cyber security in the private sector, it has primarily been through NIST.[46]

Beyond the lack of institutions for economic guidance, arguably the very strength of U.S. national security institutions prevent the government from playing a stronger role in promoting cyber security in the private sector. The National Security Agency (NSA) and collects information in part by successfully breaking into the machines of foreign governments

[42]P. W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know®* (Oxford University Press, December 2013), 200–201.

[43]Charlie Mitchell, *Hacked: The Inside Story of America's Struggle to Secure Cyberspace* (Rowman & Littlefield, June 2016), 81–100.

[44]Singer and Friedman, *Cybersecurity and Cyberwar*, 200–2001.

[45]Mitchell, *Hacked*, 81–110.

[46]Ibid., 46–47.

and organizations. In order to do so, it needs vulnerabilities in software to exist. Likewise, such vulnerabilities are necessary for operations like STUXNET, the malware which the centrifuges Iran was using to enrich uranium.[47] The U.S. government pays bounties for zero-day exploits (flaws in software that are not known about by the company that makes the software, and which therefore do not have a fix available), which it then keeps to itself for use in cyber operations. The NSA has also been accused of pressuring NIST to weaken cryptographic standards to make it easier for the NSA to decipher the communications of targets of interests.[48]

Nor is it solely those national security organizations with overseas operation that push for weaker cyber security. The Federal Bureau of Investigations (FBI) has lobbied for various ways of weakening cryptography, either via companies keeping track of cryptography keys themselves so that they could decrypt customer data when provided with a warrant by the FBI, or by having cryptography algorithms produce a special key which the FBI could use to decrypt any data. These efforts have met with quite a bit of resistance, since they would greatly weaken the security of encrypted data, and have, so far, been unsuccessful.[49] It is clear, however, that the national security lens through which the government views cyber security has given it mixed motives vis-a-vis cyber security in the private sector.

In summation, the strong national security institutions of the United States has created actors with both the incentives and the resources to promote an indigenous cyber security sector. However, due to its liberal market economy, it does not have institutions that can be readily turned to promoting cyber security in the private sector. What is more, its strong national security institutions may actually make it more difficult for the government to play a role in doing so. I turn now to South Korea, which has both a legacy of maintaining strong traditional security capabilities and of economic guidance.

2.3 South Korea

As one might expect given the legacy of the Korean War and the continuing threat of North Korea, South Korea has maintained strong traditional security capabilities. As with the U.S., these strong national security institutions result in actors with both the interest in promoting and means to promote indigenous cyber security technology.

The two main national security actors are the Ministry of National Defense (MND) and the National Intelligence Service (NIS). Though South Korea does not conduct the world-spanning military and intelligence operations of the U.S., nevertheless, they require offensive cyber capabilities to deal with North Korea, as well as other possible adversaries. Thus, for much the same reason as the military and intelligence agencies in the U.S., MND and NIS

[47]Kim Zetter, "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History," *Wired*, July 2011, accessed July 18, 2018.

[48]Singer and Friedman, *Cybersecurity and Cyberwar*, 199–200; Mitchell, *Hacked*, 146.

[49]Singer and Friedman, *Cybersecurity and Cyberwar*.

have good reason to want a strong indigenous cyber security sector. Indeed, one of the roles of MND is specifically to develop applicable cyber technologies.[50]

In some ways, these two actors are better positioned to push for their preferred policies than even the U.S. security organizations. While these two ministries do not have the direct role in national cyber-security policy-making that the Japanese bureaucratic organizations have, they have a stronger role than the bureaucratic agencies in the U.S. This is because while South Korea, like the U.S., has a presidential system (albeit with unicameral legislative body, the National Assembly), in the South Korean system the President can introduce legislation into the National Assembly. Thus, even though much of national cyber security policy is made through legislation, as in the U.S., the bureaucracy has input into the legislative process through the President, who consults with the relevant ministries on these issues.[51]

Though not nearly as well-funded as the U.S. national security organizations, South Korea does spend between 2.3–2.6% of its GDP on defense.[52] As a sense of the seriousness with which it takes the cyber security issue, MND has approximately 1,000 cyber troops (approximately ten times as many as Japan), and has recently established a research and development institution dedicated solely to developing defense-oriented cyber security technology.[53] The NIS runs the National Cyber Security Center (NCSC) which handles government security: preventing cyber threats and investigating security incidents related to the government and the public sector; holding strategy meetings; and developing cyber security master plans. It also heads a joint response team composed of members of the private, public, and military sectors.[54] Both organizations are thus well-placed to play a strong role in cyber security policy.

Thus we can see that, like the U.S., South Korea has powerful national security organizations with the motive and the means to promote an indigenous cyber security sector. Unlike the U.S., however, South Korea also has a policy legacy of economic guidance. Indeed, during its developmental period the South Korean government in some ways played a "stronger" role than the Japanese government, in the sense that it relied more on top-down

[50]Korea Internet and Security Agency, *Information Security in Korea*, 2015, 1, accessed April 23, 2018, https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/KISA_Information_Security_in_KOREA.pdf; Yong Seok Oh, *Current Cybersecurity Trends and Responses in Korea*, October 2015, 15, accessed April 23, 2018, http://www.kisa.or.kr/uploadfile/201610/201610071003367061.pdf.

[51]Jooha Lee, "Politics of Policy-Making in Korea and Japan" (University of Tokyo, Tokyo, Japan, October 2007), 10–11, accessed August 1, 2018, http://www.welfareasia.org/4thconference/papers/Lee_Politics%20of%20Policy-Making%20in%20Korea%20and%20Japan.pdf.

[52]Stockholm International Peace Research Institute, *SIPRI Military Expenditure Database*.

[53]Sam Kim, "South Korea enlists cyber warriors to battle Kim Jong-un's regime," *Independent Online*, November 2015, accessed June 21, 2018, http://global.factiva.com/redir/default.aspx?P=sa&an=INDOP00020151128ebbs004h6&cat=a&ep=ASE; Ministry of National Defense, Republic of Korea, *2016 Defense White Paper*, 2016, 78–79, accessed April 20, 2018, http://www.mnd.go.kr/user/mndEN/upload/pblictn/PBLICTNEBOOK_201705180357180050.pdf.

[54]Korea Internet and Security Agency, *Information Security in Korea*, 1; Oh, *Current Cybersecurity Trends and Responses in Korea*, 15.

commands than the Japanese government's more consensual approach.[55] Like Japan, this has left it with bureaucratic organizations whose role is to regulate, coordinate with, and implement policies related to firms in particular sectors of the economy.

For cyber security, the important ministry in this regard is the Ministry of Science and ICT (MSIP), formally known as the Ministry of Science, ICT and Future Planning. MSIP plays a similar role to Japan's MIC, in the sense that it is in charge of telecommunications, but unlike MIC it is also specifically in charge of science and technology promotion. As with MND and NIS, it can influence legislation through the President. Most importantly, MSIP is in charge of the Korea Internet & Security Agency (KISA). KISA is responsible for preventing and responding to cyber security threats in the private sector, raising public awareness about cyber security, and promoting cyber security industries and technologies.[56] What is key is that it was the Korean government's drive to build a strong ICT infrastructure that led to the founding of three agencies—the Korea Information Security Agency, the National Internet Development Agency of Korea, and Korea IT International Cooperation Agency—that would eventually be merged into KISA. The government's role in guiding the development of South Korea's ICT sector led to the creation of an agency that is tasked with promoting private security in the private sector.

Thus, we can see that as a result of its legacies of maintaining strong traditional security capabilities and of economic guidance, South Korea has bureaucratic actors willing and able to promote the cyber security sector, and actors willing and able to promote the adoption of cyber security technology in the private sector. As with the U.S., however, the presence of strong national security institutions in some ways inhibits the ability of the government to promote cyber security in the private sector. In particular, because the military and intelligence agencies supported South Korea's authoritarian regimes in the past, South Koreans worry about the concentration of authority over cyber security policy in the MND and NIS. This fear has been reinforced by a scandal in which agents from the NCSC were accused of interfering in the 2012 elections in support of the main conservative party; the NIS admitted it had done so in 2017.[57] This distrust makes public-private cooperation more difficult, and has often held up otherwise uncontroversial legislation meant to improve cyber security. Worth noting is that MSIP, an economy-oriented organization and not a national security one, does not draw these same suspicions.

[55]Evans, *Embedded Autonomy*, 53.

[56]Korea Internet and Security Agency, *Information Security in Korea*, 1; Oh, *Current Cybersecurity Trends and Responses in Korea*, 15.

[57]Donghui Park, *Cybersecurity Spotlight: South Korea*, January 2016, accessed April 19, 2018, `https://jsis.washington.edu/news/cybersecurity-spotlight-south-korea/`; Justin McCurry, "South Korea spy agency admits trying to rig 2012 presidential election," *The Guardian*, August 2017, accessed June 30, 2018.

2.4 Conclusion

The institutions that have been built up around national security and economic guidance have a strong influence on the cyber security policy-making of a country. In Japan's case, a legacy of the developmental state is strong economic bureaucratic agencies, MIC and METI, which play a large role in cyber security policy-making. In part, this strength derives from the norms of public-private economic coordination: because there are already mechanisms for coordination between MIC and METI, and firms see the government's role as coordinator as legitimate, these mechanisms could be easily turned to the promotion of cyber security. By contrast, the legacy of demilitarization after World War II has left Japan with a relatively weak set of national security institutions. Because the Self-Defense Forces can only be used for defense, the Ministry of Defense does not have as strong incentives to procure or otherwise support indigenous cyber security technologies as it otherwise might. Exacerbating this is the fact that, beyond defending its own networks, the SDF cannot play a strong role in cyber security defense, since cyber security attacks do not generally rise to the level where they would be considered military attacks. Moreover, limits on funding limit its ability to promote cyber security technologies.

In the case of the U.S., the building of strong national security institutions post-WWII and the clear national security implications of cyber security have empowered the military and intelligence agencies to play a strong role in cyber security policy. While naturally the military and intelligence agencies need strong cyber security capabilities in order to defend their own networks, the fact that they need offensive capabilities in order to fulfill their missions provides particular incentives for these organizations to support an indigenous cyber security sector. A strong indigenous cyber security sector both allows them to fund and purchase particular tools that they need, and as importantly, provides a ready source of human capital from which they can hire if needed. Their role in offensive cyber operations also means they are more aware of the ways in which foreign governments can exploit cyber security technologies that are sold to other countries. On the other hand, because the U.S. has a liberal market economy, it does not have strong institutions for economic guidance. As a result, there are not, for the most part, government actors with a strong interest in promoting cyber security in the private sector, and not good mechanisms for doing so even should they be interested.

South Korea has both strong national security institutions and strong institutions for economic guidance. Because North Korea is an ever-present threat, South Korea has developed strong military and intelligence organizations; because offensive cyber operations are a key tool for North Korea, these organizations are deeply involved in cyber security policy. These organizations have a strong interest in promoting an indigenous cyber security sector for much the same reasons as the U.S. military and intelligence organizations. The government's developmental legacy, particularly in regard to information and communications technology, means that there is are bureaucratic actors with a strong interest in promoting cyber security in the private sector; indeed, for KISA, this is essentially the reason for its existence.

Chapter 3

Sector Promotion

To reiterate the argument from the introductory chapter, advanced industrial economies with strong national security institutions will promote their cyber security sector. Actors who are socialized within national security institutions are more aware of the security implications of relying on foreign cyber security products. Well-funded national security organizations can use procurement, and often research and development funds, as instruments to promote indigenous cyber security. In countries with strong national security institutions, national security is also a ready-made excuse for such sector promotion, while a purely economic excuse would not be so clear. National security organizations also require specialized cyber security tools and cyber security expertise, something that a strong indigenous cyber security sector can provide. This last is especially true if national security organizations participate in offensive cyber operations.

As discussed in Chapter 2, due to its demilitarization post-WWII, Japan does not have strong national security institutions. This has left it without strong advocacy for cyber sector promotion, and indeed as will be demonstrated below, it does very little to promote the cyber security sector. By contrast, both the U.S. and South Korea, with much stronger national security institutions, do far more to promote indigenous cyber security sectors.

However, while this does an adequate job of explaining South Korean and U.S. behavior, in reality this does not fully explain Japanese behavior. While the economic argument for the promotion of cyber security is not as clear as the national security argument, there is an argument for it. Were Japan a liberal market economy, this economic argument would not matter—the government would be left to itself. But the Japanese government does play a strong role in coordinating the economy, and as such, it is possible that it would be moved by an economic argument to promote the cyber security sector. However, there are two reasons why the Japanese government was not convinced: the trade-offs between sector promotion and the promotion of cyber security in the private sector more broadly; and the government's previous experience in failing to promote the indigenous software sector.

This chapter proceeds as follows: first, I lay out the national security case for promoting an indigenous cyber security sector. Then I discuss the Japanese, American, and Korean efforts to promote their respective cyber security sectors, and demonstrate that it is the

Policy Legacies		Policy Outcomes
Security Capabilities Maintenance	Public-Private Economic Guidance	
Weak	Weak	No
Weak	Strong	No
Strong	Weak	Yes
Strong	Strong	Yes

Figure 3.1: The basic argument: a policy legacy of maintaining a strong traditional security capabilities leads to cyber security sector promotion.

strength of their national security institutions that explain these outcomes. Returning to the Japanese case, I describe the economic case for cyber security sector promotion, and then discuss why the Japanese government has found this case unconvincing.

3.1 National Security and Cyber Security Promotion

In terms of national security, a strong cyber security sector is useful both for defensive and offensive purposes. In terms of defense, security products developed in another country may have backdoors or other flaws introduced into it by the foreign government. Of course, this is true of information technology more broadly, but there are two reasons why this problem is compounded for cyber security products. For one, in the case of other IT products, there is some chance that security products will pick up on backdoors or at least prevent their exploitation; if the security products themselves are compromised, it is more likely to go undetected. For another, in order to function, many security products need administrative access, meaning that they can access any file, including system files. This makes them particularly useful for backdoor access.

An example of the latter is anti-virus programs. In order to function properly, anti-virus programs must have complete access to a computer, including all of the files on a computer's hard drive. This is because viruses and malware can attach themselves to files (including system files), as well as embed themselves in other parts of an operating system's configuration (such as the Windows System Registry).[1] This means that trust in the company that creates the anti-virus program is vital, since you are effectively giving that company total access to your computer.

We can see the risk of relying on foreign firms by looking at the situation playing out right now between the U.S. government and Kapersky Lab. It is a cyber security company located in Moscow. Kapersky Lab had, until recently, a stellar reputation within the cyber security industry and among cyber security experts (and to a great degree, still does). Its experts are particularly respected for being able to find government malware; it was Kapersky

[1] Desiderio and Poulsen, "Exclusive."

Lab that successfully analyzed STUXNET, the malware allegedly developed by the U.S. and Israel which targeted Iranian nuclear centrifuges.[2] Tom's Guide, a well-respected information technology testing and ratings site, listed Kapersky Lab products as the best choices for both mid-range and premium security anti-virus programs.[3]

Despite its stellar reputation, Kapersky Labs is also known for working tightly with the Russian Federal Security Service (FSB), to the point where FSB agents are sometimes embedded in the company's headquarters. Despite this fact, Kapersky Lab products have been widely used by the U.S. government. In the wake of interference by Russia in 2016, however, the government became more worried about the connections between Kapersky Lab and the Russian government. This fear was worsened by an incident where the company uploaded classified documents and source code from the home computer of a National Security Agency contractor that had been running its software.[4] The incident may have been innocent on the part of Kapersky Lab: the source code was for an NSA hacking tool, which Kapersky Lab's software correctly identified as malware and flagged for analysis; because it was part of a archived file, it ended up uploading the classified documents in the archive as well. Nevertheless, it was a clear indicator of what Kapersky Lab *could* do.[5]

In December of 2017, the U.S. government enacted the National Defense Authorization Act (NDAA), one provision of which required the government to purge itself of any hardware, software, or services that were in whole or in part developed or provided by Kapersky Lab. This has turned out to be far easier said than done, since a range of companies, including software giants like Microsoft and major government suppliers of networking hardware such as Allied Telesis have used Kapersky software development kits, and thus have Kapersky code in their products. Despite continued efforts, the software has not yet been removed from U.S. government networks, and in fact it may be impossible to do so.[6] While it is unclear whether Kapersky Lab has helped the Russian government to obtain information from the U.S. or other governments, this example clearly demonstrates the risks that governments face in using foreign cyber security technologies.

Even if a cyber security company did not exfiltrate data itself, there could be good reasons to doubt the effectiveness of foreign cyber security software. One could imagine, for example, a foreign intelligence agency pressuring a foreign company to program its anti-virus software to ignore malware created by that intelligence agency.

Nor is it only anti-virus software (nor only the Russian and Chinese governments) of

[2]Lorenzo Franceschi-Bicchierai, *Who's Afraid of Kaspersky?*, May 2018, accessed July 18, 2018, `https://motherboard.vice.com/en_us/article/wjbda5/kaspersky-sas-conference-russia-spying`; Zetter, "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History."

[3]Paul Wagenseil and Staff, *Best Antivirus Software and Apps 2018*, July 2018, accessed July 18, 2018, `https://www.tomsguide.com/us/best-antivirus,review-2588.html`. Mid-range products include anti-virus and anti-malware programs, along with other tools such as a secure browser and protection against ransomware; premium products include more tools such as file encryption, password managers, and so forth.

[4]Desiderio and Poulsen, "Exclusive." The contractor was, of course, not supposed to have classified material on his home computer, and ended up pleading guilty to mishandling classified materials.

[5]Ibid.

[6]Ibid.

which other countries have to be wary. In the U.S., the FBI has been pushing for backdoors to be installed in encryption programs. These backdoors would allow the U.S. government to decrypt any data encrypted by one of these programs.[7] Leaving aside the fact that installing such backdoors would create a potential exploit for hackers as well, this would essentially give the U.S. government the ability to decrypt the data of anyone using the software, including foreign governments and other foreign actors. So far the FBI has been unsuccessful, in no small part due to push-back from the private sector, but should the U.S. government do so, it would be unsurprising if other governments followed course.

On the offensive side, a strong indigenous cyber security sector creates the necessary technological base for a government to develop offensive cyber security tools. In particular, it provides a source of human capital in the form of trained cyber security workers. Human capital is particularly important in developing tools for offensive operations, because in order to be successful tools have to exploit unknown flaws in the software. Once the flaw is known, it can be patched and the tool is no longer useful. This means that governments have to be constantly innovating and developing new tools, which makes human capital extremely important. This is different from more traditional weapons, where the same type of weapon can be useful for long periods of time.

3.2 Japan's Sector Promotion

While it is easy to describe the theoretical national security case for promoting an indigenous cyber security sector, such an argument only matters if there are actors who recognize this as a problem and have the ability to do something about it. In the case of Japan, the Ministry of Defense does recognize the national security importance of cyber security, and has listed cyber security as an important technological base. However, because of Japan's legacy of limiting its traditional security capabilities, MOD is limited in its ability to promote the cyber security sector. Much of this weakness derives from a lack of funding—beyond the fact that MOD has a number of spending priorities it has to meet on a limited budget, the Ministry of Finance has been reluctant to fund even its limited cyber security priorities. In fact, until FY2017, MOD did not have a cyber security budget. In FY2017, it was finally given a budget of 12.4 billion yen (around $111 million), which was then reduced to 11 billion yen in FY2018 (less than $100 million), despite the fact that MOD had requested 14.5 billion yen. Given that some of this funding has to be used to fund its Cyber Defense Group of 150 people, it does not have a lot left over for acquisition or R&D.[8]

Even if MOD were able to fund more R&D, it is not clear how easily it could find partners to do so. Though this has been easing somewhat, Japanese firms have traditionally been reluctant to make too public their involvement in the development of military technology.

[7] Adam Segal, *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age* (PublicAffairs, February 2016), 201–203.

[8] Crystal Pryor, "Japan's New Approach to Defense Technology," *The Diplomat*, November 2015, accessed August 1, 2018, `https://thediplomat.com/2015/11/japans-new-approach-to-defense-technology/`.

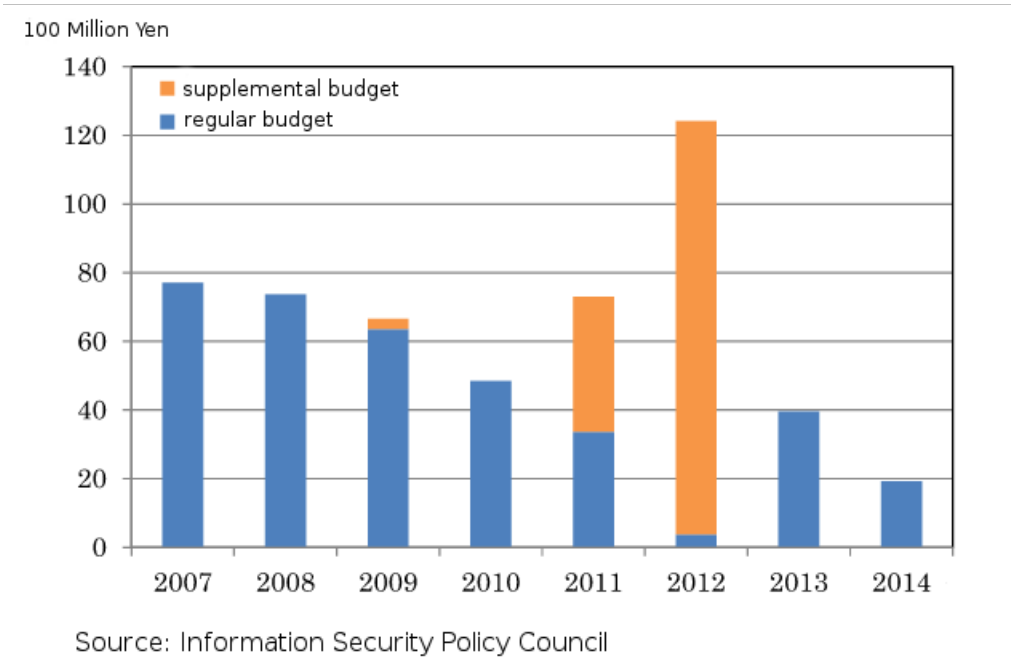

Figure 3.2: The Japanese government's research and development spending, 2007–2014.

Even though the government has been pushing to streamline defense R&D and acquisition, this reluctance on the part of the private sector continues to present it with real challenges.[9]

This is not to say that the Japanese government makes no efforts to promote the cyber security sector. It funds R&D projects, and also funds cyber security training programs in order to strengthen Japan's cyber security work force. However, can be seen in Figure 3.3, Japan's R&D spending is quite low as a percentage of GDP compared to the U.S. or South Korea. Moreover, these efforts are made by the economically-oriented ministries and agencies, not the national security ones. As I will discuss more below, METI in particular sees other IT-related technologies as a more likely source of future Japanese competitiveness than the cyber security sector. A result is that the efforts to promote cyber security technology are primarily aimed at strengthening the cyber security of other sectors, rather than at promoting the cyber security sector itself.

This focus on promoting the cyber security of other sectors is reflected in official policy documents. The First National Strategy on Information Technology promised that the government would promote R&D and technology development aimed at achieving mid- to long-term goals in the enhancement of IT infrastructure.[10] Likewise, the Second National Strategy mentions the importance of the enhancement of IT infrastructure and allowing users to use IT with a sense of security. It emphasizes that equipment should be safe and

[9]Pryor, "Japan's New Approach to Defense Technology."

