PROGRAM ON U.S.-JAPAN RELATIONS
Weatherhead Center FOR INTERNATIONAL AFFAIRS
HARVARD UNIVERSITY

HARVARD
UNIVERSITY

HOW JAPANESE CYBERSECURITY POLICY CHANGES

Benjamin Bartlett

Harvard Program on U.S.-Japan Relations
Occasional Paper Series
2019-01

https://programs.wcfia.harvard.edu/us-japan/research

Table of Contents

Tables

Introduction

In his book, *How Policies Change*, which looks at how Japan's old-age policy has changed over time, John Campbell lays out a theory of policy change that builds upon and synthesizes insights from four sets of theories of policy change. Each makes different fundamental assumptions about the nature of the policy process. Campbell argues that each approach describes the policy making process some of the time, and that which approach works best depends on whether energy, ideas, both, or neither were important to the outcome.

Though a useful framework, Campbell does not consider how one might know, *a priori*, which approach is most likely to apply for a given situation. Drawing upon historical institutionalism, I outline such an approach below, then apply it to the history of Japanese cybersecurity policymaking from the late 1990s until 2016. I find mixed results for the theory, and propose further avenues for refinement in the conclusion.

Theory

Campbell identifies four basic theoretical approaches to explaining the policy-making process. The first theoretical approach Campbell labels the "political" theories of policy change. The theories that follow this approach assume that at least two actors or coalitions of actors compete to enact their preferred policy positions, and that policy outcomes will reflect the balance of power between these actors or coalitions. These theories differ in the degree to which actors are assumed to be driven by material interests, the degree of actors rationality, and the

degree to which their relationships are determined by institutional arrangements.[1] Examples of this approach include the Institutional Analysis and Development framework, where rational actors compete over material goods and the result is largely determined by institutional arrangements, and the Advocacy Coalition Framework, where coalitions of actors drawn from a variety of institutions fight over policy outcomes. While the Institutional Analysis and Development framework mainly sees the actors involved as purely rational and the disagreement as being over the distribution of resources, the Advocacy Coalition Framework focuses on more value-driven policy arguments and draws on insights from psychology to explain the ways in which each side tends to demonize the other and to explain the effects this has on the resulting political battle.[2]

Campbell calls a second approach the "cognitive" theories of policy change. This approach assumes that policy decisions are made by actors searching for the best solution to a given problem. This does not mean that actors necessarily arrive at the optimal solution: they may fall short due to limits in time, resources, or cognition. Indeed, decision-makers may even fail to correctly identify the problem. As with the "political" theories, there can be disagreement between different participants in the policy-making process. The disagreements, however, are intellectual: over what the nature of the problem, its importance relative to other problems, and what would be the most effective solution. Disagreements are resolved via discussion and persuasion, rather than through the exercise of power.[3]

---

[1] John Creighton Campbell, *How Policies Change: The Japanese Government and the Aging Society* (Princeton University Press, 2014) 30–31.

[2] Elinor Ostrom, "Institutional rational choice: An assessment of the institutional analysis and development framework," in *Theories of the policy process*, vols., 2nd ed. (Cambridge, MA: Westview Press, 2007), 21–64; Paul A. Sabatier and C.M. Weibel, "The advocacy coalition framework: Innovations and clarifications," in *Theories of the policy process*, vols., 2nd ed. (Cambridge, MA: Westview Press, 2007), 189–220.

[3] Campbell, *How Policies Change* 29–30.

The most straight-forward version of this approach assumes that the actors are rational. Policy decisions can then be assumed to be optimal solutions to a given problem, and the nature of that problem can then be inferred by working backwards from the solution.[4], Other approaches do not make this assumption and instead seek to explain why sub-optimal decisions may be made. An example is sociological institutionalism, which assumes that both actors' thinking and the policy-making process are shaped by the institutions to which they belong. Thus, institutions can affect policy in two ways: they can change actors' thinking through learning and socialization, and they can affect what problems or solutions actually get a hearing from those actors in a position to make a decision. Sub-optimal decisions may be due to faults in actors' thinking (for example misapplying a lesson learned from an early policy-making experience to a policy situtation to which it does not truly apply) or because better ideas do not receive a hearing.[5]

Campbell labels the third approach the "artifactual" theories of policy change. These theories treat policy change as coincidences: an opportunity for change opens up, and actors use this opportunity to promote problems and solutions in which they have an interest. As a result, problems get considered regardless of importance, and solutions that may not truly be appropriate get attached to problems. An example of this approach is the Multiple Streams (MS) framework, developed by Kingdon and based on the "garbage can theory" of organizational

---

[4] See Graham Allison, *Essence of Decision* (Little, Brown, 1971). for a summary of this approach.

[5] 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 by. Peter B. Evans, Dietrich Rueschemeyer, and Theda Skocpol (Cambridge: Cambridge University Press, 1985) 120, 125–132; Judith Goldstein, "The Political Economy of Trade: Institutions of Protection," *The American Political Science Review* 80.1 (1986): 161–184; John L. Campbell, "Institutional Analysis and the Role of Ideas in Political Economy," *Theory and Society* 27.3 (1998): 377–409; Peter J. Katzenstein, "Same War: Different Views: Germany, Japan, and Counterterrorism," *International Organization* 57.4 (2003): 731–760.

choice.[6] What determines policy outcomes in this framework is time and attention. MS works under conditions of what Kingdon terms "organized anarchies", characterized by fluid participation, problematic preferences, and unclear technology. Participation is fluid when different actors drift in and out of policy-making settings, and devote different levels of energy and attention to a given decision. Preferences are problematic when actors do not know what they want. Finally, technology is unclear when it is not obvious, even to participants, how the organization turns inputs into products (in this case, policy outcomes).[7]

This is a situation in which means-ends logic does not well apply: problems are ill-defined, and information is plentiful but processing it (and deciding what is relevant) is costly. Contradictory policies are frequently a result. The framework conceives of policy-making as being made up of three independent "streams", which flow along time: a *problem stream*, a *policy stream*, and a *politics stream*. The problem stream contains problems that policy-makers may wish to address. They discover these problems via three means: indicators, focusing events, and feedback. Indicators are pieces of data that can be easily tracked and interpreted, for example, the unemployment rate. Focusing events are often some sort of crisis that reveals a major problem: a successful terrorist attack, or the outbreak of a disease, for example. Feedback includes the outcomes of previous policy decisions, by which those decisions can be judged.[8]

The policy stream consists of a set of ideas, generated by specialists in policy communities, that seek to win acceptance in policy networks. These networks may be more or

---

[6] Michael D. Cohen, James G. March, and Johan P. Olsen, "A garbage can model of organizational choice," *Administrative Science Quarterly* 17.1 (1972): 1–25.