[10]Information Security Policy Council, *The First National Strategy on Information Security*, February 2006, 27, accessed May 14, 2018, `https://www.nisc.go.jp/eng/pdf/national_strategy_001_eng.pdf`.

secure without any burden on the user.[11] The 2013 Cybersecurity Strategy was the first to mention specific technical goals: the development of technologies for cyber attack detection and analysis, encryption, technologies for dealing with more diverse and advanced forms of cyber attacks, security-supporting semiconductor devices, technologies that would inhibit integrated circuit operation errors, and technologies to assure the reliability of entire network systems. While some of these technologies could potentially be spun-off into standalone products, they are notable for being useful in securing network systems and control systems, such as consumer devices or systems used in critical infrastructure.[12] Along similar lines, the strategy promises efforts to strengthen research and development in machine-to-machine (M2M) "smart community" technologies, secure device technologies, anonymization and encryption technologies, technologies for software that can control entire networks according to various types of data, and identity verification technologies.[13] The 2015 Cybersecurity Strategy spends an entire section on securing IoT systems, as well as discusses the need to use R&D to improve detection and defense capabilities. It also describes the need to secure core technologies that may not be commercially viable.[14]

Further evidence that the government is primarily supporting the cyber security of other technologies can be seen in the projects it is currently funding. 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.[15] The last of these is of course aimed specifically at IoT devices. Technology to perform calculations on encrypted data is a tool useful for software-as-a-service (SaaS) and business-to-business functions, since it allows a company to operate on data (such as personal information) without being able to read the original data itself.[16] The first two technologies are useful for protecting networks, something in which MIC has a great deal of interest.

At the same time, METI was funding a project through the National Institute of Ad-

[11] Information Security Policy Council, *The Second National Strategy on Information Security*, February 2009, 42–44,63–64, accessed May 14, 2018, `https://www.nisc.go.jp/eng/pdf/national_strategy_002_eng.pdf`.

[12] Information Security Policy Council, *Cybersecurity Strategy*, June 2013, 43–44, accessed May 14, 2018, `https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Japan%20Cybersecurity%20Strategy%202013.pdf`.

[13] Ibid.

[14] Government of Japan, サイバーセキュリティ戦略 *[Cybersecurity Strategy]* [in Japanese], September 2015, 12–15,46–47, accessed July 17, 2017, `http://www.nisc.go.jp/active/kihon/pdf/cs-senryaku-c.pdf`.

[15] Cyber Security Strategic Headquarters, サイバーセキュリティ研究開発戦略 *[Cybersecurity Research and Development Strategy]* [in Japanese], July 2017, 30, accessed February 15, 2018, `https://www.nisc.go.jp/active/kihon/pdf/kenkyu2017.pdf`.

[16] As of now, what happens is that even if information is sent over a network encrypted, it must be decrypted on other end before any functions can be performed upon it. This increases the number of points at which data can be accessed.

vanced Industrial Science and Technology (AIST) to develop large-scale software analysis tools for verifying the validity of embedded systems for automobiles, and a project to develop technology for the high-speed processing of encrypted data, as well as attempting to create the "world's smallest cipher".[17] METI was also funding a project to develop technology to detect cyber attacks against control systems by analyzing system behavior, through the Control System Security Center (CSSC).[18] Again, what we see is a heavy emphasis on tools that are useful in securing control systems, and on cryptography, which is essential for secure communications. For example, the advantage of a small cipher is that it can be used to encrypt data on mobile devices.

Though not one of the main actors in implementing cyber security policy, the project sponsored by Ministry of Education, Culture, Sports, Science and Technology follows this pattern as well. Through the National Institute of Informatics (NII), an inter-university research institute, it is funding the construction of a system to collect and share communications data about cyber attacks related to machine-to-machine communications.[19] Machine-to-machine communications are used primarily in "smart" systems: "smart" grids which improve electric efficiency, electronic parking meters, manufacturing systems that use monitoring and feedback to improve production processes, and so forth.

NISC, too, follows this pattern in its project funding. The New Energy and Industrial Technology Organization (NEDO) is managing a major project initiated under NISC's Strategic Innovation Creation Program (SIP). The goal of this project is to develop technology that will ensure 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.[20] 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.[21] Participating in this project are a number of firms, including NTT, NTT Communications, Hitachi,

[17]Cyber Security Strategic Headquarters, サイバーセキュリティ研究開発戦略 *[Cybersecurity Research and Development Strategy]*, 30.

[18]Ibid.

[19]Ibid.

[20]Cyber Security Strategic Headquarters, サイバーセキュリティ研究開発戦略 *[Cybersecurity Research and Development Strategy]*, 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)], 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]* [in Japanese], April 2017, 8, accessed February 16, 2018, `http://www.nedo.go.jp/content/100767969.pdf`.

[21]New Energy and Industrial Technology Development Organization, *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 *[NEDO:Strategic Innovation Promotion Program/Ensuring the Cyber Security of Critical Infrastructure]* [in Japanese], 2017, accessed February 16, 2018, `http://www.nedo.go.jp/activities/ZZJP_100109.html`; 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)], 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]*, 12.

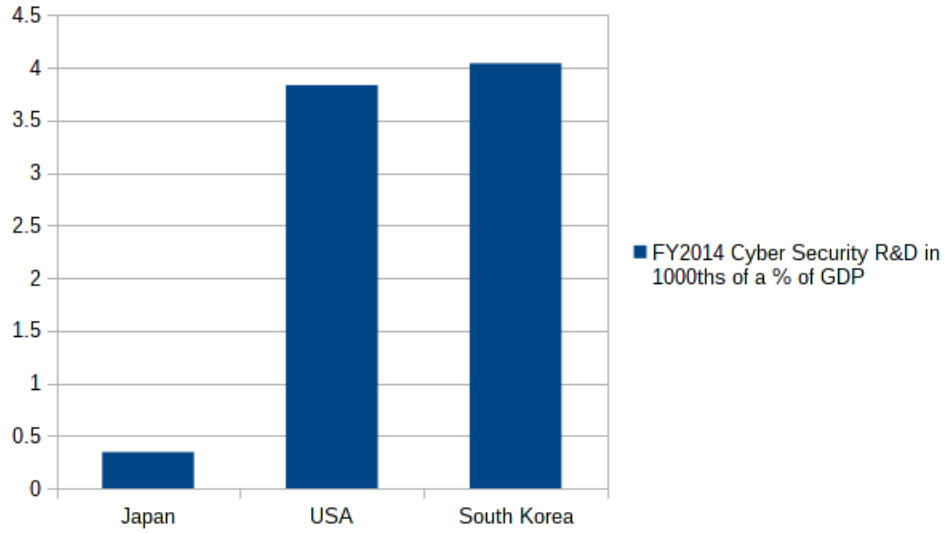

Figure 3.3: FY2014 cyber security R&D spending for Japan, the U.S., and South Korea.[24]

Fujitsu, Mitsubishi Electric, Renesas Electronics Corporation, and Panasonic.[22] 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.[23] Again, the key focus is on cyber security technology that can be used to secure the technology of other sectors, in this case critical infrastructure sectors.

Along with R&D funding, Japan also both runs its own training programs, and funds cyber security education in universities and other educational institutions, in order to strengthen the cyber security work force. While increasing the size and quality of the cyber security work force would of course be a boon for the Japanese cyber security sector, when one examines the goals and justifications of these policies, it is clear that, much as with the R&D

[22]New Energy and Industrial Technology Development Organization, 研究開発内容（全体版）*[Contents of Research and Development (Complete Version)]* [in Japanese], 2017, accessed February 17, 2018, `http://www.nedo.go.jp/content/100862901.pdf`.

[23]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)], 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]*, 10–12.

[24]이유지, *2017* 년국가사이버보안연구개발에 *1* 천억원투입 [in Korean], December 2016, accessed July 27, 2018, `https://www.bloter.net/archives/269792`; Ministry of Economy, Trade and Industry, 参考資料 *[Reference Materials]*, 2017, accessed July 23, 2018, `http://www.meti.go.jp/committee/kenkyukai/shoujo/sangyo_cyber/pdf/001_s01_00.pdf`. U.S. figure does not include NSA spending. GDPs gathered from `http://www.tradingeconomics.com`

programs, the aim is primarily to improve the cyber security human resources available to other sectors.

In terms of direct programs, the Information-technology Promotion Agency 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.[25] The NPA also runs a cyber security human resources development program, for which it requested 870 million yen in 2017.[26]

Not to be outdone, MIC has plans 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. In 2017, it requested 3.51 billion yen toward this end.[27]

In terms of university funding, the Ministry of Education, Culture, Sports, Science and Technology (MEXT) gives grants to universities and technical schools in order to promote cyber security education. In 2017, it requested 450 million yen for this purpose.[28] The government has also established a framework for the practical application of training that can be used in both the public and private sectors.[29]

Along with education, the government has sought to make it easier to match human resources with needs. For example, it has created qualification systems for cyber security, and standard ways of referring to and of visualizing cyber security skills and skill requirements.[30]

Turning to the justification for these programs, the First National Strategy on Information Security states that the government will make efforts in human resource development for government agencies, critical infrastructure, and businesses. It also highlights the need to develop specialists with multidisciplinary and comprehensive capacities, such as chief information security officers (CISO), personnel in charge of information systems, and legal personnel; in short, the types of specialists firms not directly involved in the development of cyber security technologies or services might need.[31] Likewise, the Second National Strategy on Information Security calls for the development of human resources for government agencies and for enterprises. In the case of the latter, it cites the need "to develop and

[25]Information-technology Promotion Agency, *IPA Information-technology Promotion Agency, Japan : IPA:Business Outline*.

[26]National center of Incident readiness and Strategy for Cybersecurity, 政府のサイバーセキュリティに関する予算 *[Government Budget Related to Cyber Security]*, 1.

[27]Ibid., 4.

[28]Ibid., 1.

[29]Information Security Policy Council, *Cybersecurity Strategy*, 46–47.

[30]Information Security Policy Council, *The First National Strategy on Information Security*, 28–29; Information Security Policy Council, *The Second National Strategy on Information Security*, 64–66; Information Security Policy Council, *Cybersecurity Strategy*, 47; Government of Japan, サイバーセキュリティ戦略 *[Cybersecurity Strategy]*, 50.

[31]Information Security Policy Council, *The First National Strategy on Information Security*, 28–29.

maintain personnel who are capable of the promotion of information security measures of enterprises"[32]. Again, there is a focus on personnel who can take a wider view of the needs of the firms, who can aid firms in the transition to new network technologies such as IPv6, and who can take security measures while identifying risks concerning legal compliance, information assets, and business continuity.[33] As can be seen, the focus is on the promotion of workers who can help firms improve and maintain their cyber security, rather than on workers who can develop new cyber security products or services.

This theme continues in the two Cybersecurity Strategies. The 2013 Strategy states that human resources development is necessary due to the expansion of the use of information communications technology.[34] The 2015 Strategy again emphasizes the need for cyber security professionals who are not just technology specialists. It calls for increasing the number of workers who could communicate between senior executives and cyber security professionals, and for the development of "hybrid" human resources, for example, people with competence in cyber security and the law, or cyber security and business management.[35]

Thus, as we can see, the main justification behind the government's promotion of cyber security human resources is to improve the cyber security of firms more broadly. Of course, while this reveals something about the priorities of the government, it remains the case that cyber security talent developed for the economy more broadly is also useful for the cyber security sector itself.

Thus, what we see is there are not actors that are both willing and able to strongly promote the cyber security sector. The Ministry of Defense recognizes the importance of the sector for national security, but is not in a position to promote the sector itself. Meanwhile, those economy-oriented institutions involved in cyber security policy do fund some cyber security R&D and training programs, but mainly with the goal of supporting other parts of the economy.

3.3 U.S. Sector Promotion

The strong national security institutions of the U.S. has ensured that there are bureaucratic actors, such as the DoD and the NSA, with a strong interest in promoting and the capability to promote cyber security. As important as the actual institutions, however, is the widely-held belief that the government has an important role to play in national security. This has meant that promotion of cyber security has support within the political system that promotion of technologies unrelated to national security might not. Indeed, the U.S. government promotes its cyber security sector despite the fact that the U.S. is already a leader in this area.

[32]Information Security Policy Council, *The Second National Strategy on Information Security*, 65.
[33]Ibid., 65–66.
[34]Information Security Policy Council, *Cybersecurity Strategy*, 46.
[35]Government of Japan, サイバーセキュリティ戦略 *[Cybersecurity Strategy]*, 16–17,48–49.

The U.S. has a long history of government support for the development of technology thought to be useful to the national defense. This trend began in World War II, when the government became the main source of funding for foundational scientific research. It was accelerated during the Cold War, when fears that the Soviet Union was overtaking the U.S. in technological capabilities led to the founding of the Defense Advanced Research Projects Agency (DARPA) in 1958. At this time, engineer-run spin-off firms were proving to be successful in the private sector. DARPA was able to take advantage of the competition between small start-up firms for which even a relatively small amount of government funding would make a large difference to mobilize private-sector efforts to produce technology that would be useful for the nation's security. It also used its funding networks to encourage the exchange of knowledge between competing research groups, by, for example, bringing researchers together for periodic workshops. It even worked to expand the pool of scientists, for example by funding computer science programs in U.S. universities. DARPA's successes in helping to build Silicon Valley, among other successes, helped to cement support for it among policy-makers.[36]

Of course, the fact that there exist instruments for spending on defense-related technologies does not in and of itself explain why they are spent on cyber security technology; for this, one would have to turn to the bureaucratic agencies themselves. In this case, however, the answer seems relatively self-evident: cyber attacks prevent an increasingly credible threat to the U.S., both in terms of its armed forces, which rely increasingly on information technology, and in terms of its critical infrastructure. At the same time, as the potential adversaries of the U.S. come to rely more on information technology as well, this provides opportunities for the United States' security services, particularly in terms of intelligence-gathering, but also, as STUXNET showed, in terms of operations. It is thus clearly within the interests of the security agencies to invest in cyber security technology.

Though it is impossible to prove the counter-factual, the fate of the Advanced Technology Program (ATP), which was aimed at promoting civilian rather than defense technology, provides a useful clue as to what might have been the fate of cyber security technology promotion were its usefulness for defense purposes less clear. The ATP was created in 1988 by the Omnibus Trade and Competitiveness Act, though it was not funded until 1990, when George H. W. Bush was in the White House, and Democrats controlled both chambers of Congress. It was conceived of as the civilian counterpart to DARPA, with the purpose of funding high-risk, early technology projects that could lead to developments that increase U.S. economic competitiveness. For-profits would lead any projects funded by the ATP, though other companies, universities, non-profits, and federal laboratories could participate as partners.[37]

Almost immediately, ATP came under attacks from the right, who complained that it promoted industrial policy and corporate welfare. The Bush administration was relatively

[36]Block, "Innovation and the Invisible Hand of Government," 8–10.

[37]Marian Negoita, "To Hide or Not to Hide? The Advanced Technology Program and the Future of U.S. Civilian Technology Policy," in *State of Innovation: The U.S. Government's Role in Technology Development*, ed. Fred Block and Matthew R. Keller (Boulder, CO: Paradigm Publishers, 2011), 80–81.

unenthusiastic about the program: by 1992, it was receiving funding of about $50 million, remaining a relatively insignificant program. Things changed dramatically when Clinton became President in 1993. The Democrats now controlled the Presidency, the House, and the Senate. By 1995, its appropriations had reached $340 million, and was expected to reach $1 billion by the end of the decade.[38] Unfortunately for the ATP, in 1995, the Republicans took over both chambers of Congress. The ATP's budget was slashed to $221 million in 1996, and then reduced further to just under $200 million, where it remained for the rest of the decade. It would eventually be eliminated entirely under the second Bush administration.[39]

The fate of In-Q-Tel, a venture fund run by the CIA, provides an important contrast. In response to a proposal by the CIA, In-Q-Tel was established by Congress in February 1999—the same Republican Congress that had shown such skepticism toward the ATP. While the ATP's budget was being slashed under the second Bush administration, In-Q-Tel's budget was being increased: from $28 million in 1999 to $68 million as of 2011. Moreover, in response to 9/11 and the resulting critique of the intelligence agencies' capabilities, a number of other agencies created their own venture capital firms. Of these, only one, Red Planet Ventures, was created by an agency, NASA, not involved in national security—and its funding allocation was eliminated within a year of its founding.[40]

This willingness to spend on national security means that national security organizations are well-positioned to support the cyber security market. The Pentagon alone had a budget of over $7 billion for cyber security in 2017; by contrast, the entire Japanese government spent less than $600 million.[41] Though some of this money is for staff and maintenance, that still leaves considerable funds to be spent on procurement. Moreover, it is not just the military that buys cyber security technology; the NSA and CIA do as well. The Department of Defense also provides seed funding to cyber security firms through DARPA.[42]

As mentioned above, the U.S. government has also started funding technology firms, including cyber security firms, via public venture capital. In-Q-Tel, for example, acts in some ways like a normal venture firms: it provides strategic consultation and organizational guidance, as well as equity. However, its purpose is to fund technologies that not only have the potential to be commercially successful, but that meet some need of the CIA. As of 2011, In-Q-Tel's annual budget was more than $60 million.[43] The venture companies associated

[38]Negoita, "To Hide or Not to Hide? The Advanced Technology Program and the Future of U.S. Civilian Technology Policy," 81–83.

[39]Ibid., 84–85.

[40]Matthew R. Keller, "The CIA's Pioneering Role in Public Venture Capital Initiatives," in *State of Innovation: The U.S. Government's Role in Technology Development*, ed. Fred Block and Matthew R. Keller (Boulder, CO: Paradigm Publishers, 2011), 118–126.

[41]Office of Management and Budget, "21. Cyber Security Funding"; National center of Incident readiness and Strategy for Cybersecurity, 政府のサイバーセキュリティに関する予算 *[Government Budget Related to Cyber Security]*. The entire U.S. budget was around $14 billion.

[42]Block, "Innovation and the Invisible Hand of Government"; Vinod K. Aggarwal and Andrew Reddie, "Iterative Industrial Policy: How the United States Pursues Cybersecurity" (2018).

[43]Keller, "The CIA's Pioneering Role in Public Venture Capital Initiatives," 118–119.

with the other national security organizations operate similarly.[44]

Overall, then, we see that the strong national security institutions of the U.S. lead to the strong promotion of indigenous cyber security technology. These institutions ensure both that there are actors with an interest in promoting the cyber security sector, and that they have the political support to do so. Particularly in the U.S. case, the national security organizations, especially the Department of Defense, already had programs in place for promoting technology that they could use to promote cyber security as well; though, as we can see, the U.S. government has not been lax in developing new instruments meant to better support the kinds of small and medium companies found in the software and cyber security sectors.

3.4 South Korea's Sector Promotion

Like the U.S., South Korea's strong national security institutions lead to support for an indigenous cyber security sector. As discussed in Chapter 2, both the Ministry of National Defense (MND) and the National Intelligence Service (NIS) have strong incentives to promote an indigenous cyber security sector. MND in particular has been active in cyber security procurement, going so far as to establish a fast-track acquisition program for cyber security technology in 2016.[45]

Evidence for this national security orientation toward cyber security can be seen in South Korea's procurement policies. In order to be sold to public organizations, cyber security products must pass the Korea Cryptographic Module Validation Program (KCMVP) and obtain certification. Certification requires companies to disclose their source code to the National Security Research Institute, and can be time-consuming to obtain.[46] Though not impossible for foreign firms to participate, this has created a clear advantage for domestic firms in the procurement process.

Where South Korea differs from the U.S. is that its policy legacy of economic guidance gives it a wider range of institutions that can participate in sector promotion. In fact, not only does South Korea have a policy legacy of economic guidance, it has a legacy of promoting ICT technology specifically. Between 2005–2014, it had seven major policies aimed at promoting software, using tools including R&D support, the development of human resources, the development of standards and certification, and public procurement.[47] It has also developed

[44]Keller, "The CIA's Pioneering Role in Public Venture Capital Initiatives," 125. For a further discussion of how the U.S. government promotes the cyber security sector, see Aggarwal and Reddie, "Iterative Industrial Policy: How the United States Pursues Cybersecurity."

[45]Ministry of National Defense, Republic of Korea, *2016 Defense White Paper*, 2016, 78, accessed April 20, 2018, `http://www.mnd.go.kr/user/mndEN/upload/pblictn/PBLICTNEBOOK_201705180357180050.pdf`.

[46]In-soon Kim, "Foreign security companies set out to target public market, eyeing the home ground of native companies," *The Electronic Times*, April 2014, accessed June 21, 2018, `http://global.factiva.com/redir/default.aspx?P=sa&an=ETK0000020140424ea4o00001&cat=a&ep=ASE`.

[47]Hongbum Kim, Dong-Hee Shin, and Daeho Lee, "A socio-technical analysis of software policy in Korea: Towards a central role for building ICT ecosystems," *Telecommunications Policy* 39, no. 11 (December 2015):

laws aimed at promoting the internet industry and services, including the Information and Communications Technology Industry Promotion Act (2009), the Special Act on Promotion of Information and Communications Technology, Vitalization of Convergence Thereof, etc (2013), and the Act on the Development of Cloud Computing and Protection of Its Users (2015).[48] Between 2013–2018, the South Korean government planned to spend $8.1 billion on ICT R&D.[49]

Originally these efforts were led by the Ministry of Information and Communication. Later, in 2008, the MIC was split into multiple ministries, with the Ministry of Knowledge and Economy (MKE) taking over the responsibilities for software promotion. In 2013, the MKE was replaced with the Ministry of Science, ICT, and Future Planning (MSIP), later renamed the Ministry of Science and ICT. Tools for software promotion included R&D support, the development of human resources, loans and tax incentives, standards and certifications, and public procurement.[50] In 2013, the government announced that over the next five years, it planned to spend $8.1 billion on ICT R&D.[51]

Building on these institutions, in 2015, South Korea passed The Act on the Promotion of the Information Security Industry. The Act calls for the Minister of Science and ICT to create a plan every five years to promote the cyber security industry. It also authorizes the Ministry of Science and ICT to use a number of instruments to strengthen cyber security technology. In terms of research and development, the Act allows the Ministry to implement projects meant to discover core technologies, to commercialize information security technology, to promote joint industry-academia research, to promote international joint research, and to promote trade in information security technology.[52]

In summation, while South Korea's strong national security institutions provide the impetus for promotion of the cyber security sector, it does not rely on those institutions alone for cyber security promotion. Instead, it uses institutions developed for economic guidance to promote the cyber security sector as well.

3.5 Revisiting the Argument

The argument as introduced in the introduction and the beginning of this chapter is that there is a clear national security case to be made for promoting an indigenous cyber security sector, and that states with strong national security institutions will have governmental

944–956.

[48]Korea Internet and Security Agency, *Laws on the Internet and Information Security of Korea*, 2016, 8–10.

[49]Jong-chan Kim, "S. Korea to spend $8.1 billion on ICT R&D for 5 years," *AJU NEWS*, October 2013, accessed June 21, 2018, `http://global.factiva.com/redir/default.aspx?P=sa&an=AJUENG0020131023e9an0005l&cat=a&ep=ASE`.

[50]Kim, Shin, and Lee, "A socio-technical analysis of software policy in Korea," 947–948.

[51]Kim, "S. Korea to spend $8.1 billion on ICT R&D for 5 years."

[52]Government of the Republic of Korea, *Act on the Promotion of Information Security Industry*, last amended July 2017, June 2015.

actors that recognize and act upon this. By contrast, Japan, which has strong institutions for economic guidance, but weak national security institutions, would not prioritize national security and thus would ignore the case for cyber security promotion in favor of other priorities.

There is a flaw in this simple version of the argument, however: there is an economic case to be made for cyber security promotion, as well—a case to which MIC and, in particular, METI might well respond. One economic reason a state might want to promote a particular sector is that the sector may earn high returns relative to other sectors with similar risk. Under most circumstances, such high returns would be competed away as firms in various states entered into the sector. However, in the case of some sectors, certain factors such as economies of scale, advantages of experience, and innovation potential can create barriers to entry which allow returns to remain high.[53]

It is precisely overcoming these barriers that requires government intervention. If the state is not a early-mover in entering the sector, infant domestic industries will be unable to handle the costs of investment and competition with industries in earlier-moving states. Governments can create policies to support these infant industries until they are able to compete with those of the early-mover states.[54]

Cyber security products are for the most part software. Software has a large fixed up-front cost, with very small and either static or decreasing costs for duplication and distribution. There are thus economies of scale, which provide a barrier to entry.[55]

However, relative to some other types of software and IT technology, barriers to entry into cyber security do not appear to be as high. Some types of software and IT services have strong network effects, meaning that the more people that use them, the more valuable the software or service becomes.[56] Perhaps the strongest example of this is operating systems: the more widely used an operating system is, the more profitable it is for companies to develop software for that operating system, and thus the more useful that particular operating system becomes to the end user.[57] For the most part cyber security technology does not have such an effect, since it does not serve as a platform for other technologies, nor does its usefulness rely on the number of other users (such as with social media platforms), though there may be some small network effects in terms of third party support.

More common for software than network effects are switching costs, since learning to use particular software (such as a word processor) takes time and effort on the part of users (or,

[53]Pekkanen, *Picking Winners?*, 11.

[54]Crafts, "Overview and Policy Implications," 3–4.

[55]Schmidt and Schnitzer, "Public Subsidies for Open Source - Some Economic Policy Issues of the Software Market," 477–478. Though as Ge and Huang point out, economies of scale are less for software-as-a-service companies (an increasingly popular business model), as these require the firm to manage IT infrastructure, which does not have zero variable costs. C. Ge and K. W. Huang, "Analyzing the Economies of Scale of Software as a Service Software Firms: A Stochastic Frontier Approach," *IEEE Transactions on Engineering Management* 61, no. 4 (November 2014): 620.

[56]Schmidt and Schnitzer, "Public Subsidies for Open Source - Some Economic Policy Issues of the Software Market," 486–490.

[57]Gaming systems and other specialized hardware platforms have similar properties.

in the case of enterprise technologies, on the part of the IT department).[58] However, for the most part, cyber security products are meant to run out of the box "as-is", and require very little intervention on the part of the user. With the exception of firms that require or provide specialized cyber security configurations, for most users the costs of switching are quite low.

Product differentiation, another possible barrier to entry, is also not a major issue in the cyber security sector. The products and services that cyber security firms offer are relatively indistinguishable from one another.[59]

Despite the apparent relative lack of barriers, however, the sector is dominated by a relatively small number of companies.[60] Given that cyber security is a rapidly-growing market (projected to grow with a compound interest rate of 10.16% between 2016 and 2021[61], this would suggest that either the aforementioned economies of scale are quite significant, or that some other barriers (such as advertising or brand recognition[62]) are at work.[63]

In short, though there are enough barriers to entry to create strong profits, the barriers to entry into the cyber security sector are lower than than those for some other types of information technology. Arguably, however, this supports rather than diminishes the case for government intervention in this sector: the network effects and switching costs involved with some types of software, such as operating systems, are so high that a government could not overcome them without taking drastic measures; by contrast, cyber security firms would require far more modest support (though the government would have to be wary that such support did not lead to excess competition).

A second reason a state might wish to promote a particular sector is positive spill-over effects. Some sectors yield high returns to the economy as a whole because not only do they provide their own earnings, but also provide benefits to capital and labor in other sectors.[64] However, precisely because these benefits spill-over into other sectors and cannot be captured as returns on investment, such sectors may suffer from under-investment.[65] Thus, government support may be required to reach a level of investment that is optimal for the economy as a

[58]Schmidt and Schnitzer, "Public Subsidies for Open Source - Some Economic Policy Issues of the Software Market," 490–492; Fahri Karakaya and Michael J. Stahl, "Barriers to Entry and Market Entry Decisions in Consumer and Industrial Goods Markets," *Journal of Marketing* 53, no. 2 (1989): 80–82.

[59]Emanuel Kopp, Lincoln Kaffenberger, and Christopher Wilson, *Cyber Risk, Market Failures, and Financial Stability*, IMF Working Paper WP/17/185 (International Monetary Fund, 2017), 20, accessed May 26, 2018, `http://elibrary.imf.org/view/IMF001/24475-9781484313787/24475-9781484313787/24475-9781484313787.xml`.

[60]Ibid.

[61]Vinod K. Aggarwal and Andrew Reddie, "Comparative Industrial Policy and Cybersecurity: A Framework for Analysis" (2018), 6.

[62]Karakaya and Stahl, "Barriers to Entry and Market Entry Decisions in Consumer and Industrial Goods Markets," 81–82.

[63]Another piece of evidence that the barriers to entry may be higher than it would appear is that there are not signs of excessive competition in this sector, at least in Japan.

[64]Pekkanen, *Picking Winners?*, 12; Sonia Aggarwal and Vinod K. Aggarwal, *The Political Economy of Industrial Policy*, September 2016.

[65]Harris and Carman, "Public Regulation of Marketing Activity," 56; Aggarwal and Aggarwal, *The Political Economy of Industrial Policy*.

Policy Legacies		Policy Outcomes
Security Capabilities Maintenance	Economic Guidance	
Weak	Weak	No
Weak	Strong	?
Strong	Weak	Yes
Strong	Strong	Yes

Figure 3.4: Complicating the sector promotion argument.

whole.

The primary spill-over effect of cyber security involves human capital.[66] Human capital developed for the cyber security sector can be carried over to the wider information technology sector. The programming capabilities one needs in order to work in this sector are just as applicable in other information-technology-related jobs, such as software development and quality control. Problems in cyber security may have analogues in other areas of software programming, and so solutions to those problems may be carried over by workers moving from cyber-security firms to more general software firms. Moreover, workers trained in the cyber security sector bring an additional set of knowledge, both explicit and tacit, to these other fields: a software engineer trained in cyber security will know common vulnerabilities to avoid in their own code; a quality control engineer will know for what vulnerabilities to test. This will lead to less vulnerable software in the first place. Workers trained at cyber security companies can also be useful resources in companies that rely on information and communications technology. Banks, major retailers, and increasingly manufacturing companies, among other types of companies, have need of cyber security experts to both better understand their cyber security risks and to produce and implement cyber security plans.

Figure 3.4 illustrates the problem with the simple explanation for the Japan case. It is obvious that if a state does not have a strong national security apparatus or institutions for directly coordinating firm behavior, then there will be no (or little) promotion of the cyber security sector, since the state will have neither the means nor the motivation. Having a strong national security apparatus, by contrast, provides *both* the means and the motivation. But in Japan's case, it has a weak national security apparatus, but strong institutions for coordinating private sector behavior: the means, but not *necessarily* the motivation. In other words, the outcome is indeterminate.

Without a strong security apparatus, a number of factors may influence a state's decision as to whether or not to develop cyber security. In the case of Japan, two factors are especially important. First, its earlier failed attempt at promoting software has convinced important bureaucratic actors within the government that attempts to promote cyber security firms are

[66]There are a number of positive externalities involved in investment in cyber security by firms, which will be discussed in the next chapter. Here I am dealing only with those spill-over effects that arise from the creation and growth of cyber-security firms.

Policy Legacies			Policy Outcomes
Security Capabilities Maintenance	Economic Guidance	Outcome of Promoting Similar Technology	
Weak	Weak	N/A	No
Weak	Strong	Clear Failure	No
Weak	Strong	Unclear or N/A	?
Weak	Strong	Clear Success	Yes
Strong	Weak	N/A	Yes
Strong	Strong	No	Yes
Strong	Strong	Yes	Yes

Figure 3.5: The importance of experience.

unlikely to succeed. Second, it is particularly risk-averse in this case because the government recognizes that to encourage other Japanese firms to rely on presumably-inferior Japanese cyber security products would be damaging to other sectors of the economy.

To this latter point, it is *not* the case that Japan has abandoned its efforts in promoting cutting-edge information technology more broadly. For example, while its research-and-development budget for cyber security in FY2014 was only $16.7 million[67], and its *total* cyber-security-related spending in 2017 was projected to be around $540 million dollars, its R&D budget for AI in 2017 was around $532 million dollars, and its projected R&D budget for AI in 2018 is around $692 million dollars.[68] The difference is that, at least for the time being, promoting indigenous AI does not pose obvious costs to other sectors, in part because it is often developed and used internally by firms, not yet sold as a capital good, and in part because the state of the technology is still immature worldwide.

We can see the updated argument in Figure 3.5. While we still cannot say for certain whether a state like Japan would promote the cyber security sector in the absence of a failure to promote a similar technology, the argument here is that in considering whether to promote a particular sector or technology, governments refer to past experiences promoting similar technologies. If there has been a clear failure in promoting a similar technology in the past, then the government will be unwilling to take the risk of promoting the cyber security sector,

[67]Ministry of Economy, Trade and Industry, 参考資料 *[Reference Materials]*. For whatever reason, this seems to be the last date the Japanese government produced a number for its total cyber-security-related R&D spending; the document referencing the number is from 2017, and searches through similar documents have found no newer results.

[68]National center of Incident readiness and Strategy for Cybersecurity, 政府のサイバーセキュリティに関する予算 *[Government Budget Related to Cyber Security]*; Editorial Staff, *The artificial intelligence race heats up*, March 2018, accessed July 24, 2018, `https://www.japantimes.co.jp/opinion/2018/03/01/editorials/artificial-intelligence-race-heats/`.

while if the past effort has been a clear success, there is every reason for the government to believe it will succeed and so make the attempt again. If attempts to promote similar technologies have not been made, or if the outcome of earlier attempts to promote similar technologies is unclear, then the outcome remains indeterminate. That having been said, I would argue that assuming conditions have not dramatically changed, an earlier attempt to promote a similar technology that leads to an uncertain result should make it more likely that a state will pursue cyber security technology, for whatever the same reasons it chose to pursue the similar technology.

The reason Japan has not sought to specifically target its cyber security sector is due to extreme skepticism on the part of MIC and especially METI that it can do so effectively. Japan's previous efforts to promote its software sector failed spectacularly, with negative consequences not only for the industry itself but for other sectors which had come to rely on the software. What METI and MIC took from that experience was not only that using sector-specific instruments would fail, but that it was more important to make certain that other sectors were keeping up to date with the latest technology; this has a heavy influence on its policy toward promoting cyber security in firms more broadly, as I will explain in the next chapter. Moreover, there is evidence that METI's current thinking is to enhance Japan's competitiveness by competing in new technologies where it already has some advantage, such as Internet of Things devices and self-driving automobiles, rather than to try to promote technologies where other countries are already dominant.[69] The lack of effort to promote cyber security technologies (and, moreover, the pattern of R&D in terms of what cyber security technologies the government *does* invest in) would seem to fit this thinking.

To be clear, regardless of other factors, we would not expect to see the same kind of infant industry protection policies that Japan pursued during the period of high growth. While METI, in its previous incarnation as MITI, had been a major supporter of such policies, its preferences shifted during the 1990s. By 2001, when it was reorganized into METI, it had switched to promoting economy-wide reforms over protecting infant industries. In part, this was simple survival: pressures from the U.S. in particular had already forced Japan to liberalize trade and investment, and the major Japanese firms had grown strong enough that they needed little from MITI/METI. As a result, the ministry needed to find new reasons to justify its existence and autonomy. While shifting to economy-wide reforms forced METI to cooperate with other ministries, since it required policy changes outside of METI's jurisdiction, it had the advantage of giving METI a clear purpose, and in some ways a more expanded role. Thus, instead of pushing industry-specific protectionist policies, it for the most part switched to policies that were meant to benefit a variety of industries, such as promoting the use of information technology, though in some areas where it felt as though sectors still needed to be protected, such as energy and chemicals, it continued to use more traditional tools.[70]

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

[70] Mark Elder, "Chapter 7. METI and Industrial Policy in Japan: Change and Continuity," *Japanese Economy* 28, no. 6 (November 2000): 4–6, https://www.tandfonline.com/doi/abs/10.2753/JES1097-203X28063.

However, the core policy goals that motivated METI had not changed. It still emphasized the need for an overall national economic strategy and to promote national competitiveness. It continued to promote new industries and firms, albeit via instruments mainly meant to fix specific market failures: providing information, reducing transaction costs, and helping with public goods and coordination problems. It also continued to advocate for the promotion of particular technologies, although generally in a more broadly defined way in the past (for example, "information technology" instead of "computers").[71] As we have seen, however, even given this new broader strategy, METI does very little to promote the cyber security sector.

The reason for METI's extreme skepticism is its previous experiences trying to promote the software sector. Starting in the 1970s, MITI sought to develop Japan's software sector using traditional infant-industry-protecting tools. The result was a disaster. While Japan promoted its own software standards, American standards won the day internationally, making it difficult for Japanese companies to sell their software overseas. MITI was often one step behind the curve—for example, promoting software for mainframes just as PCs took over the market. This follow-the-leader approach had worked fine in manufacturing, but was a disaster in software: once PCs were dominant, there was very little need for mainframe software. Moreover, the Japanese market continued to prefer customized software as the international market moved toward packaged software, leading to a mismatch.[72]

Worse, because software is a capital good, this had negative spillover effects into the rest of Japan's economy. Japanese firms were stuck with inefficient Japanese software, while foreign firms (particularly American firms) used the latest-and-greatest. This was not entirely MITI's fault; while it may have been responsible for promoting the software in the first place, the problem was exacerbated by the tendency of Japanese firms to favor long-term relations with suppliers. Japanese firms did not want to break with the companies providing them with custom software, and so continued those relationships even in cases where packaged software would have been better. Ultimately, MITI realized its mistake and reversed course, both pushing for Japanese producers of software to follow international standards and for Japanese companies to switch to packaged software, but in the meantime damage had been done.[73]

There are good reasons for METI and MIC not to wish to repeat this experience with cyber security technology. Beyond the obvious problem—that their efforts might fail—there is the risk that, as with software, Japanese companies would be left with inferior products, risking their own cyber security. It is no accident that support of and conformance to international standards has been a major part of METI and MIC's cyber security policy

[71] Elder, "Chapter 7. METI and Industrial Policy in Japan," 7–10.

[72] Marie Anchordoguy, *Reprogramming Japan: The High Tech Crisis Under Communitarian Capitalism* (Cornell University Press, 2005), 147–176; Sangbae Kim, ""Hardware" Institutions for "Software" Technologies: The Japanese Model of Industrial Development in the Personal Computer Industry," *Journal of International and Area Studies* 9, no. 1 (2002): 28–29.

[73] Anchordoguy, *Reprogramming Japan*, 145–176.

from the beginning.[74] In interviews with officials from both ministries, failed attempts to promote software and internet companies were the main reasons given for not doing more to promote cyber security.[75]

Given this skepticism and the other priorities of MIC and METI, it is little wonder that R&D efforts are aimed primarily at improving the cyber security of products and services in other sectors, rather than on promoting the cyber security sector. MIC's main policy concern is in keeping Japan's networks safe and well-functioning, and so it has good reason to prioritize funding in R&D for technology that will protect of networks. METI, too, has industries over which it has jurisdiction which benefit from these programs, such as automobile companies. But one gets the sense in discussing the issue with officials from METI that it is not just aiding those firms over which it has jurisdiction, but that it also sees promoting *cyber security as a feature* as part of a broader economic strategy to improve Japan's competitiveness in other high-technology areas. METI and NISC officials both were emphatic in pointing out that Japanese cyber security policy puts a strong emphasis on the economic role of cyber security. They feel that a reputation for products and services with strong cyber security could provide a competitive edge for Japan. In particular, while going to-to-toe with the U.S. on cyber security products and services may be impossible, they feel that Japan is still strong when it comes to manufacturing, and that the era of connected consumer devices provides Japan with new opportunities in this area. Making certain those devices are cyber-secure is thus a key part of METI's strategy.[76]

In summation, Japan's approach to the cyber security sector is heavily influenced by earlier failed attempts to build up its knowledge economy, and the innovation policies that came about as a result. The reason we do not see sector-specific promotion of cyber security is not because the actors involved do not recognize the importance of the sector, but because METI and MIC have become convinced that sector-specific promotion will not work. Beyond this, however, the very lack of an indigenous cyber security sector has made it more appealing for METI and MIC to spend their limited funds improving the cyber security of those technologies in which Japan is already competitive, rather than to try to reproduce more generic cyber security products.

[74] Author interviews with MIC official and former IPA official, Japan, Summer 2017.
[75] Author interviews with NISC officials, METI official and MIC official, Tokyo, Summer 2017.
[76] Author's interviews with NISC official and METI official, Tokyo, Summer 2017.

Chapter 4

Cyber Security Promotion

Cyber security is not simply a problem for governments, but for private sector organizations and for individuals as well. As with sector promotion, there are both national security and economic reasons that a government might want to promote cyber security in the private sector. On the national security side, compromised devices in the private sector can be used to launch attacks on government computers, malware can spread from the private sector into government networks, key technology specifications can be stolen from defense firms, and cyber attacks on critical infrastructure can threaten military operations. What is more, as the North Korean hacking of Sony demonstrates, private firms can now face threats from state actors, raising questions about where the boundaries of national security lie.[1] On the economic side, technology stolen from domestic firms can harm international competitiveness; cyber attacks can disrupt services and cause financial losses for firms; leaks of personal information can expose individuals to economic harm via identity theft, and make make them more hesitant to use internet-based services; and, in particular, attacks on critical infrastructure can cause enormous harm not only to the critical infrastructure firms themselves, but to those firms which rely on them.

Despite this, support from governments for the improvement of cyber security within the private sector is not automatic. While Japan and South Korea have both been active in promoting cyber security in the private sector, the U.S. has not. The difference, I argue, is that Japan and South Korea both have strong institutions for economic guidance, deriving from their histories as "developmental states". Both governments are used to working with firms and pushing for particular firm behavior meant to achieve specific economic goals. This has three results. One, there are actors within the government who recognize the economic costs of weak private-sector cyber security, and see it as part of their role to reduce those costs. Two, there are existing institutional arrangements for economic guidance that can be turned to promoting cyber security. Three, the government taking an active role in directing the private sector is already conceived of as legitimate, both by governmental and private

[1] Carr makes a similar point about critical infrastructure firms. Madeline Carr, "Public–private partnerships in national cyber-security strategies," *International Affairs* 92, no. 1 (January 2016): 43–62.

actors, and so there is not political resistance to government taking such a role with regard to the promotion of cyber security.[2]

By contrast, governments without a policy legacy of economic guidance face three hurdles. One, even if they wanted to promote cyber security in the private sector, there are not instruments readily available for doing so. Two, any attempt to promote cyber security in the private sector is more likely to create political controversy, since there is not an existing pattern of the government taking an active role in coordinating with the private sector. In particular, firms are more likely to be resistant to government action, since they will be used to being left to their own affairs. Three, there are unlikely to be strong advocates for government action within the government itself.

Strong national security institutions do not have a similar effect; even if actors within national security organizations recognize that the threat to the private sector may harm national security, they simply do not conceive of coordinating with private sector actors as part of their own role, nor do they have the instruments to do so. As I will discuss, however, there is an exception to the argument laid out above: critical infrastructure. Both because the military relies on critical infrastructure, and because of the obvious damage the loss of critical infrastructure can cause, it is a clear national security issue. Moreover, critical infrastructure firms recognize that they are at an unusually high risk of being attacked by state actors relative to other firms, and thus may be more eager than other types of firms for government action on their behalf.[3] Thus, even in the case where there are not strong institutions for economic guidance, we should expect to see governments make some effort to promote cyber security within critical infrastructure sectors. However, governments which already have strong institutions for economic guidance should be able to do this more easily, since they have readily-available instruments that can be turned to this purpose.

The rest of this chapter proceeds as follows: first, I explain why the private sector on its own does not sufficiently adopt cyber security technologies. Then, I discuss the Japanese, American, and Korean efforts to promote the adoption of cyber security technology in the private sector, and demonstrate that is the strength of their institutions for economic guidance that explains these outcomes. I then turn to critical infrastructure: looking at the U.S. and Japanese cases, I show that while due to the clearness of the threat even states without strong institutions for public-private economic coordination make an effort to promote the cyber security of critical infrastructure firms, those states which do have strong institutions for economic guidance are at an advantage in doing so.

[2]Though, of course, there may be differences of opinion about what role, precisely, the government should play.

[3]Though they and the government may have different ideas about what kind of action is appropriate. See Carr, "Public–private partnerships in national cyber-security strategies."

4.1 The Problem

The private sector has difficulty providing enough cyber security for itself. In theory, individuals and firms should calculate the risk of cyber attack, including the probability an attack will succeed and the costs of an attack should it occur, and purchase an amount of cyber security appropriate to that risk. However, a set of market failures lead to an undersupply of cyber security.

One failure that is particularly stark in cyber security is *information problems*. *Asymmetric information* is when the seller has more information about the product than the buyer.[4] Sellers know more about the level of security of their firms, services, and products than do customers. Because it is difficult for buyers to distinguish between sellers in terms of security, sellers have little incentive to improve security. For software and IT devices, this problem is compounded by the fact that there are trade-offs between ensuring security and speed of development; there is thus an incentive to shirk on security in order to be first on the market. Moreover, because buyers can distinguish products by features, it makes more sense for the seller to focus its resources on developing features that will appeal to customers, rather than on ensuring security. This problem is exacerbated by *moral hazard*: the cost of data breach, fraud, and other failures of cyber security are often born by the end user, rather than by the firm.[5]

Positive externalities are another major problem for cyber security. Positive externalities occur when the positive effects of production or consumption go not to the producer or the consumer, but to an unrelated third party or parties.[6] Improving one's own cyber security helps not just oneself, but others. A secure operating system helps protect software that runs upon it; a secure device is one less possible route for a virus, or one less bot that can be used for DDOS attack; and so forth. Particularly problematic is that a consumer's security may be less valuable to that consumer than it is to others who would be affected by that consumer's lack of security. For example, I may have a computer that contains no valuable data upon it, so there is little cost to me if it picks up malware, but my computer may then be used to launch an attack that is costly to others. Positive externalities are particularly a problem for critical infrastructure, where much of the benefit of cyber security accrues not to the operator, but to those who rely upon the infrastructure.[7] Along a similar logic is *internalities*, which are side effects born by other users of a product.[8] For example, perhaps I keep a weak password on my cloud account because I do not store anything of particular value to me, but a hacker then uses my account to break into the cloud and take the important files of others.

Network effects in IT, where a piece of software or platform is more useful the more

[4]Harris and Carman, "Public Regulation of Marketing Activity," 55.

[5]Aggarwal and Reddie, "Comparative Industrial Policy and Cybersecurity: A Framework for Analysis," 8.

[6]Harris and Carman, "Public Regulation of Marketing Activity," 56.

[7]Carr, "Public–private partnerships in national cyber-security strategies."

[8]Harris and Carman, "Public Regulation of Marketing Activity," 55.

others use it, lead to "winner take all" situations, where most users are using the same product (e.g., Windows, Facebook, etc.).[9] The result is natural monopolies, with two effects for cyber security: a lack of incentive to improve security due to a lack of competition, and lower barriers to attack, since most users are using the same software with the same vulnerabilities. Interoperability, which allows computers, devices, and different types of software to communicate with each other, also creates opportunities for malevolent programs to spread. Finally, Facebook, Google, and other platforms profit from partner companies building on their platforms; should they increase the security requirements to access these platforms, they could lose business.[10]

Another market failure is the *high cost of information*.[11] It is difficult for firms or individuals to know if their cyber security measures are truly sufficient. One possibility is to hire a team of hackers to test one's security, though this is not an option for individuals, and may even be out of the range of smaller firms. Exacerbating this problem, software updates or the purchase of new equipment may create new vulnerabilities, which require further testing.

Moreover, it is possible that some information that would be helpful for companies, such as best practices or guidelines, are not available at an cost, because the market fails to provide it. When information itself is the product, it may be impossible to reveal enough information about it to the seller to convince the seller to purchase it without effectively giving away the product itself. Worse, because information is quite cheap to reproduce, it would be difficult for the provider to internalize the value of the product.[12] Due to these various market failures, the private sector is unlikely to adequately invest in cyber security on its own.