[7] John W. Kingdon, *Agendas, Alternatives, and Public Policies*, vols., 2nd ed. (HarperCollins College Publishers, 1995); N. Zachariadis, "The multiple streams framework: Structure, limitations, prospects," in *Theories of the policy process*, 2nd ed. (Cambridge, MA: Westview Press, 2007) 67.

[8] Kingdon, *Agendas, Alternatives, and Public Policies*.

less integrated: less integrated networks are larger in size, are competitive, have lower administrative capacity, and less restricted access; more integrated networks are smaller, consensual, have higher administrative capacity, and more restricted access.[9]

Finally, the politics stream is made up of three elements: the national mood, pressure-group campaigns, and administrative or legislative turnover. Policy choices are made when these three streams are coupled together at a critical time by a policy entrepreneur. Opportunities for change come from the political stream, whereas problems and solutions come from their respective streams. Critically, because the three streams are independent, there is no guarantee that at the time a window opens, there will be a fitting solution for every problem, yet successful policy change requires drawing together both. Thus, for example, a policy entrepreneur who wants to take advantage of a policy window to raise a particular problem may have no choice but to attach a sub-optimal solution. Worse, a policy entrepreneur who wants to push a particular solution may simply attach it to an available problem, even if other, better solutions are available.[10]

What matters under these conditions is who pays attention to what, when. Time is the key, irreplaceable resource, which decision-makers seek to manage effectively. Policy is thus often determined by who happens to be in the right place at the right time, and who has the motivation to put the time into pushing a particular problem or solution.[11]

Campbell labels the last approach "inertial" theories. According to this approach, policy change occurs when some change in the world is processed in a predictable way. An example of this sort of theory is organization theory. In organization theory, an organization develops a set

---

[9] ibid.
[10] ibid.; Zachariadis, "The multiple streams framework" 68, 70–74.
[11] Kingdon, *Agendas, Alternatives, and Public Policies*.

of routines to deal with particular problems. When a problem or situation arises, the organization responds using one of these standards routines.[12] These routines can change, based on feedback about outcomes, but that change is incremental and predictable.[13]

Campbell notes that while doing research on policy change, he has found that no one of these approaches to policy change accurately describes the process all of the time. Instead, each describes policy change under specific circumstances. He argues that which approach accurately describes the policy process relies on whether or not two factors are important in the policy process: ideas and energy. *Ideas* include how something comes to be seen as a problem, how solutions are developed or identified, and how these things are linked. *Energy* is the impetus driving actors to act.[14]

Campbell's argument is summarized in Table 1. When both ideas and energy are important, then the political approach to policy change will do the best job of describing the policy-making process. In this mode, energy is linked to ideas: participants in the process have differing ideas, and the outcome is determined by the amount of energy each is able or willing to expend on the issue and how effectively they do so.[15]

When ideas are important, but not energy, then the cognitive approach does the best job describing the policy-making process. Because argumentation and persuasiveness matter, it is clear that ideas matter in this mode. But the relative power of the participants—that is, the level of energy they have avaiable to them—is not relevant to the outcome. A "good" solution

---

[12] James G. March and Herbert Alexander Simon, *Organizations* (Wiley, 1958).
[13] Campbell, *How Policies Change* 33–35.
[14] ibid., 26–27.
[15] ibid., 30.

(according to some criteria) will win the day whether it is proposed by a lowly bureaucrat or by a powerful politician[16]

The artifactual mode is the opposite of the cognitive mode: here energy matters a great deal, but the outcome has nothing to do with the quality of the ideas themselves. Non-urgent problems and sub-optimal solutions can easily rise to the fore. What matters for the outcome is if there is a policy entrepeneur with the time and energy to push for a particular policy.[17]

When the policy outcome is simply a routine, predictible shift in response to some external change, then neither the energy of the participants nor the nature of the ideas involved matter to that outcome. This is the inertial mode.[18]

Though Campbell's framework provides a useful synthesis of the various theoretical approaches, it does not tell us when we should anticipate energy or ideas to matter in the policy-making process. That is, while we can tell *a posteriori* what mode was operative, there is not a clear way to tell *a priori* which mode is likely to be operative. We need some theory of when we ought to expect energy or ideas to matter. I make a first cut attempt at this below.

It may be easiest to start with the question: when would energy—that is, political power—*not* influence the outcome? The situation in which this seems most likely is when there is general consensus on the direction or goals of policy. This is not to say there is no room for disagreement: the cognitive mode clearly has room for argument between actors involved in the policy-making process. But the very fact that pursuasion is possible suggests that disagreements in this mode are not over fundamental values. The policy changes under discussion will be those that fall under what Peter Hall calls "first order changes": adjustments that are made in response

[16] ibid., 29.
[17] ibid., 31–32.
[18] ibid., 33–34.

to the consequences of past policies or new developments rather than a fundmental rethinking of policy.[19] Note that sometimes this can be a "negative consensus": it could be a consensus that a given issue is not important. By contrast, when there is not a rough consensus around policy goals, when major shifts in policy are being considered (what Hall calls second-order or third-order change[20]), then we would expect energy to matter, as actors will different goals and values battle over their preferred policy outcome.[21] In terms of understanding when ideas would matter, we think of what would be the opposite situation of that anticipated by the multiple streams approach: participation is relatively fixed, actors know their own preferences, and technology is clear.

What factors, then, will drive changes in these modes? Historical institutionalism gives us some insight here. Institutions fix participation and make preferences clear. They help to define problems and reduce the cost of processing information.[22] In short, institutionalization should make ideas more important. They should also build consensus, at least within the institutions. However, institutionalism tells us that consensus can also be broken, usually by some exogenous shock, which makes it clear that current policies are not working, or that new solutions must be

---

[19] Peter A. Hall, "Policy Paradigms, Social Learning, and the State: The Case of Economic Policymaking in Britain," *Comparative Politics* 25.3 (1993): 281, online, Internet, 21 May. 2018.

[20] ibid., 281–287.

[21] ibid., 281.

[22] James G. March and Johan P. Olsen, "The new institutionalism: Organizational factors in political life," *The American Political Science Review* 78.3 (1984): 734–749; Theda Skocpol and Kenneth Finegold, "State capacity and economic intervention in the early new deal," *Political Science Quarterly* 97.2 (1982): 255–278; Aaron Wildavsky, "Choosing preferences by constructing institutions: A cultural theory of preference formation," *The American Political Science Review* 81.1 (1987): 4–21.

sought. Examples include the oil crisis[23] and the Great Depression[24]. The shock need not be as dramatic as these cases, but the theme is the same: some negative occurance or outcome creates a demand for "something to be done".

What does this mean for our expectations about changes in Japanese cybersecurity policy? There were two major external shocks with regard to cybersecurity in Japan: one toward the end of the 1990s and the beginning of the 2000s, when the Japanese government had been pushing forward its plan for e-government and there were a series of attacks on government websites, and a second in the early-to-mid-2010s when another set of attacks on government computers gained public attention and demonstrated that cybersecurity had not yet been achieved. Cybersecurity policy was also clearly institutionalized in 2005, with clear government responsibility placed in a pair of cabinet bodies (more on this below). A summary of the anticipated modes of policy change over time can be seen in Table 2.

Prior to 1999, the Japanese government was not focused on cybersecurity. The attacks on government websites at the end of the 1990s and beginning of the 2000s created energy for change, but without clear institutional responsibility, ideas about what to do were diffuse. We would thus anticipate that Japanese cybersecurity policy-making would enter the artifactual phase Once clear institutions were created, we would expect ideas to start mattering more: first this would lead to a period of political policy-making, but as institutionalization continued and consensus was built, we should anticipate a shift toward the cognitive mode. Finally, a second

---

[23] Peter J. Katzenstein, "Conclusion: Domestic structures and strategies of foreign economic policy," *International Organization* 31.4 (1977): 879–920; G. John Ikenberry, "The Irony of State Strength: Comparative Responses to the Oil Shocks in the 1970s," *International Organization* 40.1 (1986): 105–137; M. Stephen Weatherford and Haruhiro Fukui, "Domestic adjustment to international shocks in japan and the united states," *International Organization* 43.4 (1989): 585–623.

[24] Weir and Skocpol, "State Structures and the Possibilities for 'Keynesian' Responses to the Great Depression in Sweden, Britain, and the United States"; Goldstein, "The Political Economy of Trade.".

series of cyber attacks against the government, including data exposed via the hacking of the Japan Pension System, in 2014–2015 should break this consensus and lead again into the political mode. To see how well this theory holds up, I examine each period in turn below.

1999–2005

Prior to the end of the 1990s, cyber security was primarily the responsibility of the private sector; the Japanese government had not yet been paying much attention to the issue. Toward the end of the 1990s and the beginning of the 2000s, there were a series of attacks on government websites.[25] The series of attacks on the websites of the Japanese government had highlighted the weaknesses of Japan's cybersecurity policy: it was becoming clear that responsibility for cybersecurity needed to be clearer, and that a coherent policy had to be constructed. But it was an open question as to what ministry or agency would take charge, and a number of different proposals and possible institutional structures rose and fell before the final solution was arrived upon.

In August of 1999, the government passed the Act to Prohibit Illegal Access (不正アクセス禁止法). In September 1999, the Conference of Ministries and Agencies Related to Information Security (情報セキュリティ関係省庁局長等会議) was set up. Headed by the Deputy Cabinet Secretary, this meeting included the Deputy Chief Cabinet Secretary for Crisis Management, the Chief of Cabinet Affairs Deliberation, the Chief of the Cabinet Crisis Office, and representatives from the National Police Agency, the Financial Services Agency, the General

[25] Yurie Ito, Greg Rattray, and Sean Shank, "Japan's Cyber Security History," in *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, ed by. Jason Healey (Cyber Conflict Studies Association, 2013).

Affairs Agency, the Japan Defense Agency, the Ministry of Justice, the Ministry of Foreign Affairs, the Ministry of Finance, the Ministry of Health and Welfare, the Ministry of International Trade and Industry, the Ministry of Transport, the Ministry of Posts and Telecommunications, and the Ministry of Home Affairs. This conference released the "Action Plan for Infrastructure Development to Cope with Hackers."[26] At the same time, a group under the newly-established Strategic Headquarters for the Promotion of an Advanced Information and Telecommunications Networks Society (aka IT Strategic Headquarters), the Council for the Promotion of Information Security Measures (情報セキュリティ対策推進会議) was established. This council was created to act as a liaison between government officials and private-sector chief information security officers (CISOs). It created policies such as the Special Action Plan for Responding to Cyberterrorism on Critical Infrastructure (重要インフラのサイバーテロ対策に係る特別行動計画).[27]

During this time, debates continued about who would be given ultimate responsibility for cybersecurity policy. Because cybersecurity was both a crime prevention issue and a national security issue, two of the main candidates at the time were the National Police Agency (NPA) and the Japan Defense Agency (JDA), the latter of which would later become the Ministry of

---

[26] Motohiro Tsuchiya, "Cyber Security Governance in Japan: Two Strategies and a Basic Law," in *Information Governance in Japan: Towards a New Comparative Paradigm*, ed by. Kenji E. Kushida, Yuko Kasuya, and Eiji Kawabata (Silicon Valley New Japan Project, 2016); Office of the Prime Minister of Japan, "情報セキュリティ関係省庁局長等会議の設置について [About the Establishment of the Conference of Ministries and Agencies Related to Information Security]," n.d., online, Internet, 19 Jun. 2018., Available: https://www.kantei.go.jp/jp/it/security/taisaku/0917kyokutyou.html.

[27] 情報セキュリティ対策推進会議 [Council for the Promotion of Cybersecurity Measures], "重要インフラのサイバーテロ対策に係る特別行動計画　[Special Action Plan for Responding to Cyberterrorism on Critical Infrastructure]," Dec. 2000, online, Internet, 18 Jul. 2019., Available: https://www.nisc.go.jp/active/sisaku/2000_1215/pdf/txt3.pdf; 情報セキュリティ対策推進会議 [Council for the Promotion of Cybersecurity Measures], "情報セキュリティ対策推進会議について [About the Council for the Promotion of Information Security Measures]," Jul. 2005, online, Internet, 18 Jul. 2019., Available: https://www.nisc.go.jp/conference/suishin/ciso/pdf/konkyo.pdf.