4.2 Japanese Cyber Security Promotion

Despite the difficulties the private sector may have in providing for its own cyber security, this does not mean that governments will necessarily step in to help. The Japanese government takes action because its policy legacy of economic guidance has created government actors who see this as a problem for the government to solve, and has provided a set of instruments that can be applied to the problem. The measures it uses range from tax incentives for small- and medium-sized enterprises, to public information campaigns, to government-run technical solutions. Below I describe the main instruments the government has been using. One thing to note is that while the Japanese government is very active in the policy area, it displays a clear preference for non-coercive instruments.

[9] Allan Friedman, *Economic and Policy Frameworks for Cybersecurity Risks*, July 2011, accessed June 22, 2018, `https://www.brookings.edu/wp-content/uploads/2016/06/0721_cybersecurity_friedman.pdf`.

[10] Aggarwal and Reddie, "Comparative Industrial Policy and Cybersecurity: A Framework for Analysis," 8.

[11] Harris and Carman, "Public Regulation of Marketing Activity," 54.

[12] Ibid., 55.

Figure 4.1: Photo of a cyber-security-awareness poster in Harajuku, Tokyo. Text: "Such a simple password... does not suit you."

We can summarize Japan's cyber security promotion efforts as consisting of two parts: a set of programs, including educational programs and direct provision of cyber security, aimed at the general public; and a set of voluntary guidelines, incentives, and institutions meant to lower the cost and difficulty for firms to improve their cyber security, with a special focus on critical infrastructure firms.

The measures meant to help citizens are primarily bureaucrat-driven, and are motivated both by public safety concerns and by economic concerns. Though several agencies now play a role in this, initial efforts to better educate the public were spearheaded by MIC. 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.[13] The government established a number of programs to educate the public, including advertisements on billboards and on the web and school programs meant to teach children basic cyber security skills.

One of the government's major efforts to promote cyber security awareness among the

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

public is its "Information Security Month"[14], 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.[15]

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"[16], on which it publishes teaching materials. MIC also publishes information about cyber security through its site, "Information Security Site for Citizens"[17]. Likewise, IPA publishes easy-to-understand materials on cyber security and offers teaching materials on its (more-creatively-named) site, "From Here, Security!"[18] As part of these initiatives, the government has been encouraging cooperation between the various agencies hosting these sites to cross-link between each others' sites.[19]

The government has also been working with creators of pop media, such as music and comics, to promote cyber security.[20] 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.[21]

Education about cyber crime is another major focus of government efforts. These 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 "cybercrime 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.[22]

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. Measures include education in "information morals" and cyber security poster or slogan com-

[14]情報セキュリティ月間

[15]Information Security Policy Council, 新・情報セキュリティ普及啓発プログラム *[New Information Security Public Awareness Program]* [in Japanese], July 2014, 13, accessed February 14, 2018, `http://www.nisc.go.jp/active/kihon/pdf/awareness2014.pdf`.

[16]国民を守る情報セキュリティサイト

[17]国民のための情報セキュリティサイト

[18]これからセキュリティ！

[19]Information Security Policy Council, 新・情報セキュリティ普及啓発プログラム *[New Information Security Public Awareness Program]*, 16.

[20]Ibid., 17.

[21]Ibid.

[22]Ibid.

petitions. There are also activities aimed at educators and guardians, 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.[23]

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 password and unprepared employees are as much of a threat to a company as is unpatched or misconfigured software.

In seeking to improve the cyber security of the general public, the Japanese government goes beyond just education. It also takes more direct efforts to remove malware from and secure the computers of Japanese users. 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 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.[24]

The creation of the Cyber Clean Center came out of discussions between the government, groups like JPCERT/CC, and firms in the telecommunications sector. METI and MIC were worried that bots and other malware were doing damage to the performance of Japan's networks. While internet service providers 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, none of the them were willing to pay for it—a classic example of the collective action problem. In the end, the effort was funded entirely by the Japanese government.[25]

Along with the Cyber Clean Center, the Japanese government has also pursued more ad-hoc measures to deal with malware. For example, in 2013, Japan began being hit by VAWTRAK, a cyber banking scheme at worked as follows: first, a victim would have their PC infected with malware that came from either a malicious website or email. This malware would then begin communicating with a server controlled by the fraudsters. When the victim attempted to log into an online banking site, the malware would take them to a fake site instead; using the information the user put into the fake site, the server would then transfer

[23]Information Security Policy Council, 新・情報セキュリティ普及啓発プログラム *[New Information Security Public Awareness Program]*, 17.

[24]Telecom-ISAC, *Cyber Clean Center / What is Cyber Clean Center?*, accessed October 16, 2017, `https://www.telecom-isac.jp/ccc/en_index.html`; Kouichi Arimura, *Anti-Bot Countermeasures in Japan*, March 2008, accessed October 17, 2017, `http://www.nca.gr.jp/jws2008/WS1-ccc.pdf`; Brian Krebs, *Talking Bots with Japan's 'Cyber Clean Center' —Krebs on Security*, March 2010, accessed October 16, 2017, `https://krebsonsecurity.com/2010/03/talking-bots-with-japans-cyber-clean-center/`.

[25]Author's interview with employee of JPCERT/CC, Tokyo, August 2017.

money from the victim's account to a designated account held by the fraudsters. At one point, 44,000 computers in Japan were infected with the malware.[26]

In order to deal with this problem, the Tokyo Metropolitan Police Department came up with the following strategy: first, they identified and took control of one of the servers the fraudsters had been using. When a malware-infected computer tried to communicate with the police-controlled server, the server would send back harmless data, and the police would record the IP address of the infected computer. They then provided lists of these IPs to the appropriate ISPs, who were then able to tell the victims that their computers were infected, and to provide instruction on how to remove the malware. The NPA also shared the IP addresses of infected computers with the members of Interpol.[27]

Interestingly, though MIC had been one of the main forces behind the creation of the Cyber Clean Center, it was less supportive of these efforts. MIC initially objected on the grounds that collecting the IP addresses of affected computers amounted to collecting private information about Japanese citizens. There is a certain logic to this: one could infer something about a user's internet behavior by the fact that they had been infected by the malware in the first place. Ultimately, the police were able to convince MIC that this was the right approach, but it illustrates the trade-offs between the desire to protect citizens from malware and the desire to protect citizen privacy.[28]

Along with these more active efforts, the government also releases software tools meant to help users secure their computers. For example, in 2009, IPA created automated tools both to make it easy for users to see if they were using the latest versions of key internet-related software, and to easily disable USB auto-run, a major vector for the spread of malware.[29] These tools continue to be maintained and updated.[30]

Currently, the government is becoming increasingly concerned with the spread of bots across the Internet of Things (IoT). 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.[31]

[26] Danielle Anne Veluz, *VAWTRAK Plagues Users in Japan - Threat Encyclopedia - Trend Micro AU*, June 2014, accessed August 1, 2018, `https://www.trendmicro.com/vinfo/au/threat-encyclopedia/web-attack/3141/vawtrak-plagues-users-in-japan`; *82,000 PCs in Japan, worldwide infected with virus harvesting banking passwords*, April 2015, accessed August 1, 2018, `https://www.rt.com/news/248673-japan-vawtrak-bank-infect/`.

[27] Author's interview with NPA official, Tokyo, July 2017.

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

[29] Information-technology Promotion Agency, *JVN iPedia - Vulnerability Countermeasure Information Database / What is JVN iPedia?*, accessed June 22, 2018, `https://jvndb.jvn.jp/en/nav/jvndb.html`; Information-technology Promotion Agency, *IPA Information-technology Promotion Agency, Japan : IPA/ISEC : Vulnerabilities : "MyJVN Security Configuration Checker" released*, December 2009, accessed June 22, 2018, `https://www.ipa.go.jp/security/english/vuln/200912_myjvn_cc_en.html`.

[30] Information-technology Promotion Agency, *MyJVN - MyJVN バージョンチェッカ [MyJVN Version Checker]* [in Japanese], 2018, accessed June 22, 2018, `https://jvndb.jvn.jp/apis/myjvn/vccheck.html`.

[31] Author's interview with National Police Agency official, Tokyo, July 2017.

These efforts are made possible both by a broad norm that accepts that government has a role to play in protecting individuals from cyber attacks, and close cooperation between firms and the bureaucracy that makes such tools possible. For example, in the case of the Cyber Clean Center, since MIC has jurisdiction over and regularly consults with ISPs on regulatory issues, it was easy for MIC to bring ISPs together to form an agreement on the Center. Just as importantly, the ISPs were happy to work with the government.[32]

Even more than the theory might suggest, there are good reasons why the Japanese government might want to be involved in promoting the adoption of cyber security technology among Japanese firms. Japanese firms have lagged behind foreign competitors in being prepared to deal with cyber security. Compared to firms in many other countries, Japanese firms have relatively low awareness of cyber security risks. According to the Risk Management Survey Report 2015, conducted by Tokio Marine Nichido, only 52.5% of firms responded that information security was a risk they placed a great deal of importance on.[33] By 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.[34] 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).[35] There are a number of possible explanations for this. It is possible that because Japanese is a relatively difficult language for non-native speakers and thus a less hospitable medium for phishing attacks, there is less awareness or fear of them. 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.[36] Regardless of the reason, the fact remains that awareness of cyber risks remains relatively low, though it has been improving.

Nevertheless, the government could simply decide that this was the private sector's responsibility: should firms choose to underinvest in cyber security, so be it. Instead, as we have seen, the government is quite active in trying to get the private sector to invest more in cyber security. In large part, this is explained by the nature of Japan's bureaucracy. As discussed earlier, Japan's bureaucrats are often looking for ways to justify their relevance. Cyber security is clearly an area in which the Japanese private sector is not taking the lead—a perfect opportunity for bureaucrats to show them the way.

This situation has been a godsend for METI. As discussed in Chapter 2, as Japan's

[32]Though the fact that the ISPs were not the ones paying no doubt helped.

[33]Tokio Marine Nichido, リスクマネジメント動向調査 *2015 [Risk Management Survey Report 2015]* [in Japanese], 2015.

[34]Willis Towers Watson, *Decoding Cyber Risk: 2017 Willis Towers Watson Cyber Risk Survey, US Results*, 2017, `https://www.willistowerswatson.com/-/media/WTW/PDF/Insights/2017/06/WTW-Cyber-Risk-Survey-US-2017.pdf`.

[35]Danielle Kriz and Mihoko Matsubara, *Japanese Government Updates Cybersecurity Guidelines: Increased Focus on Cybersecurity Investments and SMBs*, December 2016, accessed February 22, 2017, `http://researchcenter.paloaltonetworks.com/2016/12/gov-japanese-government-updates-cybersecurity-guidelines-increased-focus-cybersecurity-investments-smbs/`.

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

industry matured and liberalization took hold, METI in many ways lost its role as manager of the economy. Schaede quotes a METI official saying in 2007 that "It is no longer fun to be a METI official."[37] As a result, METI was forced to seek out new roles for itself. One of those roles, as discussed earlier, has been as a promoter of innovation policies. But here, in the promotion of cyber security, was another new role for METI. Better, it was a role that in many ways echoed the role it had played in providing administrative guidance: using its informal networks, consensus-building skills, and a generous dollop of moral suasion to convince firms that they need to take cyber security more seriously.

This is not to say that bureaucratic actors do not have genuine policy concerns. MIC is concerned with maintaining Japan's networks. METI is worried about the economic consequences of cyber attacks, and, as mentioned in Chapter 3, believes that strong cyber security can be a selling point for Japanese products and services. Both MIC and METI genuinely want to strengthen the private sector's cyber security; in this case, self-interest and policy interest are mutually reinforcing.

One of the main ways they work to promote the adoption of cyber security technology is via information provision. The Japanese government provides a number of guidelines and frameworks to make it easier for Japanese companies to improve their cyber security and the cyber security of their products. Many of these guidelines are produced by IPA, which as discussed in Chapter 2 is supervised by METI, though others are developed by METI directly or are developed by NISC.

One of the earliest efforts to provide information was the Japan Vulnerability Notes (JVN), which IPA and JPCERT/CC began working on in 1993 and released in 1994. It provides vulnerability information and their solutions, including a searchable database, JVN iPedia.[38] Another effort, aimed more at executives than technical experts, was the Information Security Management Benchmark (ISM-Benchmark), released by the IPA. A firm can go to the website and answer a set of 40 question about the firm (25 about information security measures, 15 about the firm itself). The tool then produces a scatter chart, comparing the cyber security of the firm to other similar firms, as well as producing a security score and giving recommended security approaches.[39]

IPA also releases a number of practical guides, aimed at technical users. These include "How to Secure Your Web Site", "How to Use SQL Calls to Secure Your Web Site", "Approaches for Embedded System Information Security", "Web Application Firewall Guide", and "Design and Operational Guide to Protect Against "Advanced Persistent Threats"". It also regularly publishes descriptions of top security threats.[40]

[37]Schaede, "From developmental state to the 'New Japan': the strategic inflection point in Japanese business," 175–176.

[38]JPCERT/CC and Information-technology Promotion Agency, *Japan Vulnerability Notes / What is JVN?*, accessed June 22, 2018, `http://jvn.jp/en/nav/jvn.html`; Information-technology Promotion Agency, *JVN iPedia - Vulnerability Countermeasure Information Database / What is JVN iPedia?*, accessed June 22, 2018, `https://jvndb.jvn.jp/en/nav/jvndb.html`.

[39]Information-technology Promotion Agency, *Outline of Information Security Benchmark (ISM-Benchmark)*, 2007, `https://www.ipa.go.jp/files/000011798.pdf`.

[40]Information-technology Promotion Agency, *IPA Information-technology Promotion Agency, Japan :*

More recently, there has been a stronger effort to help company executives understand cyber security. In December 2015, METI and IPA released *Cybersecurity Guidelines for Business Leadership Version 1.0*. Version 1.1 was released in December of 2016, and the newest version, 2.0, was released in November 2017.[41] These guidelines urge executives to be conscious of and to plan for cyber risks, including risks not only to one's own company but to partners and suppliers. They also stress the importance of communication with stakeholders. They then give practical advice to executives for developing and implementing cyber security plans, give information about information-sharing organizations such as JPCERT/CC, and point to other resource on cyber security. In particular, the guidelines list 10 points for managers to follow which encompass large parts of ISO/IEC27001 and 27002, international standards on information security management systems.[42]

IoT is becoming a bigger issue as well. 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.[43]

These efforts to develop and promote guidelines are often done with the cooperation of the private sector. The Cyber Security Strategic Headquarters itself includes as members representatives from private sector firms[44], but beyond this, there are a number of working groups within the CSSH, within NISC, and set up by METI and by MIC that work on various aspects of cyber security. Along with allowing the government to obtain input from the private sector, it also gives the government the opportunity to put informal pressure on firms to follow the guidelines and improve their cyber security practices, as well as to educate them about cyber security issues.

One example of such a working group was the one IPA brought together to create the Smart Home Appliance Security Study Report. Between March and December 2010, IPA

IPA/ISEC：*Measures for Information Security Vulnerabilities*, 2018, accessed June 22, 2018, `https://www.ipa.go.jp/security/english/third.html#emb`.

[41]Mihoko Matsubara and Danielle Kriz, *Japan's Cybersecurity Guidelines for Business Leadership*, May 2016, accessed November 15, 2016, `http://researchcenter.paloaltonetworks.com/2016/05/japans-cybersecurity-guidelines-for-business-leadership-changing-the-japanese-business-mindset-and-potentially-raising-the-global-bar/`; Kriz and Matsubara, *Japanese Government Updates Cybersecurity Guidelines*; Ministry of Economy, Trade and Industry, *Cybersecurity Management Guidelines Revised (METI)*, November 2017, accessed June 15, 2018, `http://www.meti.go.jp/english/press/2017/1116_001.html`.

[42]Ministry of Economy, Trade and Industry and Information-technology Promotion Agency, サイバーセキュリティ経営ガイドライン *Ver 2.0 [Cybersecurity Guidelines for Business Leadership Ver 2.0]* [in Japanese], November 2017, accessed June 15, 2018, `http://www.meti.go.jp/press/2017/11/20171116003/20171116003-1.pdf`.

[43]Mihoko Matsubara, *Assessing Japan's Internet of Things (IoT) Security Strategy for Tokyo 2020*, September 2016, accessed February 22, 2017, `http://researchcenter.paloaltonetworks.com/2016/09/cso-assessing-japans-internet-of-things-iot-security-strategy-for-tokyo-2020/`.

[44]National center of Incident readiness and Strategy for Cybersecurity, サイバーセキュリティ戦略本部名簿 *[Cyber Security Strategic Headquarters, Register of Names]*.

held seven study group sessions including employees from SHARPR, Sony, Panasonic, Hitachi Consumer Electronics, and Mitsubishi Electric Corporation, with METI acting as an observer. The report covered security challenges for smart home appliances and approaches to solve those problems. Moreover, it included a specific security guide for Digital TV, including a reference for product design.[45] Obviously one advantage of such groups is that they tap the combined knowledge of industry experts to provide a more comprehensive list of vulnerabilities and possible ways to solve them. Beyond this, they help to assure corporate buy-in, and hopefully help to alleviate a race-to-the-bottom on security by creating a set of security standards to which the major firms in a sector agree to adhere.

Beyond following guidelines and standards, one practice the government is working hard to get firms to adopt is information sharing. Japanese firms are wary of information sharing programs, because in the process of letting other firms know about an attack, a firm reveals that it has been the victim of one. 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 techniques work. Furthermore, even if the techniques do work, within the information sharing institution there will be those who know the true identity of the firm, and the firm must trust that these people will not leak the information.[46]

In short, information sharing is a classic collective action problem. Though all firms would be better off if they all shared information, a given firm increases its risks of harming its reputation by sharing information. Since the information shared by other firms is available to a firm regardless of whether it shares information, a firm's optimal strategy is not to share information. It has thus been very difficult to get Japanese firms to agree to information-sharing schemes, because they are worried that the institution in charge of information-sharing will leak that they have been the victim of a cyber attack, or that the government will take some kind of action against them.[47]

One might think that the government would pass firm regulations requiring information sharing. However, the feeling within the bureaucracy is that it is better to rely on persuasion rather than regulation. In interviews, officials expressed the opinion that the problem was not that there was a fundamental difference of interests, but that instead that firms simply were not fully aware of the ways in which the information sharing programs would ultimately benefit them. They felt that if they can properly educate firms about those benefits, eventually they will come around.[48]

Beyond trying to educate firms about the benefits of information sharing, the government works reduce the fear of that sharing information will lead to government action against firms by funding private alternatives. Two of these organizations, JPCERT/CC and ICT-ISAC,

[45]Information-technology Promotion Agency, *2010 Smart Home Appliance Security Study Report*, January 2011, accessed June 22, 2018, `https://www.ipa.go.jp/files/000014115.pdf`.

[46]Author's interview with JPCERT/CC employee, Tokyo, July 2017.

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

[48]Author's interviews with METI official and NISC official, Tokyo, Summer 2017.

were discussed in Chapter 2. While all information-sharing organizations anonymize data before they share it, if the information-sharing organization is run by the government then the government has access to the original information, including the name of the firm that has experienced an attack. If the government knows the name of the firm, it is possible it will take action against the firm. From the position of the firm, then, an advantage of private information sharing organizations is that they prevent the government from knowing when a firm has been breached. In one interview, a JPCERT/CC employee emphasized that while they were funded by METI, they fiercely maintained their independence from the government precisely because it reassured firms that they could safely share information with JPCERT/CC.[49]

In truth, even if the government did create regulations requiring firms to share information about cyber attacks, this could prove costly to monitor. After all, it is difficult to know if a firm's networks have been breached unless the firm itself reveals the breach. It may be that for some types of firms, such as banks, the monitoring costs are worthwhile, but for many types of firms they may not be. Thus, there are real advantages to convincing firms to participate in information sharing voluntarily, assuming it can be done successfully.

Recognizing that, due to a lack of resources, small- and medium-sized enterprises may have a particularly difficult time properly investing in cyber security, as well as in information technology more broadly, METI and MIC have pushed for tax measures to help them. From FY 2006–2010, the government instituted a set of tax measures called the "Information Base Strengthening Tax System"[50]. 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 ans software to meet the ISO/IEC 15408 criteria for internet technology security.[51] 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.[52]

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 provisions were aimed explicitly at improving the cyber security of these companies; they were added

[49]Author's interview with JPCERT/CC employee, Tokyo, July 2017.

[50]情報基盤強化税制

[51]Ministry of Finance, 租税特別措置法等（法人税関係）の改正 *[Revision of Special Tax Measures Law, etc. (Related to Business Taxes)]* [in Japanese], 2010, 369–370, accessed November 18, 2017, `https://www.mof.go.jp/tax_policy/tax_reform/outline/fy2010/explanation/PDF/08_P350_420.pdf`.

[52]Ibid., 369.

"based on the circumstances that progress in the computerization of small- and medium-sized enterprises, *including dealing with unauthorized access and system faults*, has certainly not been sufficient" (emphasis mine).[53]

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 more 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 a virtual server. The reason given for these tax incentives was to improve the efficiency of small- and medium-sized businesses' use of information technology hardware.[54] 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.[55]

Two other changes were more explicitly aimed at improving cyber security. One change was that while coordination software (defined in the new provisions as "software that receives commands from data processing systems, and performs commands on systems other than data processing systems"[56]) 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.[57]

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 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

[53]"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" Ministry of Finance, 租税特別措置法等（法人税関係）の改正 *[Revision of Special Tax Measures Law, etc. (Related to Business Taxes)]*, 366

[54]Ibid., 366–367.

[55]Ibid., 367.

[56]ibid. "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, 情報処理の促進に関する法律, (略) 情報処理促進法 *[Law Concerning the Promotion of Data Processing]* [in Japanese], last revised in 2008, 1970, accessed November 22, 2017, `http://www.houko.com/00/01/S45/090.HTM`

[57]Ministry of Finance, 租税特別措置法等（法人税関係）の改正 *[Revision of Special Tax Measures Law, etc. (Related to Business Taxes)]*, 367.

to create an IoT platform for the manufacturing industry that, among other things, can automate machines based on data from manufacturing facilities.[58] METI recognizes, however, that in order for the initiative to succeed, strong cyber security is also necessary.[59] Specifically, METI and MIC are calling for 26.092 billion yen in tax breaks (approximately 234.5 million U.S. dollars) in order to support these "Connected Industries" for the next two years.[60] Though it is not clear exactly what percentage of that will go to cyber security, the increase in cyber threats 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 construct security systems able to withstand various cyber-attacks, and will also promote the introduction of further security measures."[61]

Though the existence of strong institutions for economic guidance explains why the Japanese government is so heavily involved in promoting security in the private sector, it does not explain why the government prefers to rely on voluntary measures. Interestingly, the answer is not resistance from the firms, as one might expect. While Japanese firms are somewhat leery of information sharing, due to reputational concerns, they would welcome clear cyber security regulations. For firms, it is difficult to know what the risk of cyber attack is, and how much to invest in order to prevent that attack; at the same time, they cannot simply invest endlessly in cyber security. With a clear set of regulations, they would be able to know for certain whether they were doing enough to protect cyber security. Because Japan has strong norms of public-private coordination, the firms have turned to METI to request such guidance.[62]

METI has resisted, however. METI officials fear that should the government develop such regulations, the firms would simply do what they needed to meet these regulations, without considering their actual cyber security needs. Worse, because cyber security is a quickly shifting problem, there could quickly become a mismatch between what the regulations

[58]Ministry of Economy, Trade and Industry, *Connected Industries (METI)*, accessed February 18, 2018, http://www.meti.go.jp/english/policy/mono_info_service/connected_industries/index.html.