Defense (MOD).[28] The NPA had been relatively quick to realize that cybercrime would be an increasing prolem: in 2001 it had begun convening meetings with members of industry and academia as well as other concerned parties to discuss cybersecurity issues.[29] At the same time it set up the Cyber Force Center (CFC) to provide technical support in dealing with cyber crime.[30] JDA had not been nearly as proactive, but was a natural possibility given the national security concerns involved.[31]

The prospects of NPA or JDA being responsible for cybersecurity policy worried cybersecurity experts outside of government. It was their fear that these two agencies would not properly appreciate the role that international standards and cooperation play in cybersecurity, and might pursue Japan-specific policies without consideration for the ramifications for software development or the Japanese information technology sector as a whole. The director of JPCERT/CC, Dr. Yamaguchi Suguru, was particularly concerned.[32] JPCERT/CC had been set up in 1992 as a volunteer task force in the private sector, though it had begun receiving support from MITI in 1996. It functioned as Japan's main Computer Security Incident Response Team (CSIRT), and had largely been responsible for Japanese cybersecurity until this point.[33] In order

---

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

[29] National Police Agency, "警察庁　総合セキュリティ対策会議　概要 [National Police Agency - Coordinated Security Measures Council - Summary]," 2001, online, Internet, 11 Jul. 2019., Available: http://www.npa.go.jp/cyber/csmeeting/h13/pdf/h13gaiyou.pdf; 総合セキュリティ対策会議 [Coordinated Security Measures Council], "第 1 回総合セキュリティ対策会議　発言要旨　[The First Meeting of the Coordinated Security Measures Council - Summary of Remarks]," Dec. 2001, online, Internet, 11 Jul. 2019., Available: http://www.npa.go.jp/cyber/csmeeting/h13/pdf/h13youshi1.pdf; 総合セキュリティ対策会議 [Coordinated Security Measures Council], "情報セキュリティ対策における連携の推進について [About the Coordinated Promotion of Information Security Measures]," Mar. 2002, online, Internet, 11 Jul. 2019., Available: http://www.npa.go.jp/cyber/csmeeting/h13/pdf/pdf13a.pdf.

[30] Ito, Rattray, and Shank, "Japan's Cyber Security History.".

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

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

[33] ibid.; 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]," n.d., online, Internet, 16 Apr. 2017., Available: http://www.jpcert.or.jp/about/05.html. JPCERT/CC continues to play a large role in protecting the cybersecurity of Japan's private sector.

to make certain that the international aspects of cybersecurity were properly considered, Dr. Yamaguchi reached out to two powerful ministries within the Japanese government: Ministry of Economy, Trade and Industry (METI) and Ministry of Internal Affairs and Communications (MIC).[34]

METI and MIC were in many ways obvious allies for these outside experts to recruit. The ministers of both sat on the IT Strategic Headquarters and both had extensive experience with and jurisdiction over information technology issues. Both were likely to see cybersecurity in a way similar to the outside experts. Both had good reasons of their own to be worried about cybersecurity. METI was worried about the effects that cybercrime and other cybersecurity issues could have on Japan's economic competitiveness. Japan had been slow to move shopping and other services over to the internet, and METI feared that should the Japanese public come to fear that they could not use the internet safely, this would exacerbate the problem. MIC was worried about the effects that malware and cyber attacks might have on the networks and internet service providers (ISPs) that were under its jurisdiction. On top of this, both ministries were interested in expanding their own jurisdictions, with METI in particular looking for new roles as Japan's economy became less reliant upon its directions.[35]

METI and MIC were not, however, natural allies with one another. The predecessors of the two ministries had fought a long turf battle over information communications technology policy in the 1970s and 1980s, in which MIC's predecessor had largely come out on top.[36] The

---

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

[35] Interviews with MIC official and NISC official, Tokyo, July 2017. Ulrike Schaede, "From developmental state to the 'New Japan': The strategic inflection point in Japanese business," *Asia Pacific Business Review* 18.2 (2012): 167–185

[36] See Chalmers Johnson, "MITI, MPT, and the Telecom Wars," in *Politics and Productivity: How Japan's Development Strategy Works*, ed by. Chalmers Johnson, Laura D'Andrea Tyson, and John Zysman (Ballinger Publishing Company, 1989), 177–240. for a full exposition of this battle.

two ministries continued to regard each other as opponents. It took a number of meetings in Dr. Yamaguchi's office to convince the two ministries that when it came to cybersecurity policy, their interests were aligned. Ultimately, however, the outside experts prevailed, and an alliance was formed.[37]

Now allied, METI and MIC decided to coopt the possible opposition instead of fight an all-out turf battle. In part, they were able to do this thanks to a change in Japanese policy-making that had begun with Prime Minister Koizumi, in which more policy-making was being done in bodies created within the cabinet instead of within the ministries themselves.[38] This meant that the policy-making process could more easily incorporate the views of multiple ministries and agencies.

Bureaucrats from METI and MIC began meeting regularly with bureaucrats from NPA and JDA. Forging an agreement between the four bodies proved difficult, but the MIC bureaucrats were particularly industrious and managed to build consensus via two means. First, they found that despite the differences between the bodies, all four agreed that protecting critical infrastructure from cyber attacks was as key priority. This gave them a basis for cooperation and a key set of policies around which consensus could be built. Second, they gathered the opinions and concerns of all of the bureaucrats involved in the meetings, and then worked overtime to produce a policy document addressing all of those concerns. It was difficult for the other parties involved to raise further objections upon being presented with this document, and MIC was able to present this document to the government as the consensus opinion of the four bodies involved.[39]

---

[37] Author's interview with MIC official, Tokyo, July 2017.
[38] Schaede, "From developmental state to the 'New Japan'.".
[39] Interview with MIC official, Tokyo, July 2017.

From these meetings the First National Strategy on Information Security was born. More importantly, however, these meetings led to a new structure in which cybersecurity policy would be decided. Following policy recommendations decided upon during this meeting, in May 2005 the Prime Minister ordered the establishment of the Information Security Policy Council (ISPC).[40] The ISPC was located under the IT Strategic Headquarters in the Cabinet Office. It was chaired by the Chief Cabinet Secretary. Its members included the Minister of Internal Affairs and Communications; the Minster of Economy, Trade and Industry, the Chairman of the National Public Safety Commission (who is in charge of the NPA); the Director General of the Japan Defense Agency (later the Minister of Defense); and the Minister of State for Science and Technology policy, who headed the ITSH and served as vice-chair for the ISPC. Note that this includes the leadership of METI, MIC, NPA, and JDA/MOD. Beyond these members of government, the ISPC included six members from the private sector. In 2012, the Minister of Foreign Affairs was added as well.[41]

As secretariat to this new cabinet body, the National Information Security Center (NISC) was formed.[42] While major policy decisions came out of the ISPC, the ground-work and details of implementation were mainly left to NISC: ISPC would meet around 5 times per year for around 30–60 minutes per meeting, while NISC was operational year-round. Though NISC had

---

[40] Ito et al. claim that the ISPC was founded in 2001, citing Munenori Kitahara, "Information society law in japan," *US-China Law Review*1 (2011): 21–40, but I have not been able to locate this information in the work they cite, and all other information I have found points to 2005 as the founding year. See Ito, Rattray, and Shank, "Japan's Cyber Security History" 243–244. It is possible that Ito et al. confused the Information Security Policy Council (情報セキュリティ政策会議) with the Council for the Promotion of Information Security Measures (情報セキュリティ対策推進会議), which was active in 2000 and which was responsible for releasing the policy documents which Ito et al. credit to ISPC.

[41] Information Security Policy Council, "The First National Strategy on Information Security," Feb. 2006, online, Internet, 14 May. 2018., Available: https://www.nisc.go.jp/eng/pdf/national_strategy_001_eng.pdf; Tsuchiya, "Cyber Security Governance in Japan.".

[42] In point of fact, NISC was formed first, in April 2005.

some technical staff as well, it was primarily staffed by bureaucrats from METI, MIC, MOD, and NPA who had been seconded to it.[43]

The drafting of the national cybersecurity strategies, which would ultimately be released by ISPC, were done by the bureaucrats staffing NISC along with input from outside experts. During this period this process consisted of NISC creating working groups explicitly for this purpose, and then inviting experts to be part of those working groups.[44] Of course, the ISPC had input into these drafts as well, but because the time the politicians sitting on it had to devote to these issues was limited relative to the bureaucrats, the groundwork was done primarily by NISC.

This period fits the description of the artifactual mode of policy change rather well. The eventual outcome was largely determined by the energy put into it by the Dr. Yamaguchi and the outside experts and then the bureaucrats at MIC, in turn. The primary problem arrived upon, protecting critical infrastructure, reflected the priorities of those at the table, and the solution, ISPC and NISC, was based as much in their own interests in further influencing policy as it was in tackling the problem. This is not to say the problem or solution were particularly bad (indeed, it is easy to argue that protecting critical infrastructure *should* be a priority), but it is easy to imagine that had Dr. Yamaguchi's energy been used elsewhere, a very different set of problems and solutions would have emerged.

---

[43] National center of Incident readiness and Strategy for Cybersecurity, "サイバーセキュリティ戦略本部 [cyber security strategic headquarters]," n.d., online, Internet, 16 Jul. 2018., Available: http://www.nisc.go.jp/conference/cs/index.html; Tsuchiya, "Cyber Security Governance in Japan.".

[44] Tsuchiya, "Cyber Security Governance in Japan.".

2006–2010

In the period between 2006–2010 there were no obvious crises, and instead policy-making was now embedded in the ISPC and NISC. According to the theory laid out in Section 2, this should lead us first into the political mode, as participation is now fixed and actor preferences are now clear. As socialization within the institutions continues throughout the period, we should anticipate that consensus will be reached and should shift toward the cognitive mode. As will be seen, this is not quite what happens.

During this period the First and Second National Strategies on Information Security were released. The First National Strategy, which came out of the meetings described in the previous section and which was released in 2006, set out three objectives for information security: the continuous development of Japan as a major economic power, the realization of better lives for the people, and ensuring national security, in that order.[45] The Second National Strategy, released in 2009, reaffirmed these goals, though switched the focus from preventing cyber attacks to responding to them.[46] The order of these three goals well represents the priorities of Japan's cybersecurity strategy during this time: a focus first on economic security, then on individual security, and only then on national security. Beyond the efforts to improve government cybersecurity, Japan's efforts can be summarized as consisting of two parts: a set of guidelines, incentives, and institutions meant to encourage the private sector (and particularly critical infrastructure firms) to improve their cybersecurity; and a set of programs aimed at improving the cybersecurity of the general public.

---

[45] Information Security Policy Council, "The First National Strategy on Information Security" 2.

[46] Information Security Policy Council, "The Second National Strategy on Information Security," Feb. 2009, online, Internet, 14 May. 2018., Available: https://www.nisc.go.jp/eng/pdf/national_strategy_002_eng.pdf.

One of the main ways the government worked to improve private sector cybersecurity was by providing cybersecurity guidelines and frameworks for Japanese firms. Importantly, these targeted not only technical workers within the firms, but also business executives and others. An example from this time period is the Information Security Management Benchmark (ISM-Benchmark), which is maintained on a government website. An executive can go to this website and answer a set of 40 question about their firm and then received information on how their firm is doing on cybersecurity relative to other, similar firms. The website also gives recommendations on how their firm could improve its cybersecurity based on these answers.[47] These guidelines and frameworks were often developed in coordination with industry. An example was the working group formed to develop the Smart Home Appliance Security Study Report. Between March and December 2010, the government 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.[48]

Along with releasing guidelines, the Japanese government also made efforts to encourage firms to participate in information sharing programs. These programs reduce the probability that the same attack will be effective against different firms: once one firm detects and reports a particular attack, other firms can adapt their systems to prevent it. However, firms are reluctant to participate in these programs, because it requires a firm that has been the victim of an attack to report that attack. This is not only potentially embarrassing, but can harm the stock value of the

[47] Information-technology Promotion Agency, "Outline of Information Security Benchmark (ISM-Benchmark)," 2007, online, Internet., Available: https://www.ipa.go.jp/files/000011798.pdf.

[48] Information-technology Promotion Agency, "2010 Smart Home Appliance Security Study Report," Jan. 2011, online, Internet, 22 Jun. 2018., Available: https://www.ipa.go.jp/files/000014115.pdf.

company, driving away investment. Though information sharing arrangements generally anonymize reports, this has not always been enough to reassure firms. The government works to educate firms about the benefits of information sharing. It also helps to fund some information-sharing organizations, such as JPCERT/CC.[49]

From FY 2006–2010, the government also instituted a set of tax measures meant to strengthen the IT of small-to-medium-sized enterprises, including their cyberscurity. The "Information Base Strengthening Tax System"[50] rewarded firms for acquiring or replacing 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. This incentivized companies both to buy cybersecurity software and equipment and to upgrade to equipment and software that met with current security standards. 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.[51]

The government also took specific steps to improve the cybersecurity of critical infrastructure firms. This included releasing standards and guidelines for specifically for critical infrastructure firms. Additionally, 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.[52] These transfer information

---

[49] Author's interviews with METI official, NISC official, and JPCERT/CC employee, Tokyo, July 2017. Tsuchiya, "Cyber Security Governance in Japan."