[59]Ministry of Economy, Trade and Industry, 「*Connected Industries*」東京イニシアティブ *2017 ["Connected Industries" Tokyo Initiative 2017]* [in Japanese], October 2017, accessed November 18, 2017, http://www.meti.go.jp/press/2017/10/20171002012/20171002012-1.pdf; Ministry of Economy, Trade and Industry, 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 Revision Requests]* [in Japanese], 2017, accessed November 18, 2017, http://www.meti.go.jp/main/yosangaisan/fy2018/pdf/01_10.pdf.

[60]Ministry of Economy, Trade and Industry, 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 Revision Requests]*; Ministry of Internal Affairs and Communications, 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 Revision Requests]* [in Japanese], 2017, accessed November 28, 2017, http://www.mof.go.jp/tax_policy/tax_reform/outline/fy2018/request/soumu/30y_soumu_k.pdf.

[61]Ministry of Economy, Trade and Industry, 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 Revision Requests]*, 128.

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

require and what would actually be required for security.[63] A lack of regulations also leaves METI in the position of continuing to provide informal guidance to firms, which is clearly an advantageous position for it. Thus, while the Japanese government does quite a bit to promote cyber security in the private sector, it does so by encouraging firms to adopt cyber security technologies rather than by requiring them to do so.

4.3 U.S. Cyber Security Promotion

The U.S. does not have a policy legacy of economic guidance. Without an existing set of instruments that can be easily turned to sector promotion, policy-makers interested in promoting the adoption of cyber security technology in the private sector have turned to legislation. So far, these attempts have not been successful, failing in the face of opposition from the private sector.

often falling apart due to opposition from the business community

For example, one of the early bills meant to promote cyber security promotion in the private sector, proposed by Senators Rockefeller and Snowe in April 2009, would have given responsibility for doing so to the Commerce Department. It would also have required NIST to create auditable industry standards for cyber security, and a certification process for cyber security professionals. Business groups heavily opposed these measures, and ultimately the bill went nowhere. The Obama administration released a proposal for a different bill in 2011, calling only for auditing of critical infrastructure, which also met with massive opposition from firms and went nowhere.[64]

In another attempt, the Cybersecurity Act (CSA) was introduced in February 2012 by Senators Lieberman, Collins, Rockefeller, and Feinstein. It would have authorized DHS to establish mandatory baseline requirements for cyber security in critical infrastructure sectors; it also included provisions to encourage information sharing. Again, it met with strong opposition from industry groups, as well as from Republicans. Industry was worried this could open the door to tort liability for failure to meet standards. Industry representatives also argued that it would be ineffective and would hinder innovation, and that instead of encouraging security, it would simply encourage "compliance": because cyber security threats quickly shift, the regulations would quickly become outdated, but companies would still be forced to spend money complying with them rather than shifting their cyber security investments to meet these new threats.[65]

As a result of this resistance from firms and their political allies, there is not a clear national policy for promoting the adoption of cyber security technology. But the lack of strong

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

[64] Mitchell, *Hacked*, 26–28.

[65] Melanie J. Teplinsky, "Fiddling on the Roof: Recent Developments in Cybersecurity," *American University Business Law Review* 2 (2013): 225–322. Note that while this same argument plays out in Japan, the actors are reversed: businesses are clamoring for regulations, while it is METI that argues this would lead to compliance rather than security.

Figure 4.2: Example of a poster available for download at www.stopthinkconnect.org

institutions for economic guidance has a second effect: there is a lack of actors in government with the motivation and capabilities to promote technology adoption. The bureaucratic actor in charge of domestic cyber security is the Department of Homeland Security, but because DHS has so many different responsibilities, cyber security promotion tends to be neglected. For example, DHS does make some efforts to educate the public about cyber security practices, but these efforts are relatively weak compared to those of Japan. Starting in 2010, DHS was put in charge of the "Stop. Think. Connect." campaign, in partnership with the Anti-Phishing Working Group and the National Security Alliance. Promotional and educational materials are available on its website, as well as the campaign's own website; an example

can be seen in Figure 4.2.[66] DHS also partners with other government agencies, non-profit organizations, and colleges and universities. The campaign also has corporate sponsors such as Google and Microsoft.[67] The campaign relies mainly on the web and social media, as well as participation by partners; as a result, is has less visibility than the Japanese efforts.[68] DHS does not have the kinds of connections with or authority over firms that bureaucratic institutions like MIC or METI have, and so does not play a major role in promoting the cyber security of firms. Moreover, even when it has participated in efforts to create purely voluntary cyber security standards, it has often been met with suspicion from industry.[69]

The DHS does have one important program, the National Cybersecurity and Communications Integration Center (NCCIC), which shares information between the private and public sector on cyber security threats. Founded in 2009, in 2018 it absorbed several other organizations, including US-CERT, the US equivalent to JPCERT/CC, and ICS-CERT, which performed similar functions but specifically for infrastructure. Like JPCERT/CC, NCCIC offers information exchanges, vulnerability analysis, and incident response and recovery.[70] NCCIC has a much heavier focus on critical infrastructure than JPCERT/CC, however.

Despite the fact that DHS has authority over domestic cyber security, arguably the most influential government actor in this area is the National Institute of Standards and Technology. As mentioned in Chapter 2, NIST in charge of producing technical standards and guidelines. It is a small organization, with no regulatory power, staffed with three thousand people and with a budget of $900 million as of 2015. In terms of cyber security promotion, however, its small size is in many ways its strength. It has a clear mission with regard to cyber security, to produce technical standards and guidelines, and it has the expertise to do so successfully. Precisely because it has no regulatory power, firms are not suspicious of its involvement. Moreover, it regularly consults with industry on standards development, through requests for comments and other mechanisms.[71]

NIST comes closest to the kind of economically-oriented bureaucratic actor that one sees in Japan, albeit without regulatory power. Though it does not conduct the more extensive types of programs we see in Japan, it does produce cyber-security-related standards and guidelines. Federal Information Processing Standards (FIPS) are security standards for

[66]Department of Homeland Security, *Stop.Think.Connect. | Homeland Security*, accessed June 23, 2018, `https://www.dhs.gov/stopthinkconnect`; Stop Think Connect, *Stop.Think.Connect.*, accessed July 31, 2018, `https://stopthinkconnect.org/`.

[67]Department of Homeland Security, *Stop.Think.Connect. National Network*, August 2012, accessed July 31, 2018, `https://www.dhs.gov/stopthinkconnect-national-network`; Stop Think Connect, *Our Partners*, accessed June 23, 2018, `https://stopthinkconnect.org/get-involved/our-partners`.

[68]Though it is hardly a scientific sample, I have seen cyber security advertisements in a number of prominent locations in Japan; I have yet to see a single such advertisement in the U.S.

[69]For a number of examples, see Mitchell, *Hacked*.

[70]US-CERT, *National Cybersecurity and Communications Integration Center | US-CERT*, accessed July 31, 2018, `https://www.us-cert.gov/nccic`; Department of Homeland Security, *National Cybersecurity & Communications Integration Center*, May 2011, accessed June 24, 2018, `https://www.dhs.gov/national-cybersecurity-and-communications-integration-center`; US-CERT, *About Us | US-CERT*, accessed July 31, 2018, `https://www.us-cert.gov/about-us`.

[71]Mitchell, *Hacked*, 46.

federal agencies (except for national security systems), but can also be adopted by non-federal government organizations and the private sector. They are issued by NIST after approval by the Secretary of Commerce.[72] It also publishes Special Bulletins (SP), two series of which deal with cyber security: SP 800 and SP 1800. SP 800 publications are aimed at the computer security community, and include guidelines, recommendations, technical specifications, and annual reports of NIST's cyber security activities. SP 1800 are also aimed at the cyber security community, but demonstrate how to apply standards and best practices; that is, they are "how-to" guides.[73]

Despite the efforts of NIST, we can see that overall the U.S. does little to promote the adoption of cyber security technology in the private sector. In the main, this is due to a lack of strong institutions for economic guidance. However, an additional factor is the strength of its own national security institutions, and the privacy concerns that these raise. Because intelligence agencies have an incentive to gather personal information about users, there is little trust for them among privacy groups in the civil sector. This has made some efforts to promote cyber security in the private sector, such as information sharing, particularly difficult. For example, in 2012, the Republican House passed the Cyber Intelligence Sharing and Protection Act (CISPA) which would have promoted information sharing between private firms and federal agencies, including law enforcement and the NSA. However, the bill was ultimately killed due to opposition from the ACLU and its allies within the Democratic Party, including the Obama White House.[74]

In this manner, cyber security policy has been quite controversial in the U.S., having to thread the needle between firms opposed to regulation and their mostly-Republican allies, and privacy advocates who worry about the government collecting private information and their mostly-Democratic allies. This, along with a lack of government organizations with the incentives and capabilities to promote cyber security in the private sector, means that the U.S. does little in this area.

4.4 South Korean Cyber Security Promotion

In South Korea, as in Japan, a policy legacy of economic guidance has created both the motivation and tools for the promotion of the adoption of cyber security technology in the private sector. In fact, the government's promotion of ICT infrastructure in many ways set the stage for the need for government promotion of cyber security in the private sector. Due to the government's efforts, South Korea is one of the most wired countries in the world, but the security of its firms has not kept up. According to MSIP, as of 2014, only 3% of

[72]Thelma A. Allen, *FIPS General Information*, February 2010, accessed June 24, 2018, `https://www.nist.gov/itl/fips-general-information`.

[73]Thelma A. Allen, *NIST Special Publication 800-series General Information*, May 2018, accessed June 24, 2018, `https://www.nist.gov/itl/nist-special-publication-800-series-general-information`; Thelma A. Allen, *NIST Special Publication 1800-series General Information*, May 2018, accessed June 24, 2018, `https://www.nist.gov/itl/nist-special-publication-1800-series-general-information`.

[74]Mitchell, *Hacked*, 31.

South Korean companies invested more than 5% of their IT budget into security; by contrast, about 40% of American companies did so.[75] The combination of strong ICT infrastructure and weak cyber security left South Korea especially vulnerable to cyber attacks, both from within the country and from without. North Korea, of course, provides a particularly strong external challenge, but hackers from other countries have also found South Korea a useful playground on which to test out their techniques.[76]

Decisions that were made by both firms and the government in the development of South Korea's web site ecology have also made stronger private sector cyber security a particularly important issue for South Korea. In South Korea, every individual is given a resident registration number (RRN), used as a unique identifier for the individual, to be used for government services, banking, and so forth. Most South Korean web sites require users to use their RRN to create an account. In theory, this is a way of verifying the identity of users and reducing transaction costs between services, but it has had major consequences for the security of the personal information of South Korean citizens: it increases the number of places a person's RRN is stored, and allows a person to be traced across different web sites and information about their behavior to be collected.[77] Worse, it turns out that these RRNs can be easily extracted from encrypted data, meaning there is no easy way to keep them protected.[78]

The government has encouraged the practice of collecting RRNs: a law on encrypted online communications requires internet companies to keep the RRNs of users in order to provide online transaction services. Again, this has the advantage of making transactions easier, but the result is that RRNs are stored in more locations, increasing the risk that they will be stolen. What is more, in an attempt to resolve problems with online bullying and libel, in 2010 the government created a regulation requiring internet users to create a verifiable real-name registration to comment on sites with more than 10 thousand daily users. The result is that there are now a number of sites where the real name of users is stored along with their RRNs, increasing the risk of identity theft.[79]

As a result of these conditions, starting in the mid-2000s the leaking of personal information became a major problem in South Korea. Not all of these leaks were the result of hacking, either: in some cases, websites of both private and public organizations posted

[75]"Incentives to be given for information security," *Joins.com*, August 2014, accessed June 21, 2018, `http://global.factiva.com/redir/default.aspx?P=sa&an=JOONAI0020140731ea8100018&cat=a&ep=ASE`.

[76]Nir Kshetri, "Cybersecurity in South Korea," in *The Quest to Cyber Superiority* (Springer, Cham, 2016), 175; Soyoung Ho, *Haven for Hackers*, October 2009, accessed April 19, 2018, `https://foreignpolicy.com/2009/10/26/haven-for-hackers/`.

[77]Tong-hyung Kim, "Calls for Independent Privacy Agency Grow," *Korea Times*, April 2010, accessed June 19, 2018, `http://global.factiva.com/redir/default.aspx?P=sa&an=KORTIM0020100422e64l0000h&cat=a&ep=ASE`.

[78]Latanya Sweeney and Ji Su Yoo, "De-anonymizing South Korean Resident Registration Numbers Shared in Prescription Data," *Technology Science*, September 2015, accessed July 5, 2018, `https://techscience.org/a/2015092901/`.

[79]Kim, "Calls for Independent Privacy Agency Grow."

names, RRNs, and other personal information publicly.[80] As an example of the scale of the problem, in 2008 alone eBay's local unit was broken into by Chinese hackers who stole the information of 18.6 million customers, and 20 million subscribers of an online service from a major retailer, Shinsegae, and its social media site, I Love School, had their data stolen.[81] In 2011, SK Communications, an ISP and web portal company, was hacked and the information of 35 million people was stolen.[82] These are only some of the bigger examples of data being stolen.

Nor is the only problem data being stolen. There have been a number of attacks on financial institutions, leading to service outages. This includes a DDOS attack in 2009; malware that erased the hard drives of one of the largest banks in 2011, leaving customers without access to ATM services for days; a 3 week attack on Nonghyup Agricultural Bank, also in 2011; and the outage of ATMs and online banking systems in 2013, again due to malware that wiped out hard drives. There have also been attacks on the media, including the destruction of databases at two major conservative South Korean newspapers in 2012. Worse, in 2014, South Korea's nuclear power plant operator, Korea Hydro and Nuclear Power Co Ltd (KHNP) faced cyber attacks and had data stolen, including power plant blueprints, testing data, and payroll information. The South Korea government claims that North Korea's cyber attacks alone cost South Korea over $805 million between 2009 and 2013.[83]

Given the heavy government involvement in the promotion of ICT, and the threats to personal information and to South Korean firms, it is unsurprising that South Korea has passed a number of laws aimed at improving private-sector cyber security. The earliest of these was the Framework Act on Information Promotion in 1995, which included basic matters related to cyber security. This were followed by the Act on the Protection of Information and Communications Structure (2001), the Act on Promotion of Digitalization of Administrative Work for E-Government Realization (2001), the Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc. (originally the Act on Promotion of Utilization of Information and Communications Network, but revised in 2001 to strengthen cyber security regulation, and then amended again in 2004; referred to hereon as the Network Act), and the National Cyber Security Management Regulation (2005). Laws and regulations targeted at specific sectors, such as finance, have also been enacted. The most important of these are the Electronic Financial Transactions Act (EFTA), which among other things prohibits intrusion into the network systems of financial companies, and the Credit Information Use and Protection Act (hereon the Credit Information

[80]Hee-seop Kim, "Internet Leakage of Personal Details Reaching Epic Proportions: KISA," *Chosun Ilbo*, December 2004, accessed June 19, 2018, `http://global.factiva.com/redir/default.aspx?P=sa&an=DIGCHO0020041223e0cn0000k&cat=a&ep=ASE`; "More Personal Information Leaks Found," *Dong-A Ilbo Daily*, April 2006, accessed June 19, 2018, `http://global.factiva.com/redir/default.aspx?P=sa&an=DONGAI0020060405e24600009&cat=a&ep=ASE`.

[81]Kim, "Calls for Independent Privacy Agency Grow."

[82]Seung-hyun Jung, "Seoul gets tough with cyber security," *Joins.com*, August 2011, accessed June 19, 2018, `http://global.factiva.com/redir/default.aspx?P=sa&an=JOONAI0020110809e7890000m&cat=a&ep=ASE`.

[83]Kshetri, "Cybersecurity in South Korea," 171–172.

Act), which regulates organizations that use, manage, or provide credit information.[84]

Like Japan, South Korea has a set of bureaucratic organizations that play a large role in promoting the adoption of cyber security technology in the private sector. The most important may be the Korea Internet & Security Agency, which was created both to promote network infrastructure and to improve South Korea's private sector cyber security. Because the justification of its continued existence and budget is so clearly tied to the promotion of cyber security, it is extremely active in doing so.

KISA takes a number of actions meant to improve the cyber security of the general public. In 2011, the government ran a national campaign to encourage people to change their passwords on a regular basis and to protect themselves from personal data theft.[85] It also takes direct actions to improve the cyber security of the public. KISA maintains the Cyber Curing System, which works in much the same way as Japan's Cyber Clean Center. But KISA goes beyond this: it also monitors South Korean web pages, looking for malicious code. If it finds such code, it contacts the owner of the web page to inform them of the problem; if the problem is not quickly fixed, KISA deletes the web page. It also monitors foreign web pages and blocks access to them from the South Korean internet if they contain malicious code. It also runs the DDoS Cyber Shelter, which operators of web servers can ask for aid in defending themselves from distributed denial-of-service attacks. Finally, it maintains a 24/7 call center, which users and operators can call for advice and to report an attack.[86]

The Ministry of Science and ICT takes on the role of encouraging firms to adopt cyber security technologies. Along with the production of guidelines and other information provision services, it provides incentives for meeting certain guidelines. In particular it grants the Information Security Management System (ISMS) certification to organizations that establish and operate a "comprehensive management system". A comprehensive management system is made up of administrative, technical, and physical measures to secure and ensure reliability of network systems. A company that receives this certification is given additional credit when being evaluated for other government-issued certifications. It may also receive a discount when buying data protection-related insurance.[87]

MSIP also provides tax incentives and subsidies to encourage firms to invest in cyber security. Until 2014, it gave a 7% tax waver for cyber security spending at small- and mid-size companies; in 2014 this was increased to 10% through 2017. MSIP also gives companies a 25% subsidy toward spending on regular inspections and consulting by security expert, and up to 900,000 won (around $800) per person per month to hire cyber security experts. Beyond direct incentives, MSIP has also urged insurers to give a discount of up to 15% to

[84]Korea Internet and Security Agency, *2017 Korea Internet White Paper*, 2017, 29–30; Doil Son and Sun Hee Kim, *Korea Cybersecurity –Getting The Deal Through –GTDT*, January 2018, accessed April 20, 2018, `https://gettingthedealthrough.com/area/72/jurisdiction/35/cybersecurity-korea/`.

[85]Jung, "Seoul gets tough with cyber security."

[86]Oh, *Current Cybersecurity Trends and Responses in Korea.*

[87]Son and Kim, *Korea Cybersecurity –Getting The Deal Through –GTDT.*

local businesses that are recognized for strong cyber security.[88]

The Korean Communications Commission (KCC), which is in charge of regulation the telecommunications and broadcasting sectors, also has an obvious interest in promoting cyber security in the private sector. It awards certifications under the Personal Information Management System (PIMS). Online service providers can obtain certifications for implementing certain technical, administrative, and physical measures to ensure the protection of personal information. A benefit of PIMS certification is that should a breach of the Network Act occur, the online service provider may obtain up to a 50% deduction from the resulting fine.[89]

Unlike Japan, which relies heavily on voluntary measures, South Korea places a number of legal requirements regarding cyber security on its firms. Under the Personal Information Protection Act (PIPA), enacted on September 30, 2011, any entity managing personal information must appoint a chief privacy officer (CPO). This officer is responsible for monitoring the personal information management of the entity and reporting any violations of data security laws to the head of the organization. Moreover, if a company is designated as an "online service provider", the Network Act requires that its CPO, in addition to the duties above, must also deal with customers' privacy-related complaints; additionally, the company must also hire a chief information-security officer (CISO) to monitor the company's data security system and ensure there are no weaknesses. Additionally, any company whose sales revenue from their information and communications business for the preceding year is at least 10 billion won (slightly more than $9 thousand), or who have more than 1 million average daily users, or whose annual sales are at least 150 billion won (about $140 million) is required to acquire Information Security Management System (ISMS) certification.

More specific obligations include:

- creating and then implementing a management plan that sets out organizational and procedural details relating to information security, including response plans in the case of cyber security incidents;
- restricting access to personal data;
- adopting measures to securely keep and transfer personal information;
- adopting measures to prevent forging and falsification of access logs;
- installing and updating security programs for protecting personal information; and
- establishing a secure storage space for personal information.

The MOIS is authorized to investigate companies to assess their protection of personal data. Additionally, the Personal Information Protection Committee, under the jurisdiction of the President, can ask companies for materials demonstrating their level of compliance with

[88] "Incentives to be given for information security."

[89] Son and Kim, *Korea Cybersecurity –Getting The Deal Through –GTDT*.

the law. Failure to take sufficient security measures which leads to loss, theft, leakage, falsification, or damage to personal information can lead to up to two years of imprisonment or a fine of up to 20 million won (around $18.6 thousand).[90]

Financial companies have even stronger obligations. They, too, must appoint a CISO, but with expanded responsibilities. Beyond monitoring and protecting the IT systems, the CISO must create strategies to ensure the safety of electronic financial transactions, including preventing accidents; must manage the personnel and the budget for securing IT systems, as well as train officers and employees in IT security; and must conduct self-assessments of the safety and security of IT systems. Additionally, should the company hire at least one thousand full-time employees and have total assets of at least 10 trillion won (around $9 billion), the CISO is prohibited from taking on responsibilities beyond those listed above, to ensure that the CISO is properly focused on ensuring cyber security. Financial companies also must follow security standards set by the Financial Services Commission (FSC). These standards cover personnel, facilities, electronic devices, and other expenses. Companies must also report the results of analyses of their network and electronic financial transaction systems.[91]

The Credit Information Act places specific cyber security requirements on credit information companies. Specifically, they must:

- establish and implement access-control systems;
- implement measures to prevent the alteration of, tampering with, or destruction of credit information;
- establish a structure that provides different rights to credit information to different persons depending upon their positions and tasks; and,
- carry out periodic inspections of credit information examination logs.[92]

Finally, under the Location Information Act, there are specific requirements for companies engaged in the collection and use of location information. These companies must:

- designate a location information management officer;
- implement access control for each stage of location data flow;
- establish guidelines on the responsibilities of the people handling location information;
- manage records of the provision of location information; and
- conduct regular self-audits to make certain that location information is being properly protected.[93]

[90] Son and Kim, *Korea Cybersecurity –Getting The Deal Through –GTDT*.
[91] Ibid.
[92] Ibid.
[93] Ibid.

There are also strict reporting requirements for the various types of companies. Any company that handles personal data must report an information leak involving at least 10 thousand people to MOIS or to KISA, or face a fine of up to 30 million won (almost $28 thousand). An online service provider that has had an electronic intrusion incident must report to MSIP or to KISA, or face a fine of up to 10 million won (a little over $9 thousand). They are also required to report information leaks regardless of the number of people affected, or face a fine of up to 30 million won (almost $28 thousand). Credit information companies must notify the affected subjects of credit information leaks or face a fine of up to 50 million won (around $45 thousand). Finally, financial companies must report any electronic intrusion incidents to the FSC or face a fine of up to 10 million won (a little over $9 thousand).[94]

Thus, we can see that the strong institutions for economic guidance within South Korea have led to a very active approach to promoting cyber security. But, as with the U.S., in some ways the fact that South Korea has strong national security institutions has made promotion of cyber security within the private sector more difficult. For example, the government passed amendments to the 2007 Protection of Communications Secrets Act in order to expand its own surveillance capabilities. These amendments require that telecommunications companies and ISPs retain a large amount of data about users: access records and log files, web sites visited, time of access, and files downloaded and uploaded for at least three months. It also required that telephone numbers of callers and receives and GPS locations be kept for 12 months.[95] This certainly makes the job of the National Intelligence Services easier, but also creates a wide variety of personal information that can be obtained and abused by hackers.