[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)]," 2010 369–370, online, Internet, 18 Nov. 2017., Available: https://www.mof.go.jp/tax_policy/tax_reform/outline/fy2010/explanation/PDF/08_P350_420.pdf.

[52] 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.

from the Cabinet Secretariat via the responsible ministries to their members, which are the firms of the relevant sector. The government also created a CEPTOAR Council, which has representatives from each CEPTOAR and shares information across sectors.[53]

Efforts to improve public cybersecurity during this period mainly took the form of education programs. These including advertisements on billboards and on the web and school programs meant to teach children basic cyber security skills, and short courses mixing information about cybercrime with examples of actual cases. The government also established "Information Security Month"[54] 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 broadcast over its streaming station.[55]

The Japanese government also took steps to deal with cybersecurity threats to the public more directly. Perhaps the most extensive of these efforts was the Cyber Clean Center. Running from December 2006 until March 2011, this was a joint effort between the telecommunications companies, JPCERT/CC, and the government. The Center would detect and analyze malware that turned computers into bots (a computer that can be used to run software or launch cyber operations of which its legitimate user is unaware). The CEnter also monitored the Japanese internet, and upon detecting a bot coming from a certain IP address, would then send a notice to the Internet Service Provider (ISP) that owned that address. The ISP would then forward this

---

[53] Information Security Policy Council, "Action Plan on Information Security Measures for Critical Infrastructures," Dec. 2005, online, Internet, 19 May. 2018., Available: http://www.nisc.go.jp/eng/pdf/actionplan_ci_eng.pdf.

[54] 情報セキュリティ月間

[55] 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]," Jul. 2014 13, 17, online, Internet, 14 Feb. 2018., Available: http://www.nisc.go.jp/active/kihon/pdf/awareness2014.pdf.

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.[56] The effort was funded entirely by the Japanese government.[57] The government also released software tools meant to help users secure their computers. For example, in 2009, the government 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.[58]

What we see throughout this period is a continued focus on using cybersecurity as a means to protect Japan's economic strength. Moreover, the policies the government adopts during this period place very little burden on private firms: there are no hard regulations, only government support and encouragement. This suggests an outcome more in line with the preferences of METI and MIC rather than a consensus arrived at by the four actors.

This outcome is what we would expect from the political mode. MIC and METI had several advantages over the other two ministries, particularly during this period in time. Due to their ministerial responsibilities, both were in a position to actually oversee the implementation of many aspects of cyber security policy. Both had strong connections with experts in the private sector and could draw on this expertise in crafting policy and supporting their positions. Both had a great deal of expertise in bureaucratic politics, particularly relative to MOD which was still

---

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

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

[58] Information-technology Promotion Agency, "JVN iPedia - Vulnerability Countermeasure Information Database / What is JVN iPedia?" n.d., online, Internet, 22 Jun. 2018., Available: 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," Dec. 2009, online, Internet, 22 Jun. 2018., Available: https://www.ipa.go.jp/security/english/vuln/200912_myjvn_cc_en.html.

new as a ministry. Most importantly, as discussed earlier the two ministries had formed an alliance with one another over cybersecurity policy, which gave them a great advantage when pushing their views.[59]

Both MIC and METI are further strengthened by overseeing incorporated administrative agencies which perform specific cyber-security-related functions. These are staffed with experts, providing a source of expertise for policy advice and for proper implementation of policy. 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.[60] 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.[61]

NPA was also a skilled bureaucratic actor with its own experts in cybersecurity, but lacked the connections with the private sector that MIC and METI could leverage to push their own policies. MOD was even weaker. It was 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). It was primarily staffed with bureaucrats from other ministries, which greatly reduced its political power. In 2007, however, the Diet passed legislation

---

[59] Interview with MIC official, Tokyo, July 2017. See also Tsuchiya, "Cyber Security Governance in Japan.".

[60] National Institute of Information and Communications Technology, "About NICT NICT Charter NICT-National Institute of Information and Communications Technology," n.d., online, Internet, 24 Mar. 2017., Available: https://www.nict.go.jp/en/about/charter.html.

[61] Information-technology Promotion Agency, "IPA Information-technology Promotion Agency, Japan : IPA:Business Outline," n.d., online, Internet, 24 Mar. 2017., Available: http://www.ipa.go.jp/english/about/outline.html.

establishing MOD as a cabinet ministry.[62] This strengthened it, but it was not yet an experienced player in bureaucratic politics.

Moreover, MOD did not have a strong network of experts in the private sector to draw upon, nor did it have much expertise of its own. It was not until 2014, well after this period, that MOD created a Cyber Defense Unit.[63] MOD was also highly restricted in terms of playing a role in implementing policy. 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.[64] Since most cyber operations are below the threshold of an armed attack, the SDF has little leeway to act.[65] Short of an actual armed attack against Japan, the MOD would not be involved in protecting cybersecurity other than its own. On top of this, while MOD and NPA did not always agree with METI and MIC, neither were their interests entirely aligned with one another: MOD was mainly concerned with protecting the Self-Defense Forces' networks, and NPA was mainly concerned with catching criminals.[66] Thus, they did not form the same kind of alliance that was formed between MIC and METI.

There are also examples of explicit political conflict over policy during this time. For example, MIC and NPA disagreed over whether internet service providers should be required to hold onto meta-data. While data is the content of internet communications, meta-data is the

---

[62] Yuki Tatsumi, *Japan's national security policy infrastructure: Can Tokyo meet Washington's expectation?* (Washington, DC: Henry L. Stimson Center, 2008).

[63] Ministry of Defense, "Establishment of the Cyber Defense Unit," *Japan Defense Focus*52 (2014), online, Internet, 16 Apr. 2017., Available: http://www.mod.go.jp/e/jdf/sp/no52/sp_activities.html#article03.

[64] Tsuchiya, "Cyber Security Governance in Japan.".

[65] Mihoko Matsubara, "How Japan's Pacifist Constitution Shapes Its Approach to Cyberspace," *Council on Foreign Relations*, May. 2018, online, Internet, 15 Jul. 2018., Available: https://www.cfr.org/blog/how-japans-pacifist-constitution-shapes-its-approach-cyberspace.

[66] Author's interviews with NISC official, Tokyo, July 2017.

information about the communications themselves: the time they were sent, the computer they were sent from, the computer they were sent to, the time they were received, and so forth. The NPA saw this meta-data as valuable evidence in prosecuting cyber-crime, but it is not easy for the NPA to get its hands on this data. Under Japanese law, the NPA can request that an ISP preserve specified traffic data. In order to make such a request, the NPA must identify the IP addresses—the numbers assigned to a particular computer or subnet on the internet—of people suspected of cybercrime. Much as with obtaining a warrant for a wiretap, the data is only collected after initial evidence of a potential crime has been collected. The problem is that once the NPA has evidence that a cybercrime has occurred, it cannot go back and look at the old meta-data to provide supporting evidence of that crime, because the ISP is under no obligation to store that data. It can only obtain meta-data related to future crimes committed by the suspects. In order to overcome this problem, the NPA would have liked (and in fact, would still like) to establish rules that require ISPs to retain meta-data for a given amount of time for all users without a request from the NPA. Then, if evidence of a crime arises, the NPA could retrieve the meta-data related to this crime.[67] The MIC, however, opposed this idea. MIC worried that this would pose too much of a burden on ISPs and that this would be a violation of privacy, as guaranteed by the constitution. The MIC successfully used its political power to block any such measures[68]

In some ways, this fits with what we expect: ideas matter more in this period thanks to the institutionalization of cybersecurity policy-making. What we do not see, however, is any shift toward consensus over this period. The 2009 National Strategy reflects the same basic priorities

[67] Author's interview with NPA official, Tokyo, July 2017.
[68] Author's interviews with NPA and MIC officials, Tokyo, July 2017.

as the 2006 Strategy, and the ideas of MIC and METI continue to dominate throughout this period. One reason this could be the case is that NISC does not truly operate as its own institution: its non-technical staff is seconded there, and retain their primary loyalty to their own ministries and agencies. Thus, we do not see the sort of socialization we would normally anticipate would occur among members of the same institution. That having been said, the policy disagreements during this period were handled relatively quietly during this period, as opposed to the all-out turf wars that were a hallmark of earlier decades of policy-making. Energy still mattered to the outcome, but not quite to the same degree—and not nearly as much of it was brought to bear. Thus, we can perhaps say this is a period in which a "semi-cognitive" political mode best explains the policy process.

2011–2016

Beginning in the 2010s, new events demonstrated that cybersecurity was still a challenge for Japan. In 2011, Japan's largest defense contractor, Mitsubishi Heavy Industries Ltd., was breached by Chinese hackers. The hackers were able to access classified submarine, missile, fighter jet, and nuclear power plant data.[69] In 2011, a server of the Lower House was penetrated and the passwords of all of the members were stolen. Japan's embassies and consulates were also attacked. In 2013, the Japanese government was the target of around 5 million cyber attacks.[70]

[69] Jeff Kingston, "Japan's cybersecurity upgrade — too little, too late?" *The Japan Times*, May. 2016, online, Internet, 15 Nov. 2016., Available: http://www.japantimes.co.jp/opinion/2016/05/21/commentary/japans-cybersecurity-upgrade-little-late/; Tsuchiya, "Cyber Security Governance in Japan.".

[70] Tsuchiya, "Cyber Security Governance in Japan.".

Most dramatically, in 2015, the Japan Pension Service was hacked into, and the data of 1.2 million users was exposed.[71]

These shocks caused the Diet to become truly involved in cybersecurity for the first time. In particular, Hirai Takuya, an LDP member of the Lower House who also served as chariman of the LDP's IT Strategy Special Committee, decided that a Basic Law needed to be passed in order to better equip the government to deal with cybersecurity. Though he was a member of the LDP, Hirai was not a member of the Abe Cabinet. Hirai worried that a proposal coming from the Cabinet would be too associated with the Abe administration's efforts to strengthen Japan's security posture—an agenda surrounded by no small amount of controversy—and that this would politicize the issue. Hirai felt that in order for the law to be truly successful, he would need to build consensus around it. Thus, while he and his committee did receive input from NISC, the bill was submitted by him and not by the administration. His efforts in consensus-building were successful: in 2014, the bill passed with the support of almost all lawmakers, including those in the DPJ, the main opposition party at the time. Indeed, the only lawmakers to vote against were those in the Social Democratic Party and the Communist Party.[72].

The Basic Cybersecurity Act made one very important set of changes: it restructured and strengthened the cabinet bodies responsible for cybersecurity. The ISPC was replaced with the Cyber Security Strategic Headquarters (CSSH). While the ISPC had been located under the IT Strategic Headquarters, the CSSH was placed directly under the authority of the Prime Minister, on par with the IT Strategic Headquarters. Moreover, the CSSH was given its which has its own

---

[71] Kingston, "Japan's cybersecurity upgrade — too little, too late?".

[72] Tsuchiya, "Cyber Security Governance in Japan"; Japan House of Representatives, "衆法 第186回国会 35 サイバーセキュリティ基本法案," 2014, online, Internet, 24 Jun. 2018., Available: http://www.shugiin.go.jp/internet/itdb_gian.nsf/html/gian/keika/1DBB2DA.htm

Minister of State in charge of cybersecurity. Beyond this, the composition of the CSSH was largely unchanged from the ISPC, though an additional expert member was added.[73]

At the same time, NISC was renamed the National center of Incident readiness and Strategy for Cybersecurity. Its composition also remained unchanged, but it was granted a great deal more authority than had previously been the case. Prior to the Basic Cybersecurity Act, NISC could do no more than create cybersecurity policy; it had no actual ability to implement the policy. Now, NISC was given the ability to request information from other parts of governments and to request cooperation to fulfill its functions. It was now also authorized to advise other ministries and agencies about cybersecurity. NISC was also clearly given responsibility to monitor illegal activities targeted at government networks. Beyond these specifics, the Act also gave a clear legal basis for NISC, which strengthened its jurisdiction.[74]

Hoewever, the original Basic Cybersecurity Law only gave NISC these abilities with regard to organizations that were clearly part of the government. Semi-public organizations, such as the Japan Pension Service, were not included within the bounds of its authority. The subsequent hack on the Japan Pension Service quickly demonstrated to lawmakers that the Act

---

[73] 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]*, November 2016, online, Internet, 21 Nov. 2016., Available: 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]," Feb. 2015, online, Internet, 24 Mar. 2017., Available: 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]," Apr. 2016, online, Internet, 24 Mar. 2017., Available: http://www.nisc.go.jp/conference/cs/pdf/meibo.pdf; Ryusuke Masuoka and Tsutomu Ishino, *Cyber Security in Japan (v.2)* (Center for International Public Policy Studies, December 2012), online, Internet, 20 Nov. 2016., Available: http://www.cipps.org/group/cyber_memo/003_121204.pdf.