The strong national security institutions have also made passing legislation to improve private sector cyber security more difficult. While there has been wide agreement between the right and the left that the government needs to push forward measures to promote cyber security, there has been strong disagreement over what actors should be given responsibility for these measures. The right has tended to favor existing national security organizations while the left has pushed for new, independent agencies to be created. The skepticism of the left is not unwarranted—not only did the security agencies support the authoritarian governments of the past, they have more recently intervened in elections on behalf of the right as well. In 2012, the director and other senior officials of the National Intelligence Service mobilized a team of psychological warfare experts to ensure that the conservative party won the election. A recent in-house investigation found that its cyber warfare unit formed as many as 30 extra-departmental teams in order to run a propaganda campaign in support of the conservatives.[96]

An example of the effect this has had on efforts to strengthen private sector cyber security can be seen in the debate over the passage of Personal Information Protection Act. Though passed in 2011, initial debate over PIPA began in 2008, in response to a number of highly-publicized leaks of personal information. Notably, both the ruling conservative party and

[94]Son and Kim, *Korea Cybersecurity –Getting The Deal Through –GTDT*.

[95]*South Korea | OpenNet Initiative*, August 2012, accessed August 6, 2018, `https://opennet.net/research/profiles/south-korea#footnote106_196rpsn`.

[96]McCurry, "South Korea spy agency admits trying to rig 2012 presidential election."

the main opposition party agreed that the government needed to take stronger measures to protect personal information, and in many ways agreed on what needed to be done. Where agreement ended was on who should be in charge of enforcing the Act. The ruling conservative party favored the Ministry of Public Administration and Security (MPAS, now the Ministry of the Interior and Safety), which was at the time in charge of overseeing privacy regulations. Opposition lawmakers, supported by civil liberty advocates, wanted to establish an independent body instead. Though their stated reason was that the Ministry had failed to protect private information so far, there was also a fear that this would further promote an intrusive state.[97] Ultimately the conservatives would win and the legislation would pass, but only after discussions had been dragged out over three years. This, despite the fact that both sides fundamentally agreed on the types of measures the government needed to take.

Another example of this dispute occurred in 2013, when the ruling conservative party proposed a bill to establish an agency under the jurisdiction of NIS that would investigate cyber attacks on the private sector. Because NIS was involved, however, this proposal was met with considerable skepticism from the opposition. The opposition worried that such a law would give NIS more opportunities to interfere in domestic politics.[98] This time it was the left that won: whatever the merits in terms of strengthening private sector cyber security, they did not want to give that kind of power to NIS.

Thus we can see that while strong institutions for economic guidance have led South Korea to pursue strong measures for improving cyber security in the private sector, its strong national security institutions in some ways make this more difficult. Moreover, while in both the U.S. and South Korea the involvement of intelligence and security agencies in cyber security raises privacy concerns, in South Korea these concerns are exacerbated by a history of involvement by the NIS in domestic politics. Despite these issues, the South Korean government is still quite active in promoting cyber security in the private sector.

4.5 Critical Infrastructure

Critical infrastructure is a partial exception to the argument presented at the beginning of this chapter. Critical infrastructure is one area of cyber security in which we do see signs of eventual convergence, despite differences in policy legacies. The threat to a state, its economy, and its population of a cyber attack on critical infrastructure is so clear that any state with the capabilities will work to strengthen the cyber security of its critical infrastructure firms. Indeed, an OECD report in 2007 that looked at Australia, Canada, Japan, South Korea, the Netherlands, the United Kingdom, and the United States found that all seven had clear policies for strengthening the cyber security of critical infrastructure.[99]

[97] Kim, "Calls for Independent Privacy Agency Grow."

[98] Ji-hye Jun, "Parties at odds over cyber security agency," *The Korea Times; Seoul* (Seoul, South Korea, Seoul), March 2013,

[99] Nick Mansfield, *Development of Policies for Protection of Critical Information Infrastructures*, Ministerial Background Report DSTI/ICCP/REG(2007)20/FINAL (OECD, 2007), accessed July 25, 2018, `http:`

Policy Legacies		Policy Outcomes	
Security Capabilities Maintenance	Economic Guidance	Critical Infrastructure Cyber Security Promotion	Other Private Sector Cyber Security Promotion
Weak	Weak	Yes	No
Weak	Strong	Yes	Yes
Strong	Weak	Yes	No
Strong	Strong	Yes	Yes

Figure 4.3: Critical infrastructure firms as the exception.

This does not mean, however, that institutions play no role. Countries with a policy legacy of economic guidance have a readily available set of instruments to be used in the promotion of cyber security in critical infrastructure sectors that countries without do not. As a result, even though both types of countries will promote the cyber security of critical infrastructure, those with a policy legacy of economic guidance can do so more quickly and easily. The differences between U.S. promotion of critical infrastructure cyber security and Japan's illustrate this point.

In the U.S., the need to protect the cyber security of critical infrastructure is widely recognized. Despite this, it has not been easy to implement measures to do so. The U.S. has taken two main steps to improve the cyber security of critical infrastructure: it has encouraged information sharing, and it has created a voluntary framework for critical infrastructure cyber security.

The first of these measures was relatively easy to implement. In 2002, Congress passed the Critical Information Infrastructure Act, which created the Protected Critical Information Infrastructure program. Under this program, any information that critical infrastructure operators share is secure from Freedom of Information Act (FOIA) requests; state, local, tribal, and territorial disclosure laws; use in regulatory actions; and use in civil litigation. NCCIC restricts access to the data to trained and certified government employees and contractors.[100] As one might imagine, this particular measure was quite popular with critical infrastructure firms.

The second measure, the Framework for Improving Critical Infrastructure Cybersecurity is entirely voluntary. It does not consist of specific technical information, but instead provides a general approach to understanding and providing for the cyber security of critical infrastructure facilities, with specific functions to be achieved (such as identifying the cyber security needs and assets of the company, or making certain cyber attacks can be detected

//www.oecd.org/sti/40761118.pdf.

[100]National Cybersecurity and Communications Integration Center, *NCCIC Year in Review 2017: Operation Cyber Guardian*, 2018, accessed July 31, 2018, https://www.us-cert.gov/sites/default/files/publications/NCCIC_Year_in_Review_2017_Final.pdf.

and analyzed), with categories and subcategories containing more specific types of actions to be taken. It is meant to help operators understand the state of cyber security for their firms, and to provide direction as to where to improve. The Framework also points to specific technical specifications that may be helpful for enacting the actions listed under the subcategories. It is meant to be customizable, with the recognition that different critical infrastructure sectors will have different needs.[101]

Despite its voluntary nature, there were a number of difficulties in developing the framework. Development began on February 12, 2013 when President Obama signed Executive Order 13636, which called for the development of a framework to protect the cybersecurity of U.S. critical infrastructure. Responsibility for the effort was given to NIST, which decided that the best way to proceed would be to bring together stakeholders and collectively create a framework. NIST released a Request for Information (RFI) in February 2013 in order to collect information from critical infrastructure firms about current best practices, and to create a baseline for discussion. It then set up a series of workshops that would take place over a year, where stakeholders would be able to come together and help to shape the framework. Participation in the workshops would be voluntary. NIST was able to play this role because it is well-known and well-respected by the private sector, and because it has had a lot of experience in working with the private sector to create standards and guidelines.[102]

Though a number of firms agreed to participate in the process, they were deeply suspicious of the motives of the government. While the government claimed that the framework would be entirely voluntary, industry was worried that the "voluntary" framework would be turned into regulations. The involvement of DHS in the process exacerbated those fears. DHS was participating because, despite its lack of regulatory power, it is officially responsible for the nation's critical infrastructure. But firms were suspicious that DHS would want to create mandatory regulations, because this would enhance its own position. These fears seemed confirmed when the DHS mentioned "metrics" in one of the workshops. In fact, DHS had been tasked by the government with creating performance goals, and had only meant the metrics to be a way of measuring progress, but from the perspective of the firms, metrics would give the government a way to judge which firms were and were not performing adequately. This would make it easy to take the next step of penalizing firms who were not measuring up. Seeing the reaction from industry representatives, DHS dropped this language entirely, which greatly reassured the firms.[103]

The other issue that almost derailed the process was privacy. The initial version of the framework had an extensive privacy section, which industry groups wanted killed, again worrying that it would lead to regulation. Privacy advocates, including the ACLU, warned that retreating from the privacy commitments would allow the government to collect citizen data using cyber security as an excuse. Ultimately, NIST dropped the privacy section,

[101]National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*, technical report NIST Cybersecurity White Paper (Gaithersburg, MD, April 2018), v–vi, accessed June 23, 2018, `http://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.02122014.pdf`.

[102]Mitchell, *Hacked*, 46–50.

[103]Ibid., 56–58.

instead including a general privacy methodology that had the support of both sides, along with the promise that it would work on a separate initiative on privacy engineering starting in 2014.[104]

Ultimately, the voluntary framework was adopted, and industry was quite enthusiastic about the final product. But the amount of effort it required to institute what was an entirely voluntary framework, with a large amount of flexibility in how it was applied, for only that portion of the private sector most vital to national security, gives a sense of just how difficult policy-making in this area has been in the U.S. Part of the problem is there are not established norms for collaboration between the government and the private sector. Whereas the Japanese government has a number of ongoing working groups discussing cyber security standards, NIST had to set up a special process to create this framework. The other major problem is the distrust of the government on the part of the firms. Though ultimately the framework was successfully created, it almost fell apart several times because the firms did not trust the intentions of the government: despite the fact that the government had stated from the beginning that this framework would be voluntary, the firms had difficulty believing this.

By contrast, the Japanese government has had little difficulty in promoting critical infrastructure cyber security. Of course, as we have seen, the Japanese government promotes the cyber security of firms more broadly, and these measures apply to critical infrastructure firms as well. However, recognizing that cyber attacks on critical infrastructure present a far greater threat than those on other types of firms, it takes special measures in this area. While the U.S. had to develop a process for consulting with critical infrastructure firms, the Japanese government could rely on existing instruments. In particular, it already has a system by which particular ministries are responsible for particular critical infrastructure sectors, and it can draw on these existing relationships both to consult with industry about cyber security measures, and to push firms to adopt particular cyber security practices.

As with the private sector more broadly, one of the Japanese government's main tools for promoting cyber security is information provision. The Cabinet Secretariat regularly reviews and releases two important documents regarding critical infrastructure cyber security: the Guidelines for Safety Principles for Ensuring CI Security[105], and the Manual for Prioritization of Information Security Measures.[106] The former is essentially a guide to rule-making: it describes not particular standards, but what ought to be taken into consideration when standards are designed, and what types of information they should include. The document defines "safety standards" broadly: standards set by the government under industry laws, recommended standards from the government, industry standards and guidelines developed by industry groups, and internal rules developed by critical infrastructure operators all fall

[104]Mitchell, *Hacked*, 64,69–70.

[105]Also sometimes translated as the Guidelines for the Establishment of Safety Standards of CIIP.

[106]Cyber Security Strategic Headquarters, *The Cybersecurity Policy for Critical Infrastructure Protection (4th Edition)*, April 2017, 12, accessed May 19, 2018, `http://www.nisc.go.jp/eng/pdf/cs_policy_cip_eng_v4.pdf`.

under the category of "safety standards", and the intention is that all should follow the recommendations laid out in the guidelines.[107]

The manual is aimed at helping critical infrastructure operators create effective plans for improving the security of their information technology systems, with a particular focus on risk assessment, which was first raised as an issue in the 3rd Edition of the Cybersecurity Policy for Critical Infrastructure Protection. It is based on the guidelines found in ISO/IEC 27005:2011, an international standard for information security risk management. In essence, the manual lays out one way an operator might implement the recommendations found in the Cybersecurity Policy for Critical Infrastructure Protection, though the document is clear it is meant only as a single example, and that other implementations are also acceptable.[108]

Along with these two documents, the Cabinet Secretariat conducts and releases surveys on the status and trends of facilities and technologies from the perspective of cyber security in order to aid operators with risk assessment. It analyzes new sources of risk inherent to such facilities and technologies, and shares this information with critical infrastructure operators. It also analyzes and produces information about spillover effects from critical infrastructure outages, and provides the Risk Assessment Guidelines for Mission Assurance.[109]

Another way in which the government promotes critical infrastructure cyber security is by setting up and supporting organizations for information sharing and other types of cyber security promotion. To make it easier for the government to share information meant to help prevent or quickly recover from cyber attacks among critical infrastructure firms, in 2006 the government created a Capability for Engineering of Protection, Technical Operation, and Response (CEPTOAR) for each of critical infrastructure sector.[110] Essentially these are organizations whose membership is the firms of the relevant sector, and which transfer information from the Cabinet Secretariat via the responsible ministries to their members. The government also created a CEPTOAR Council, which has representatives from each CEPTOAR and shares information across sectors.[111] Prior to 2017, critical infrastructure operators were supposed to submit information to the Cabinet Secretariat via responsible ministries.[112] However, operators were reluctant to submit information—which, again, is entirely voluntary—because they were afraid of being subject to disciplinary guidance by the government as a result. In order to address this, the government created an additional

[107]Cyber Security Strategic Headquarters, *The Cybersecurity Policy for Critical Infrastructure Protection (4th Edition)*.

[108]Information Security Policy Council, *The Basic Policy of Critical Information Infrastructure Protection (3rd Edition)*, May 2014, `http://www.nisc.go.jp/eng/pdf/actionplan_ci_eng_v3.pdf`; Cyber Security Strategic Headquarters, *The Cybersecurity Policy for Critical Infrastructure Protection (4th Edition)*.

[109]Cyber Security Strategic Headquarters, *The Cybersecurity Policy for Critical Infrastructure Protection (4th Edition)*, 22–23,32.

[110]At the time there were only ten sectors considered "critical infrastructure", but the number of CEPTOAR has been increased as new sectors have been added to that list.

[111]Information Security Policy Council, *Action Plan on Information Security Measures for Critical Infrastructures*, December 2005, accessed May 19, 2018, `http://www.nisc.go.jp/eng/pdf/actionplan_ci_eng.pdf`.

[112]Each critical infrastructure sector has a ministry that is responsible for overseeing that sector.

method of information reporting. Now, instead of reporting to a ministry, an operator can choose to report the data to the CEPTOAR secretariat. The secretariat then anonymizes the data before passing it along to the government, protecting the firm from disciplinary guidance.[113]

Another important organization related to critical infrastructure is the Control System Security Center, which was established by METI in 2012 to promote the security of control systems. Though control systems can increasingly be found in consumer products as well, traditionally they are found in machines associated with critical infrastructure such as those found in power and sewage plants, and with machines involved in the manufacturing process. METI founded CSSC due to its worries about the security of control systems in critical infrastructure, particularly in the wake of STUXNET (which attacked Iran's nuclear centrifuges) and the 3/11 earthquake and tsunami, which while a natural disaster demonstrated the kinds of effects an attack on critical infrastructure could have. The CSSC certifies control systems, and, perhaps more importantly, has a base in Tohoku that runs seven test beds for research and development on control systems security. The latter is particularly important for critical infrastructure because the risks and costs of running cyber security experiments on real plants are too high.[114]

Voluntary cross-sectoral exercises are another instrument the government uses to promote the cyber security of critical infrastructure firms. Run by the Cabinet Secretariat, these bring together operators from different critical infrastructure sectors to participate in tabletop and functional exercises, meant to identify problems and responses that are common cross-sectorally. This information is then distributed even to those operators that did not participate in the exercise.[115]

Overall, then, states with policy legacies of economic guidance make stronger efforts to promote cyber security in the private sector. In the main, this is because governments in such states see doing so as part of their role, and firms and other private sector actors, used to cooperating with the government, do not oppose such efforts. However, even in the area of critical infrastructure, where the need for government action is relatively clear, states with policy legacies of economic guidance have an advantage over states without.

[113]Cyber Security Strategic Headquarters, *The Cybersecurity Policy for Critical Infrastructure Protection (4th Edition)*.

[114]Seiichi Shin, "A status of control system security in Japan," in *2015 10th Asian Control Conference (ASCC)* (May 2015), 1–4.

[115]Information Security Policy Council, *Action Plan on Information Security Measures for Critical Infrastructures*; Cyber Security Strategic Headquarters, *The Cybersecurity Policy for Critical Infrastructure Protection (4th Edition)*.

Chapter 5

Conclusion

5.1 Revisiting the Argument

A state's cyber security policy is determined in large part by particular policy legacies. Policy legacies affect current policy by making certain policy instruments available, and by socializing actors to seek out and try to solve particular types of problems. Whether a state has a policy legacy of maintaining strong traditional security capabilities determines whether it promotes its cyber security sector. Actors within national security institutions are conditioned to view the promotion of indigenous technologies through the prism of national security. Both in order to protect military networks from intrusion, and in order to have the human capital to build specialized cyber security tools, actors within such institutions have strong reasons for wanting a strong indigenous technological base. Moreover, strong national security institutions have funds that can be used to support the cyber security sector, through procurement and other means. Indeed, we see that the U.S. and South Korea, which have policy legacies of maintaining strong traditional security capabilities, have been quite active in promoting their cyber security sectors. As Japan does not have such a legacy, promoting the cyber security sector lacks strong support within the government.

States with a policy legacy of economic guidance promote the adoption of cyber security technology in the private sector. These states have government actors whose duties involve shaping firm behavior to the benefit of the economy as a whole. From the perspective of these actors, under-investment in cyber security technologies or a failure to adopt best security practices are little different than other types of behavior that may harm economic growth and international competitiveness. For these actors, promoting the adoption of cyber security technology is a natural extension of their duties.

Aiding these efforts is the fact that firms in countries with policy legacies of economic guidance are used to government involvement. This does not mean they will see eye-to-eye with the government on everything, but they are more likely to negotiate and work with the government rather than to reflexively oppose government action. Moreover, the existing institutions for coordinating on economic issues can easily be adapted to cyber security.

Thus, we see that in Japan and South Korea, which have these institutions, there is strong promotion of cyber security within the private sector. By contrast, in the U.S., which does not, there are not government actors who clearly see this as part of their responsibilities; moreover, it is clear that U.S. firms would prefer the government leave cyber security to them.

This does not tell the entire story, however. Even in the absence of a strong national security institutions, there is still an economic case to be made for promoting the cyber security sector. Japan's lack of interest in promoting the sector is not solely due to a legacy of restrained traditional security capabilities, but also because its government does not buy this case. Its earlier experience trying to promote the Japanese software sector has made the government skeptical that sector promotion efforts would be successful. What is more, there is a trade-off between promoting indigenous cyber security and promoting the adoption of cyber security technology: increasing demand for indigenous products requires reducing other firms' cyber security, at the least in the short-term and potentially longer. Given these factors, the Japanese government has decided to focus its efforts elsewhere; even its cyber security research-and-development is aimed at improving the cyber security of products and services from other sectors rather than the cyber security sector itself.

Also, while for the most part the U.S. does not follow Japan and South Korea in promoting cyber security in the private sector, there is one clear exception: critical infrastructure. Though arguably its efforts are not as strong as the other two countries, here all three governments do make efforts to coordinate with firms and to encourage them to improve their cyber security. Critical infrastructure is a case where the threat—to national security, to the economy, to public safety—is so clear that governments understand that they must take action, and cannot simply leave cyber security to the firms themselves.

In summation, whether and to what degree a government makes efforts to promote the cyber security sector or to promote the adoption of cyber security technology relies largely on whether it has a policy legacy of maintaining strong traditional security capabilities and whether it has a legacy of economic guidance. However, in circumstances where there is a possible but not clear-cut case to be made for a policy decision, experience can play a role as well.

5.2 Implications and Future Work

The most likely path for Japan's cyber security technology promotion efforts are that it continues on much as now. Cyber security plays a key role in the Japanese government's economic plans, but primarily as a feature of other Japanese products and services, rather than as products and services themselves. METI in particular believes that other technologies, such as IoT devices and self-driving automobiles, are technologies in which Japan is likely to be competitive. Research and development funds spent on cyber security will continue to be mainly devoted to projects that improve the cyber security of these other technologies.

What might cause Japan to promote the cyber security sector more strongly? Given the findings of this dissertation, there are at least two ways this could happen: MOD could be strengthened, or METI and MIC could have cause to reconsider the economic argument for sector promotion.

One way in which MOD could be strengthened would be through the overturning of or substantial altering of Article 9 to allow Japan to maintain offensive military capabilities, and the transformation of the JSDF into a traditional military force. A Japanese military would be able to play a major role in responding to cyber attacks where the JSDF cannot. This would also clearly allow Japan's national security institutions to undertake offensive cyber security measures, which would increase the usefulness of an indigenous cyber security sector.[1] Given this and the resulting strengthened influence of MOD over cyber security policy, we should expect that sector promotion would become a central part of Japanese cyber security policy. Moreover, whatever their skepticism, METI and MIC would likely increase their own promotion efforts in order to maintain their influence over this sector versus MOD.

However, the overturning of Article 9 is not a very likely scenario in the near future. Though still not particularly likely, a more likely scenario would be an increase in defense spending. Though defense spending has been kept to 1% of GDP or below, there is no legal reason spending could not be higher. Unlike the overturning of Article 9, this would not dramatically empower the MOD, since it would still only be able to play a limited role in responding to cyber security attacks. We thus would not expect to see a dramatic shift in promotion policies. However, greater funding would increase the ability of MOD to use procurement, contracting, and other instruments to provide support for the sector. Given that the political position of MOD would not have fundamentally changed, however, we should not expect to see the dramatic shift in policy we would see if Article 9 were overturned. METI and MIC would be likely to continue on much as now, leaving any promotion efforts to MOD. Nevertheless, this would lead to stronger sector promotion relative to the present.

The third scenario by which MOD could be strengthened, at least in terms of its influence over cyber security policy, would not involve a domestic change but rather an international one: a key existing threat to Japan could be reduced or removed, freeing up MOD resources for cyber security. Resolution of its territorial dispute with China, or an international agreement that reduced tensions with North Korea, might allow MOD to spend less resources on traditional weapons systems and more on cyber security. It should be noted that because cyber attacks generally do not rise to the level of a military attack, an increase in cyber attacks or the cyber threat in and of itself is unlikely to lead to an increase in MOD's spending on the issue, given its other priorities.

The other possible route through which Japan could change its policy on sector promotion is by METI and MIC reevaluating the economic case for the promotion of cyber security.

[1]The Abe administration is already considering giving the JSDF offensive capabilities, but constitutionally it is unclear to what degree they can actually use these capabilities. See Matsubara, *How Japan's Pacifist Constitution Shapes Its Approach to Cyberspace* for a good discussion of the challenges Article 9 poses for Japan's cyber security.

One way this could happen would be for domestic cyber security firms to successfully build products and services that provide similar levels of cyber security to foreign products and services. This would reduce or remove entirely the trade-off between supporting indigenous cyber technology and promoting strong cyber security. Promotion, however, would still be useful, not to turn a weak cyber security sector into a strong one, but instead to maintain and promote the competitiveness of the indigenous cyber security sector. Thus, we might very well see sector promotion follow success, rather than lead to it.

Another possibility is that the government could find success in promoting another technology, such as artificial intelligence, that creates "lessons learned" which METI and MIC believe can be successfully applied to the cyber security sector as well. In much the same way that failing to promote the software sector has made these actors skeptical of their ability to promote the cyber security sector, success in promoting a similar technology would give METI and MIC good reason to reconsider.

Though it is the least likely scenario, an event that led METI and MIC to reconsider the costs or risks of relying on foreign cyber security technology could also lead to increased sector promotion. This is unlikely because the potential costs or risks of relying on foreign cyber security technology are fairly well known, but it is not entirely impossible. For example, if other countries (particularly the U.S.) began to consider putting strong export restrictions on cyber security technology, METI and MIC would have reason to worry that without an indigenous cyber security sector, Japanese firms would not be able to acquire necessary cyber security technologies.

Major shifts in Japan's policy toward promoting the adoption of cyber security technology are less likely than shifts in policy toward sector promotion, particularly because the government is relatively active in this area. Certainly it is hard to imagine the government becoming *less* involved: given the growing importance of cyber security, there is every reason to believe that for MIC and especially for METI involvement in the promotion of cyber security will continue to be a good way to justify their own importance. The most likely scenario is that the government will continue to innovate around the current basic strategy, by finding new ways to encourage information sharing, for example, or creating new programs similar to the Cyber Clean Center.

A clear failure of the current strategy is one potential source of change. Much as the clear failure of its software promotion efforts led METI to reconsider its promotion strategy, some event that demonstrated that the current approach was not sufficient should lead the government to shift that approach, though in this case the most likely outcome would be to strengthen efforts or to use more coercive measures such as regulations, rather than to abandon the attempt. Repeated leaks of personal information by firms, for example, might lead to a rethinking of this approach.

A shift in strategy would also occur should METI and MIC lose influence over cyber security policy. The current strategy, including the reliance on voluntary measures, primarily reflect the interests of these two actors. If they were somehow to be removed from the policy-making process, regulations would become much more likely, for two reasons: one, MOD and NPA do not share METI and MIC's opposition to regulations; and two, because

METI and MIC bring with them networks and tools for informal pressure that would be lost, making other tools such as regulations more appealing. The fact that Japanese firms want clear cyber security regulations would make this outcome even more likely. Perhaps ironically, however, the regulations the NPA would most like to see passed—a requirement for ISPs to store meta-data—would still be difficult to pass, given that MIC would continue to have responsibility for the ISPs. It should be noted, however, that precisely because METI and MIC have jurisdictional responsibility over related sectors, and because most of the instruments for promotion of the adoption of cyber security technology are under their control or the control of related agencies such as IPA and NICT, it is extremely unlikely that they would be dislodged from cyber security policy-making.

Turning to Japanese security policy more broadly, while recent observations that Japan has been taking steps to strengthen its security apparatus cannot be denied[2], these findings suggest that earlier observations that Japan tends to view national security through an economic lens are not yet obsolete.[3] Japanese cyber security policy is motivated primarily by economic concerns—both potential risks and potential opportunities—rather than by traditional security concerns. Japan may be enhancing its ability to act within the traditional security sphere, but we have not yet seen a sea change in its security priorities.

Moving beyond Japan, though states with strong national security institutions do more to promote the cyber security sector, there are reasons to expect that in the long run, states without strong national security institutions could provide their firms with a competitive advantage in assuring their customers of the cyber security of their products and services. States with strong national security institutions have government actors that have incentives to weaken the cyber security of products and services—either openly, such as would be the case if cryptography algorithms were required to produce a key for use by the FBI, or covertly, such as with NSA operations. By contrast, governments of states without strong national security institutions have little reason to undermine the cyber security of the products and services of their firms. There are good reasons, then, for consumers to trust products and services from countries with weak national security institutions over strong ones.

In terms of developing and implementing cyber security policies, whether there are bureaucratic organizations with clear responsibility for a particular aspect of cyber security policy makes a great deal of difference as to the effort put into implementation. For example, while both the Department of Homeland Security in the U.S. and the Information-technology Promotion Agency in Japan have the responsibility of educating the public about good cyber security practices, for DHS this is a small part of its many responsibilities, whereas for the IPA this is a core part of its mission. It is no surprise, then, that the IPA makes far more

[2]For a good overview of recent changes, see Oros, *Japan's Security Renaissance*; for earlier movements in this direction, see Michael Green, *Japan's Reluctant Realism: Foreign Policy Challenges in an Era of Uncertain Power* (Palgrave Macmillan, September 2003); Richard J. Samuels, *Securing Japan: Tokyo's Grand Strategy and the Future of East Asia* (Cornell University Press, 2007).

[3]Peter J. Katzenstein and Nobuo Okawara, "Japan's National Security: Structures, Norms, and Policies," *International Security* 17, no. 4 (1993): 84–118; Eric Heginbotham and Richard J. Samuels, "Mercantile Realism and Japanese Foreign Policy," *International Security* 22, no. 4 (1998): 171–203.

efforts in this regard, inventing creative ways to educate the public while the DHS takes mostly perfunctory actions in this regard. That agency enthusiasm matters for policy implementation is hardly a new observation.[4] But this research does highlight that while two states may have the same policy on paper, a state with an agency that sees that policy as a core part of its mission will see that policy implemented more enthusiastically and creatively. Governments should carefully consider agency design and assigning of responsibilities as part of their cyber security policy-making.

Further work is needed to understand how governments design cyber security implementation. Both South Korea and Japan pursue strong policies for the promotion of the adoption of cyber security technology, for example, but South Korea relies far more heavily on regulations, while Japan prefers to rely on voluntary measures and informal pressure. Questions of convergence and divergence are particularly important: are certain implementations determined by the nature of the problem, versus institutions? Do we see patterns where implementation is the same at the intermediate level, but differs in the details—for example, do all governments encourage information sharing as a way of improving private sector cyber security, but use different instruments to do so? What explains these patterns? Having a clearer understanding of what institutional factors drive particular implementation is important both for a clearer understanding of comparative cyber security policy, and for designing policy recommendations that take institutional differences into account.

Though for analytic purposes in this dissertation I treat the policy-making system of each state as independent from the other, in fact there is quite a bit of interaction between these systems, particularly via international communities of cyber security experts. These communities work together to develop international standards and guidelines. Moreover, governments learn not only from their own experiences, but from those of other governments. A promising area for future work is to study the diffusion of cyber security policies across countries, drawing on the existing literature on diffusion.[5].

Turning to sector promotion more broadly, many researchers have observed that even if a government wants to use sector promotion to strengthen its economy, there is no clear way for a government to know which sectors to promote. They often rely on heuristics, such

[4]See, for example, Paul Sabatier and Daniel Mazmanian, "The Conditions of Effective Implementation: A Guide to Accomplishing Policy Objectives," *Policy Analysis* 5, no. 4 (1979): 481–504.

[5]Some of the work in this area includes Jacqui True and Michael Mintrom, "Transnational Networks and Policy Diffusion: The Case of Gender Mainstreaming," *International Studies Quarterly* 45, no. 1 (2001): 27–57; Beth A. Simmons and Zachary Elkins, "The Globalization of Liberalization: Policy Diffusion in the International Political Economy," *American Political Science Review* 98, no. 1 (February 2004): 171–189; Sarah M. Brooks, "Interdependent and Domestic Foundations of Policy Change: The Diffusion of Pension Privatization around the World," *International Studies Quarterly* 49, no. 2 (2005): 273–294; Frank Dobbin, Beth Simmons, and Geoffrey Garrett, "The Global Diffusion of Public Policies: Social Construction, Coercion, Competition, or Learning?," *Annual Review of Sociology* 33, no. 1 (August 2007): 449–472; Craig Volden, Michael M. Ting, and Daniel P. Carpenter, "A Formal Model of Learning and Policy Diffusion," *American Political Science Review* 102, no. 3 (August 2008): 319–332; Fabrizio Gilardi, "Who Learns from What in Policy Diffusion Processes?," *American Journal of Political Science* 54, no. 3 (2010): 650–666.

as focusing on "high technology" sectors.[6] Here we see that the Japanese government has considered two other factors in making its decision not to promote cyber security. First, it has considered the probability of success: the government (in particular METI and MIC) has decided that efforts to promote cyber security are likely to fail. This determination is heavily based on its experience in trying to promote a similar sector, in this case software. Second, it has considered the trade-offs between promoting cyber security and other sectors. It both believes that Japan is more likely to be successful in other sectors, and that it should spend its limited resources there. Moreover, in some of these sectors (such as self-driving cars and IoT devices), strengthening cyber security through proper adoption of state-of-the-art cyber security technology is more important than competing in the cyber security sector itself. This suggests two broader lessons: that governments consider the prospect of success when deciding to promote a particular sector, and this consideration is based in part on experience in promoting similar sectors; and that governments do not look at promoting sectors in isolation, but take the interactions and trade-offs between multiple sectors in making their decisions. Exactly how these factor into government decisions is an area for future research.

While for the most part this dissertation emphasizes the divergence of state behavior, it does find that in the case of critical infrastructure, states behave more closely to the way threat-based explanations would expect. An area of future work is to better understand if particular types of threats lead to convergence—whether there are certain potential threats that are so clear that governments form some response regardless of the nature of their domestic institutions. One possible explanation is that it is the breadth of the potential threat that matters. Cyber attacks on critical infrastructure pose threats to the military, to the economy, and to public safety. Regardless of the way in which policy-makers conceive of "security", cyber attacks on critical infrastructure are almost certain to pose a threat to it. Looking at a variety of potential threats, both within cyber security and more broadly, would lead to a better understanding of this outcome.

As our reliance on information and communications technology continues to grow, cyber security will only become a bigger issue, in Japan and elsewhere. Though from a technical perspective the challenges posed to cyber security are similar across countries, policy responses vary considerably. Given that both the production and consumption of cyber security technology are important for strengthening cyber security, advocates for stronger cyber security have good reason to encourage governments to adopt policies that will encourage both. But advocates need to be flexible both with the framing of their arguments and with the specifics of their policy recommendations. While national security arguments are convincing to some governments, economic arguments will make a stronger case to others. Policy proposals that most resemble current policies and that use existing sets of instruments are more likely to meet with support and be adopted than those that are not. Taking domestic political and economic institutions into account is key to crafting cyber security policies that will succeed.

[6] Warwick, *Beyond Industrial Policy*, 23; Komiya, "Introduction," 8; Pekkanen, *Picking Winners?*, 7–8.

Bibliography

Aggarwal, Sonia, and Vinod K. Aggarwal. *The Political Economy of Industrial Policy*, September 2016.

Aggarwal, Vinod K., and Andrew Reddie. "Comparative Industrial Policy and Cybersecurity: A Framework for Analysis." 2018.

———. "Iterative Industrial Policy: How the United States Pursues Cybersecurity." 2018.

Allen, Thelma A. *FIPS General Information*, February 2010. Accessed June 24, 2018. `https://www.nist.gov/itl/fips-general-information`.

———. *NIST Special Publication 1800-series General Information*, May 2018. Accessed June 24, 2018. `https://www.nist.gov/itl/nist-special-publication-1800-series-general-information`.

———. *NIST Special Publication 800-series General Information*, May 2018. Accessed June 24, 2018. `https://www.nist.gov/itl/nist-special-publication-800-series-general-information`.

Amenta, Edwin, and Kelly M. Ramsey. "Institutional Theory." In *The Handbook of Politics: State and Civil Society in Global Perspective*, edited by Kevin T. Leicht and J. Craig Jenkins, 15–39. New York: Spring, 2010.

Anchordoguy, Marie. *Reprogramming Japan: The High Tech Crisis Under Communitarian Capitalism*. Cornell University Press, 2005.

Arimura, Kouichi. *Anti-Bot Countermeasures in Japan*, March 2008. Accessed October 17, 2017. `http://www.nca.gr.jp/jws2008/WS1-ccc.pdf`.

Bitzinger, Richard A. "Reforming China's defense industry." *Journal of Strategic Studies* 39, nos. 5-6 (September 2016): 762–789.

Block, Fred. "Innovation and the Invisible Hand of Government." In *State of Innovation: The U.S. Government's Role in Technology Development*, edited by Fred Block and Matthew R. Keller, 1–30. Boulder, CO: Paradigm Publishers, 2011.

Brander, James A., and Barbara J. Spencer. "Export subsidies and international market share rivalry." *Journal of International Economics* 18, no. 1 (February 1985): 83–100.

Brooks, Sarah M. "Interdependent and Domestic Foundations of Policy Change: The Diffusion of Pension Privatization around the World." *International Studies Quarterly* 49, no. 2 (2005): 273–294.

Cabinet Secretariat of Japan. 内閣官房組織令（抄）*[Order for the Organization of the Cabinet Secretariat (Excerpt)]* [in Japanese]. Accessed March 23, 2017. `http://www.nisc.go.jp/law/pdf/soshikirei.pdf`.

Campbell, John L. "Institutional Analysis and the Role of Ideas in Political Economy." *Theory and Society* 27, no. 3 (1998): 377–409.

Carr, Madeline. "Public–private partnerships in national cyber-security strategies." *International Affairs* 92, no. 1 (January 2016): 43–62.

US-CERT. *About Us | US-CERT*. Accessed July 31, 2018. `https://www.us-cert.gov/about-us`.

———. *National Cybersecurity and Communications Integration Center | US-CERT*. Accessed July 31, 2018. `https://www.us-cert.gov/nccic`.

Chiang, Jong-Tsong. "From 'mission-oriented' to 'diffusion-oriented' paradigm: the new trend of U.S. industrial technology policy." *Technovation* 11, no. 6 (September 1991): 339–356.

Crafts, Nicholas. "Overview and Policy Implications." In *Learning From Some of Britain's Successful Sectors: An Historical Analysis of the Role of Government*, 1–17. BIS Economics Paper 6. March 2010.

Cyber Security Strategic Headquarters. *The Cybersecurity Policy for Critical Infrastructure Protection (4th Edition)*, April 2017. Accessed May 19, 2018. `http://www.nisc.go.jp/eng/pdf/cs_policy_cip_eng_v4.pdf`.

———. サイバーセキュリティ戦略本部　第 *1* 回会合　議事概要 *[Cyber Security Strategic Headquarters, First Meeting, Summary of Proceedings]* [in Japanese], February 2015. Accessed March 24, 2017. `http://www.nisc.go.jp/conference/cs/dai01/pdf/01gijigaiyou.pdf`.

———. サイバーセキュリティ研究開発戦略 *[Cybersecurity Research and Development Strategy]* [in Japanese], July 2017. Accessed February 15, 2018. `https://www.nisc.go.jp/active/kihon/pdf/kenkyu2017.pdf`.

Department of Homeland Security. *National Cybersecurity & Communications Integration Center*, May 2011. Accessed June 24, 2018. `https://www.dhs.gov/national-cybersecurity-and-communications-integration-center`.

———. *Stop.Think.Connect. | Homeland Security*. Accessed June 23, 2018. `https://www.dhs.gov/stopthinkconnect`.

Department of Homeland Security. *Stop.Think.Connect. National Network*, August 2012. Accessed July 31, 2018. https://www.dhs.gov/stopthinkconnect-national-network.

Desiderio, Andrew, and Kevin Poulsen. "Exclusive: U.S. Government Can't Get Controversial Kaspersky Lab Software Off Its Networks." *The Daily Beast*, May 2018. Accessed July 18, 2018. https://www.thedailybeast.com/exclusive-us-government-cant-get-controversial-kaspersky-lab-software-off-its-networks.

Devore, Marc R. "Arms Production in the Global Village: Options for Adapting to Defense-Industrial Globalization." *Security Studies* 22, no. 3 (July 2013): 532–572.

Dobbin, Frank, Beth Simmons, and Geoffrey Garrett. "The Global Diffusion of Public Policies: Social Construction, Coercion, Competition, or Learning?" *Annual Review of Sociology* 33, no. 1 (August 2007): 449–472.

"More Personal Information Leaks Found." *Dong-A Ilbo Daily*, April 2006. Accessed June 19, 2018. http://global.factiva.com/redir/default.aspx?P=sa&an=DONGAI00200604 05e24600009&cat=a&ep=ASE.

Dunn Cavelty, Myriam. *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*. Routledge, November 2007.

Dyson, Tom. "Convergence and Divergence in Post-Cold War British, French, and German Military Reforms: Between International Structure and Executive Autonomy." *Security Studies* 17, no. 4 (December 2008): 725–774.

Editorial Staff. *The artificial intelligence race heats up*, March 2018. Accessed July 24, 2018. https://www.japantimes.co.jp/opinion/2018/03/01/editorials/artificial-intelligence-race-heats/.

Edler, J., L. Georghiou, K. Blind, and E. Uyarra. "Evaluating the demand side: New challenges for evaluation." *Research Evaluation* 21, no. 1 (March 2012): 33–47.

Elder, Mark. "Chapter 7. METI and Industrial Policy in Japan: Change and Continuity." *Japanese Economy* 28, no. 6 (November 2000): 3–34. https://www.tandfonline.com/doi/abs/10.2753/JES1097-203X28063.

Elman, Colin. "Horses for courses: Why nor neorealist theories of foreign policy?" *Security Studies* 6, no. 1 (September 1996): 7–53.

Evans, Peter B. *Embedded Autonomy: States and Industrial Transformation*. Princeton University Press, March 1995.

Fischer, Eric A. *Federal Laws Relating to Cybersecurity: Overview of Major Issues, Current Laws, and Proposed Legislation*, December 2014.

Franceschi-Bicchierai, Lorenzo. *Who's Afraid of Kaspersky?*, May 2018. Accessed July 18, 2018. https://motherboard.vice.com/en_us/article/wjbda5/kaspersky-sas-conference-russia-spying.

Friedman, Allan. *Economic and Policy Frameworks for Cybersecurity Risks*, July 2011. Accessed June 22, 2018. https://www.brookings.edu/wp-content/uploads/2016/06/0721_cybersecurity_friedman.pdf.

Gady, Franz-Stefan. "Japan's Defense Ministry Plans to Boost Number of Cyber Warriors." *The Diplomat*, July 2017. Accessed August 2, 2018. https://thediplomat.com/2017/07/japans-defense-ministry-plans-to-boost-number-of-cyber-warriors/.

Gallagher, Ryan. *The Untold Story of Japan's Secret Spy Agency*, May 2018. Accessed August 2, 2018. https://theintercept.com/2018/05/19/japan-dfs-surveillance-agency/.

Gartner. *Gartner Forecasts Worldwide Security Spending Will Reach $96 Billion in 2018, Up 8 Percent from 2017*, December 2017. Accessed July 18, 2018. https://www.gartner.com/newsroom/id/3836563.

Ge, C., and K. W. Huang. "Analyzing the Economies of Scale of Software as a Service Software Firms: A Stochastic Frontier Approach." *IEEE Transactions on Engineering Management* 61, no. 4 (November 2014): 610–622.

Gilardi, Fabrizio. "Who Learns from What in Policy Diffusion Processes?" *American Journal of Political Science* 54, no. 3 (2010): 650–666.

Goldstein, Judith. "The Political Economy of Trade: Institutions of Protection." *The American Political Science Review* 80, no. 1 (1986): 161–184.

Gourevitch, Peter Alexis. "Breaking with Orthodoxy: The Politics of Economic Policy Responses to the Depression of the 1930s." *International Organization* 38, no. 1 (1984): 95–129.

Government of Japan. サイバーセキュリティ戦略 *[Cybersecurity Strategy]* [in Japanese], September 2015. Accessed July 17, 2017. http://www.nisc.go.jp/active/kihon/pdf/cs-senryaku-c.pdf.

———. 情報処理の促進に関する法律,（略）情報処理促進法 *[Law Concerning the Promotion of Data Processing]* [in Japanese]. Last revised in 2008, 1970. Accessed November 22, 2017. http://www.houko.com/00/01/S45/090.HTM.

Government of the Republic of Korea. *Act on the Promotion of Information Security Industry*. Last amended July 2017, June 2015.

Green, Michael. *Japan's Reluctant Realism: Foreign Policy Challenges in an Era of Uncertain Power*. Palgrave Macmillan, September 2003.

Hall, Peter A., and David Soskice. "Introduction." In *Varieties of Capitalism: The Institutional Foundations of Comparative Advantage*, edited by Peter A. Hall and David Soskice, 1–68. New York: Oxford University Press, Inc., 2001.

Hall, Peter A., and Rosemary C. R. Taylor. "Political Science and the Three New Institutionalisms." *Political Studies* 44, no. 5 (December 1996): 936–957.

Harris, Robert G., and James M. Carman. "Public Regulation of Marketing Activity: Part I: Institutional Typologies of Market Failure." *Journal of Macromarketing* 3, no. 1 (June 1983): 49–58.

Hauge, Janice A, and James E. Prieger. "Demand-Side Programs to Stimulate Adoption of Broadband: What Works?" *Review of Network Economics* 9, no. 3 (January 2010).

Heginbotham, Eric. "The Fall and Rise of Navies in East Asia: Military Organizations, Domestic Politics, and Grand Strategy." *International Security* 27, no. 2 (October 2002): 86–125.

Heginbotham, Eric, and Richard J. Samuels. "Mercantile Realism and Japanese Foreign Policy." *International Security* 22, no. 4 (1998): 171–203.

Ho, Soyoung. *Haven for Hackers*, October 2009. Accessed April 19, 2018. `https://foreignpolicy.com/2009/10/26/haven-for-hackers/`.

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

Ikenberry, G. John. "The Irony of State Strength: Comparative Responses to the Oil Shocks in the 1970s." *International Organization* 40, no. 1 (1986): 105–137.

Information Security Policy Council. *Action Plan on Information Security Measures for Critical Infrastructures*, December 2005. Accessed May 19, 2018. `http://www.nisc.go.jp/eng/pdf/actionplan_ci_eng.pdf`.

———. *Cybersecurity Strategy*, June 2013. Accessed May 14, 2018. `https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Japan%20Cybersecurity%20Strategy%202013.pdf`.

———. *The Basic Policy of Critical Information Infrastructure Protection (3rd Edition)*, May 2014. `http://www.nisc.go.jp/eng/pdf/actionplan_ci_eng_v3.pdf`.

———. *The First National Strategy on Information Security*, February 2006. Accessed May 14, 2018. `https://www.nisc.go.jp/eng/pdf/national_strategy_001_eng.pdf`.

———. *The Second National Strategy on Information Security*, February 2009. Accessed May 14, 2018. `https://www.nisc.go.jp/eng/pdf/national_strategy_002_eng.pdf`.

Information Security Policy Council. 新・情報セキュリティ普及啓発プログラム *[New Information Security Public Awareness Program]* [in Japanese], July 2014. Accessed February 14, 2018. http://www.nisc.go.jp/active/kihon/pdf/awareness2014.pdf.

Information-technology Promotion Agency. *2010 Smart Home Appliance Security Study Report*, January 2011. Accessed June 22, 2018. https://www.ipa.go.jp/files/000014115.pdf.

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

———. *IPA Information-technology Promotion Agency, Japan : IPA/ISEC : Measures for Information Security Vulnerabilities*, 2018. Accessed June 22, 2018. https://www.ipa.go.jp/security/english/third.html#emb.

———. *IPA Information-technology Promotion Agency, Japan : IPA/ISEC : Vulnerabilities : "MyJVN Security Configuration Checker" released*, December 2009. Accessed June 22, 2018. https://www.ipa.go.jp/security/english/vuln/200912_myjvn_cc_en.html.

———. *JVN iPedia - Vulnerability Countermeasure Information Database / What is JVN iPedia?* Accessed June 22, 2018. https://jvndb.jvn.jp/en/nav/jvndb.html.

———. *JVN iPedia - Vulnerability Countermeasure Information Database / What is JVN iPedia?* Accessed June 22, 2018. https://jvndb.jvn.jp/en/nav/jvndb.html.

———. *MyJVN - MyJVN バージョンチェッカ [MyJVN Version Checker]* [in Japanese], 2018. Accessed June 22, 2018. https://jvndb.jvn.jp/apis/myjvn/vccheck.html.

———. *Outline of Information Security Benchmark (ISM-Benchmark)*, 2007. https://www.ipa.go.jp/files/000011798.pdf.

Johnson, Chalmers. *MITI and the Japanese Miracle: The Growth of Industrial Policy : 1925-1975*. Stanford University Press, 1982.

"Incentives to be given for information security." *Joins.com*, August 2014. Accessed June 21, 2018. http://global.factiva.com/redir/default.aspx?P=sa&an=JOONAI00201407 31ea8100018&cat=a&ep=ASE.

Jones, Bryan D. "Bounded Rationality and Political Science: Lessons from Public Administration and Public Policy." *Journal of Public Administration Research and Theory* 13, no. 4 (October 2003): 395–412.

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

JPCERT/CC. *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 [JPCERT Coordination Center, About JPCERT/CC: The Various Activities of JPCERT/CC]* [in Japanese]. Accessed April 16, 2017. `http://www.jpcert.or.jp/about/05.html`.

———. *JPCERT コーディネーションセンターインシデント対応とは？[JPCERT Coordination Center: What is Incident Response?]* [In Japanese]. Accessed February 20, 2018. `https://www.jpcert.or.jp/ir/`.

JPCERT/CC and Information-technology Promotion Agency. *Japan Vulnerability Notes / What is JVN?* Accessed June 22, 2018. `http://jvn.jp/en/nav/jvn.html`.

Judgment concerning the constitutionality of Kyoto City Ordinance No. 10 of 1954 on Assembly, Marching, and Demonstration, December 1969.

Jun, Ji-hye. "Parties at odds over cyber security agency." *The Korea Times; Seoul* (Seoul, South Korea, Seoul), March 2013.

Jung, Seung-hyun. "Seoul gets tough with cyber security." *Joins.com*, August 2011. Accessed June 19, 2018. `http://global.factiva.com/redir/default.aspx?P=sa&an=JOONAI0020110809e7890000m&cat=a&ep=ASE`.

Kapstein, Ethan Barnaby. "International Collaboration in Armaments Production: A Second-Best Solution." *Political Science Quarterly* 106, no. 4 (1991): 657–675.

Karakaya, Fahri, and Michael J. Stahl. "Barriers to Entry and Market Entry Decisions in Consumer and Industrial Goods Markets." *Journal of Marketing* 53, no. 2 (1989): 80–91.

Katzenstein, Peter J. "Same War: Different Views: Germany, Japan, and Counterterrorism." *International Organization* 57, no. 4 (2003): 731–760.

Katzenstein, Peter J., and Nobuo Okawara. "Japan's National Security: Structures, Norms, and Policies." *International Security* 17, no. 4 (1993): 84–118.

Kawabata, E. "Dual Governance: The Contemporary Politics of Posts and Telecommunications in Japan." *Social Science Japan Journal* 7, no. 1 (April 2004): 21–39.

Keller, Matthew R. "The CIA's Pioneering Role in Public Venture Capital Initiatives." In *State of Innovation: The U.S. Government's Role in Technology Development*, edited by Fred Block and Matthew R. Keller, 109–132. Boulder, CO: Paradigm Publishers, 2011.

Keohane, Robert Owen. *Neorealism and Its Critics*. Columbia University Press, 1986.

Kim, Hee-seop. "Internet Leakage of Personal Details Reaching Epic Proportions: KISA." *Chosun Ilbo*, December 2004. Accessed June 19, 2018. `http://global.factiva.com/redir/default.aspx?P=sa&an=DIGCHO0020041223e0cn0000k&cat=a&ep=ASE`.

Kim, Hongbum, Dong-Hee Shin, and Daeho Lee. "A socio-technical analysis of software policy in Korea: Towards a central role for building ICT ecosystems." *Telecommunications Policy* 39, no. 11 (December 2015): 944–956.

Kim, Jong-chan. "S. Korea to spend $8.1 billion on ICT R&D for 5 years." *AJU NEWS*, October 2013. Accessed June 21, 2018. http://global.factiva.com/redir/default.aspx?P=sa&an=AJUENG0020131023e9an0005l&cat=a&ep=ASE.

Kim, Sam. "South Korea enlists cyber warriors to battle Kim Jong-un's regime." *Independent Online*, November 2015. Accessed June 21, 2018. http://global.factiva.com/redir/default.aspx?P=sa&an=INDOP00020151128ebbs004h6&cat=a&ep=ASE.

Kim, Sangbae. ""Hardware" Institutions for "Software" Technologies: The Japanese Model of Industrial Development in the Personal Computer Industry." *Journal of International and Area Studies* 9, no. 1 (2002): 17–36.

Kim, In-soon. "Foreign security companies set out to target public market, eyeing the home ground of native companies." *The Electronic Times*, April 2014. Accessed June 21, 2018. http://global.factiva.com/redir/default.aspx?P=sa&an=ETK0000020140424ea4o00001&cat=a&ep=ASE.

Kim, Tong-hyung. "Calls for Independent Privacy Agency Grow." *Korea Times*, April 2010. Accessed June 19, 2018. http://global.factiva.com/redir/default.aspx?P=sa&an=KORTIM0020100422e64l0000h&cat=a&ep=ASE.

Komiya, Ryutaro. "Introduction." In *Industrial Policy of Japan*, edited by Ryutaro Komiya, Masahiro Okuno, and Kotaro Suzumura, 1–22. San Diego, CA: Academic Press, 1988.

Kopp, Emanuel, Lincoln Kaffenberger, and Christopher Wilson. *Cyber Risk, Market Failures, and Financial Stability*. IMF Working Paper WP/17/185. International Monetary Fund, 2017. Accessed May 26, 2018. http://elibrary.imf.org/view/IMF001/24475-9781484313787/24475-9781484313787/24475-9781484313787.xml.

Korea Internet and Security Agency. *2017 Korea Internet White Paper*, 2017.

———. *Information Security in Korea*, 2015. Accessed April 23, 2018. https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/KISA_Information_Security_in_KOREA.pdf.

———. *Laws on the Internet and Information Security of Korea*, 2016.

Krebs, Brian. *Talking Bots with Japan's 'Cyber Clean Center' —Krebs on Security*, March 2010. Accessed October 16, 2017. https://krebsonsecurity.com/2010/03/talking-bots-with-japans-cyber-clean-center/.

Kriz, Danielle, and Mihoko Matsubara. *Japanese Government Updates Cybersecurity Guidelines: Increased Focus on Cybersecurity Investments and SMBs*, December 2016. Accessed February 22, 2017. http://researchcenter.paloaltonetworks.com/2016/12/gov-japanese-government-updates-cybersecurity-guidelines-increased-focus-cybersecurity-investments-smbs/.

Kshetri, Nir. "Cybersecurity in South Korea." In *The Quest to Cyber Superiority*, 171–182. Springer, Cham, 2016.

Lau, Lynette. *Cybercrime 'pandemic' may have cost the world $600 billion last year*, February 2018. Accessed August 8, 2018. https://www.cnbc.com/2018/02/22/cybercrime-pandemic-may-have-cost-the-world-600-billion-last-year.html.

Lechevalier, Sébastien. *The Great Transformation of Japanese Capitalism*. Translated by J.A.A. Stockwin. Nissan Institute/Routledge Japanese Studies Series. New York, NY: Routledge, 2014.

Ledyard, John O. *Market Failure*. Edited by Steven N. Durlauf and Lawrence E. Blume. London, 2008.

Lee, Jooha. "Politics of Policy-Making in Korea and Japan." University of Tokyo, Tokyo, Japan, October 2007. Accessed August 1, 2018. http://www.welfareasia.org/4thconference/papers/Lee_Politics%20of%20Policy-Making%20in%20Korea%20and%20Japan.pdf.

Lin, Justin, and Ha-Joon Chang. "Should Industrial Policy in Developing Countries Conform to Comparative Advantage or Defy it? A Debate Between Justin Lin and Ha-Joon Chang." *Development Policy Review* 27, no. 5 (2009): 483–502.

Mansfield, Nick. *Development of Policies for Protection of Critical Information Infrastructures*. Ministerial Background Report DSTI/ICCP/REG(2007)20/FINAL. OECD, 2007. Accessed July 25, 2018. http://www.oecd.org/sti/40761118.pdf.

March, James G. *A Primer on Decision-Making*. New York: Free Press, 1994.

———. "Bounded Rationality, Ambiguity, and the Engineering of Choice." *The Bell Journal of Economics* 9, no. 2 (1978): 587–608.

Masuoka, Ryusuke, and Tsutomu Ishino. *Cyber Security in Japan (v.2)*. Technical report. Center for International Public Policy Studies, December 2012. Accessed November 20, 2016. http://www.cipps.org/group/cyber_memo/003_121204.pdf.

Matsubara, Mihoko. *Assessing Japan's Internet of Things (IoT) Security Strategy for Tokyo 2020*, September 2016. Accessed February 22, 2017. http://researchcenter.paloaltonetworks.com/2016/09/cso-assessing-japans-internet-of-things-iot-security-strategy-for-tokyo-2020/.

Matsubara, Mihoko. *How Japan's Pacifist Constitution Shapes Its Approach to Cyberspace*, May 2018. Accessed July 15, 2018. https://www.cfr.org/blog/how-japans-pacifist-constitution-shapes-its-approach-cyberspace.

Matsubara, Mihoko, and Danielle Kriz. *Japan's Cybersecurity Guidelines for Business Leadership*, May 2016. Accessed November 15, 2016. http://researchcenter.paloaltonetworks.com/2016/05/japans-cybersecurity-guidelines-for-business-leadership-changing-the-japanese-business-mindset-and-potentially-raising-the-global-bar/.

Mazzucato, Mariana, and Caetano CR Penna. "Beyond Market Failures: The Market Creating and Shaping Roles of State Investment Banks." *SSRN Electronic Journal*, 2015. Accessed March 15, 2018. http://www.ssrn.com/abstract=2559873.

McCurry, Justin. "South Korea spy agency admits trying to rig 2012 presidential election." *The Guardian*, August 2017. Accessed June 30, 2018.

Ministry of Defense. "Establishment of the Cyber Defense Unit." *Japan Defense Focus*, no. 52 (May 2014). Accessed April 16, 2017. http://www.mod.go.jp/e/jdf/sp/no52/sp_activities.html#article03.

———. *Strategy on Defense Production and Technological Bases: Toward strengthening the bases to support defense forces and 'Proactive Contribution to Peace'*, June 2014. Accessed June 20, 2018. http://www.mod.go.jp/atla/soubiseisaku/soubiseisakuseisan/2606honbuneigo.pdf.

Ministry of Economy, Trade and Industry. *Connected Industries (METI)*. Accessed February 18, 2018. http://www.meti.go.jp/english/policy/mono_info_service/connected_industries/index.html.

———. 「*Connected Industries*」東京イニシアティブ *2017 ["Connected Industries" Tokyo Initiative 2017]* [in Japanese], October 2017. Accessed November 18, 2017. http://www.meti.go.jp/press/2017/10/20171002012/20171002012-1.pdf.

———. *Cybersecurity Management Guidelines Revised (METI)*, November 2017. Accessed June 15, 2018. http://www.meti.go.jp/english/press/2017/1116_001.html.

———. 参考資料 *[Reference Materials]*, 2017. Accessed July 23, 2018. http://www.meti.go.jp/committee/kenkyukai/shoujo/sangyo_cyber/pdf/001_s01_00.pdf.

———. 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 Revision Requests]* [in Japanese], 2017. Accessed November 18, 2017. http://www.meti.go.jp/main/yosangaisan/fy2018/pdf/01_10.pdf.

Ministry of Economy, Trade and Industry and Information-technology Promotion Agency. サイバーセキュリティ経営ガイドライン *Ver 2.0 [Cybersecurity Guidelines for Business Leadership Ver 2.0]* [in Japanese], November 2017. Accessed June 15, 2018. http://www.meti.go.jp/press/2017/11/20171116003/20171116003-1.pdf.

Ministry of Finance. 租税特別措置法等（法人税関係）の改正 *[Revision of Special Tax Measures Law, etc. (Related to Business Taxes)]* [in Japanese], 2010. Accessed November 18, 2017. https://www.mof.go.jp/tax_policy/tax_reform/outline/fy2010/explanation/PDF/08_P350_420.pdf.

Ministry of Internal Affairs and Communications. 平成 3 0 年度税制改正に関する総務省要望のポイント *[MIC's 2018 Tax Revision Requests]* [in Japanese], 2017. Accessed November 28, 2017. http://www.mof.go.jp/tax_policy/tax_reform/outline/fy2018/request/soumu/30y_soumu_k.pdf.

Ministry of National Defense, Republic of Korea. *2016 Defense White Paper*, 2016. Accessed April 20, 2018. http://www.mnd.go.kr/user/mndEN/upload/pblictn/PBLICTNEBOOK_201705180357180050.pdf.

———. *2016 Defense White Paper*, 2016. Accessed April 20, 2018. http://www.mnd.go.kr/user/mndEN/upload/pblictn/PBLICTNEBOOK_201705180357180050.pdf.

Mitchell, Charlie. *Hacked: The Inside Story of America's Struggle to Secure Cyberspace*. Rowman & Littlefield, June 2016.

Morgan, Steve. *Cybersecurity Market Reaches $75 Billion In 2015; Expected To Reach $170 Billion By 2020*, December 2015. Accessed July 25, 2018. https://www.forbes.com/sites/stevemorgan/2015/12/20/cybersecurity%E2%80%8B-%E2%80%8Bmarket-reaches-75-billion-in-2015%E2%80%8B%E2%80%8B-%E2%80%8Bexpected-to-reach-170-billion-by-2020/.

National center of Incident readiness and Strategy for Cybersecurity. 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 *[About Support for Strenghtening Cyber Security Measures]* [in Japanese]. Technical report 9. November 2016. Accessed November 21, 2016. http://www.kantei.go.jp/jp/singi/keizaisaisei/miraitoshikaigi/4th_sangyokakumei_dai2/siryou9.pdf.

———. サイバーセキュリティ戦略本部　名簿 *[Cyber Security Strategic Headquarters, Register of Names]* [in Japanese], April 2016. Accessed March 24, 2017. http://www.nisc.go.jp/conference/cs/pdf/meibo.pdf.

———. 政府のサイバーセキュリティに関する予算 *[Government Budget Related to Cyber Security]* [in Japanese], 2017. Accessed April 22, 2017. https://www.nisc.go.jp/active/kihon/pdf/yosan2017.pdf.

National Cybersecurity and Communications Integration Center. *NCCIC Year in Review 2017: Operation Cyber Guardian*, 2018. Accessed July 31, 2018. https://www.us-cert.gov/sites/default/files/publications/NCCIC_Year_in_Review_2017_Final.pdf.

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

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

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

National Institute of Standards and Technology. *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*. Technical report NIST Cybersecurity White Paper. Gaithersburg, MD, April 2018. Accessed June 23, 2018. http://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.02122014.pdf.

Negoita, Marian. "To Hide or Not to Hide? The Advanced Technology Program and the Future of U.S. Civilian Technology Policy." In *State of Innovation: The U.S. Government's Role in Technology Development*, edited by Fred Block and Matthew R. Keller, 77–95. Boulder, CO: Paradigm Publishers, 2011.

New Energy and Industrial Technology Development Organization. *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 *[NEDO:Strategic Innovation Promotion Program/Ensuring the Cyber Security of Critical Infrastructure]* [in Japanese], 2017. Accessed February 16, 2018. http://www.nedo.go.jp/activities/ZZJP_100109.html.

———. 研究開発内容（全体版）*[Contents of Research and Development (Complete Version)]* [in Japanese], 2017. Accessed February 17, 2018. http://www.nedo.go.jp/content/100862901.pdf.

Office of Management and Budget. "21. Cyber Security Funding." In *An American Budget: Analytical Perspectives*, 273–287. Washington, D.C.: U.S. Government Publishing Office, 2017. Accessed July 23, 2018. https://www.whitehouse.gov/wp-content/uploads/2018/02/ap_21_cyber_security-fy2019.pdf.

Oh, Yong Seok. *Current Cybersecurity Trends and Responses in Korea*, October 2015. Accessed April 23, 2018. http://www.kisa.or.kr/uploadfile/201610/2016100710033367061.pdf.

Okimoto, Daniel I. *Between MITI and the Market: Japanese Industrial Policy for High Technology*. Stanford University Press, 1989.

Omori, Kazuaki. *Cybersecurity Policy and Projects by Ministry of Internal Affairs and Communications (MIC)*. Tokyo, November 2016. Accessed February 20, 2018. https://www.oasis-open.org/events/sites/oasis-open.org.events/files/1.6%20MIC%20Kazuaki%20Omori.pdf.

Oros, Andrew L. *Japan's Security Renaissance: New Policies and Politics for the Twenty-First Century*. Columbia University Press, March 2017.

Pack, Howard Saggi, Kamal. *The Case For Industrial Policy : A Critical Survey*. Policy Research Working Papers. The World Bank, February 2006. Accessed July 26, 2018. https://elibrary.worldbank.org/doi/abs/10.1596/1813-9450-3839.

Park, Donghui. *Cybersecurity Spotlight: South Korea*, January 2016. Accessed April 19, 2018. https://jsis.washington.edu/news/cybersecurity-spotlight-south-korea/.

Pekkanen, Saadia M. *Picking Winners?: From Technology Catch-up to the Space Race in Japan*. Stanford University Press, 2003.

Pryor, Crystal. "Japan's New Approach to Defense Technology." *The Diplomat*, November 2015. Accessed August 1, 2018. https://thediplomat.com/2015/11/japans-new-approach-to-defense-technology/.

82,000 PCs in Japan, worldwide infected with virus harvesting banking passwords, April 2015. Accessed August 1, 2018. https://www.rt.com/news/248673-japan-vawtrak-bank-infect/.

Sabatier, Paul, and Daniel Mazmanian. "The Conditions of Effective Implementation: A Guide to Accomplishing Policy Objectives." *Policy Analysis* 5, no. 4 (1979): 481–504.

Samuels, Richard J. *"Rich Nation, Strong Army": National Security and the Technological Transformation of Japan*. Cornell University Press, 1994.

———. *Securing Japan: Tokyo's Grand Strategy and the Future of East Asia*. Cornell University Press, 2007.

———. *The business of the Japanese state: energy markets in comparative and historical perspective*. Cornell University Press, 1987.

Schaede, Ulrike. "From developmental state to the 'New Japan': the strategic inflection point in Japanese business." *Asia Pacific Business Review* 18, no. 2 (April 2012): 167–185.

Schmidt, Klaus M., and Monika Schnitzer. "Public Subsidies for Open Source - Some Economic Policy Issues of the Software Market." *Harvard Journal of Law & Technology* 16 (2002): 473–506.

Segal, Adam. *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age*. PublicAffairs, February 2016.

Shin, Dong-Myeon. *Social and Economic Policies in Korea: Ideas, Networks and Linkages*. Abingdon, Oxon: Routledge, 2003.

Shin, Seiichi. "A status of control system security in Japan." In *2015 10th Asian Control Conference (ASCC)*, 1–4. May 2015.

Silipo, Damiano Bruno, and Avi Weiss. "Cooperation and competition in an R&D market with spillovers." *Research in Economics* 59, no. 1 (March 2005): 41–57.

Simmons, Beth A., and Zachary Elkins. "The Globalization of Liberalization: Policy Diffusion in the International Political Economy." *American Political Science Review* 98, no. 1 (February 2004): 171–189.

Simon, Herbert A. "Human Nature in Politics: The Dialogue of Psychology with Political Science." *American Political Science Review* 79, no. 2 (June 1985): 293–304.

Singer, P. W., and Allan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know®*. Oxford University Press, December 2013.

Snyder, Jack. *Myths of Empire: Domestic Politics and International Ambition*. Cornell University Press, 1991.

Son, Doil, and Sun Hee Kim. *Korea Cybersecurity –Getting The Deal Through –GTDT*, January 2018. Accessed April 20, 2018. https://gettingthedealthrough.com/area/72/jurisdiction/35/cybersecurity-korea/.

South Korea | OpenNet Initiative, August 2012. Accessed August 6, 2018. https://opennet.net/research/profiles/south-korea#footnote106_196rpsn.

Stockholm International Peace Research Institute. *SIPRI Military Expenditure Database*, 2018. Accessed July 30, 2018. https://www.sipri.org/sites/default/files/3_Data%20for%20all%20countries%20from%201988%E2%80%932017%20as%20a%20share%20of%20GDP.pdf.

Stop Think Connect. *Our Partners*. Accessed June 23, 2018. https://stopthinkconnect.org/get-involved/our-partners.

———. *Stop.Think.Connect.* Accessed July 31, 2018. https://stopthinkconnect.org/.

Succar, Patricia. "The Need for Industrial Policy in LDC's-A Re-Statement of the Infant Industry Argument." *International Economic Review* 28, no. 2 (1987): 521–534.

Sweeney, Latanya, and Ji Su Yoo. "De-anonymizing South Korean Resident Registration Numbers Shared in Prescription Data." *Technology Science*, September 2015. Accessed July 5, 2018. https://techscience.org/a/2015092901/.

Taliaferro, Jeffrey W. "State Building for Future Wars: Neoclassical Realism and the Resource-Extractive State." *Security Studies* 15, no. 3 (September 2006): 464–495.

Tatsumi, Yuki. *Japan's National Security Policy Infrastructure: Can Tokyo Meet Washington's Expectation?* Washington, DC: Henry L. Stimson Center, 2008.

Telecom-ISAC. *Cyber Clean Center / What is Cyber Clean Center?* Accessed October 16, 2017. `https://www.telecom-isac.jp/ccc/en_index.html`.

Teplinsky, Melanie J. "Fiddling on the Roof: Recent Developments in Cybersecurity." *American University Business Law Review* 2 (2013): 225–322.

Tokio Marine Nichido. リスクマネジメント動向調査 *2015 [Risk Management Survey Report 2015]* [in Japanese], 2015.

True, Jacqui, and Michael Mintrom. "Transnational Networks and Policy Diffusion: The Case of Gender Mainstreaming." *International Studies Quarterly* 45, no. 1 (2001): 27–57.

Tsuchiya, Motohiro. "Cyber Security Governance in Japan: Two Strategies and a Basic Law." In *Information Governance in Japan: Towards a New Comparative Paradigm*, edited by Kenji E. Kushida, Yuko Kasuya, and Eiji Kawabata. Silicon Valley New Japan Project, 2016.

Veluz, Danielle Anne. *VAWTRAK Plagues Users in Japan - Threat Encyclopedia - Trend Micro AU*, June 2014. Accessed August 1, 2018. `https://www.trendmicro.com/vinfo/au/threat-encyclopedia/web-attack/3141/vawtrak-plagues-users-in-japan`.

Vogel, Steven K. *Japan Remodeled: How Government and Industry are Reforming Japanese Capitalism*. Cornell University Press, 2006.

———. *Marketcraft: How Governments Make Markets Work*. Oxford University Press, February 2018.

Volden, Craig, Michael M. Ting, and Daniel P. Carpenter. "A Formal Model of Learning and Policy Diffusion." *American Political Science Review* 102, no. 3 (August 2008): 319–332.

Wagenseil, Paul, and Staff. *Best Antivirus Software and Apps 2018*, July 2018. Accessed July 18, 2018. `https://www.tomsguide.com/us/best-antivirus,review-2588.html`.

Walt, Stephen M. "The Renaissance of Security Studies." *International Studies Quarterly* 35, no. 2 (1991): 211–239.

Waltz, Kenneth Neal. *Theory of International Politics*. McGraw-Hill, January 1979.

Warwick, Ken. *Beyond Industrial Policy*. OECD Science, Technology and Industry Policy Papers 2. April 2013. Accessed February 9, 2017. `http://www.oecd-ilibrary.org/science-and-technology/beyond-industrial-policy_5k4869clw0xp-en`.

Weir, Margaret, and Theda Skocpol. "State Structures and the Possibilities for "Keynesian" Responses to the Great Depression in Sweden, Britain, and the United States." In *Bringing the State Back In*, edited by Peter B. Evans, Dietrich Rueschemeyer, and Theda Skocpol, 107–164. Cambridge: Cambridge University Press, 1985.

Willis Towers Watson. *Decoding Cyber Risk: 2017 Willis Towers Watson Cyber Risk Survey, US Results*, 2017. https://www.willistowerswatson.com/-/media/WTW/PDF/Insights/2017/06/WTW-Cyber-Risk-Survey-US-2017.pdf.

Zetter, Kim. "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History." *Wired*, July 2011. Accessed July 18, 2018.

이유지. *2017* 년국가사이버보안연구개발에 *1* 천억원투입 [in Korean], December 2016. Accessed July 27, 2018. https://www.bloter.net/archives/269792.

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)]. 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]* [in Japanese], April 2017. Accessed February 16, 2018. http://www.nedo.go.jp/content/100767969.pdf.