[74] Cabinet Secretariat of Japan, "内閣官房組織令（抄） [order for the organization of the cabinet secretariat (excerpt)]," n.d., online, Internet, 23 Mar. 2017., Available: http://www.nisc.go.jp/law/pdf/soshikirei.pdf; Tsuchiya, "Cyber Security Governance in Japan.".

had not gone far enough, and thus it was amended to give NISC authority with regard to semi-public organizations as well.[75]

Beyond this, the Basic Cybersecurity Act mainly reaffirmed in law what had already been prioritized in the national cybersecurity policies. The provisions are by-and-large broadly worded, and discuss coordination between the central government, local governments, and critical infrastructure operators; recognizes that the government must take measures to implement cybersecurity policies; that the government must work to prevent and respond to cybercrime; that the government should promote private-sector cybersecurity and research into cybersecurity; and that the Japanese government should work with other governments to promote cybersecurity.[76] The law was important, however, in helping to legitimize those policies by giving them a clear legal basis.

Within NISC and the Cyber Security Strategic Headquarters, policy-making continued much as before, with a heavy emphasis on economic security and critical infrastructure. The government continued to promote information sharing and to produce guidelines aimed at businesses. 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. These provisions were aimed explicitly at improving the cybersecurity of these firms.[77] In the wake of STUXNET (which damaged Iran's nuclear centrifuges) and the 3/11 earthquake and tsunami, which demonstrated the effects damage to infrastructure could have on Japan's economy and public safety, in 2012 METI established the Control System

---

[75] Tsuchiya, "Cyber Security Governance in Japan.".

[76] "サイバーセキュリティ基本法 [cyber security basic law]," Apr. 2016, online, Internet, 23 Mar. 2017., Available: http://law.e-gov.go.jp/htmldata/H26/H26HO104.html.

[77] 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.

Security Center (CSSC) to promote the security of control systems, which are vital for critical infrastructure.[78]

However, there were some indications that NPA and MOD were beginning to have more influence in this area. For example, in 2013, Japan began being hit by VAWTRAK, a cyber banking scheme that worked by infecting computers with malware. At one point, 44,000 computers in Japan were infected with the malware.[79] 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 would provide lists of these IP addresses to the appropriate ISPs who could inform their users as to how to remove the malware. This had the support of the NPA, but as was the case with the rules for storing meta-data, MIC initially objected on the basis of user privacy. In this case, however, the police won out, and the system was implemented.[80]

Likewise, in 2014 MOD 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.[81] Though the unit was small, with around 110

---

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

[79] Danielle Anne Veluz, "VAWTRAK Plagues Users in Japan - Threat Encyclopedia - Trend Micro AU," Jun. 2014, online, Internet, 1 Aug. 2018., Available: 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," *RT International*, Apr. 2015, online, Internet, 1 Aug. 2018., Available: https://www.rt.com/news/248673-japan-vawtrak-bank-infect/.

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

[81] Ministry of Defense, "Establishment of the Cyber Defense Unit.".

members in 2016, it nevertheless gave the MOD some much-needed expertise, and has the potential to grow in the future.[82]

What is interesting about this time period is that, despite a series of crises, the nature of Japanese cybersecurity policy-making did not change. Indeed, what is interesting is that in the Diet, where we might have most expected to see the political mode apply, one instead finds a process that looks far more like the cognitive mode: a careful attempt to pursuade and build consensus around a particular policy solution. By contrast, at the bureaucratic level, the political mode that was evident in the previous period continued, with some shifting in the "energy" held by each of the actors leading to some changes in policy, albeit relatively low-key ones. What is interesting is that the crises did in some sense break the consensus around existing cybersecurity policy and brought a new set of actors (the members of the Diet) into cybersecurity policy-making, but within the Diet a new consensus around strengthening the existing institutional structures was quickly reached. Given that the institutional structures governing the bureaucracy were left unchanged, it is unsurprising that policy-making at this level continued on much as before. This suggests two things relative to the theory posited in Section 2: first, that while crises do apparently promote policy change, they do not *necessarily* lead to the conflict between ideas that is fundamental to the political or artifactual modes; and second, that different modes can be operative simultaneously in different policymaking arenas (in this case, the Diet versus the bureaucracy).

---

[82] Franz-Stefan Gady, "Japan's Defense Ministry Plans to Boost Number of Cyber Warriors," *The Diplomat* (2017), online, Internet, 2 Aug. 2018., Available: https://thediplomat.com/2017/07/japans-defense-ministry-plans-to-boost-number-of-cyber-warriors/.

Conclusion

Building upon John Campbell's synthesized theory of policy-making, this paper has proposed the theory that two factors can determine whether energy or ideas will be important in determining policy, and thus which mode of policy-making will be applicable to the situation: the level of consensus around an issue area, and the degree of institutionalization of the policy-making process. It has posited that consensus makes energy less important to the outcome, and that exogenous shocks that break this consensus should thus make energy more important. Further, it has posited that because institutionalization socializes actors within the institutions, institutions should build consensus and reduce the importance of energy. Finally, it argues that institutionalization fixes membership in policy-making and makes preferences clearer, increasing the importance of ideas in the policy-making process.

Applying this theory to the history of Japanese cybersecurity policy-making, the results are decidedly mixed. There seems to be a fair bit of support for the proposition that institutionalization makes ideas more important: in the earliest period, when there were not yet established institutions for Japanese cybersecurity policy-making, policy-making operated within the artifactual mode, in which only energy is important; after institutionalization, it operated in either the political or cognitive modes, as expected. Morover, the attacks on government websites in the late-1990s and early-2000s broke consensus as expected, and energy played a key role in this early round of policy-making.

However, institutionalization did not lead to the anticipated building of consensus. Instead, the four main bureaucratic actors involved in cybersecurity policy-making, METI, MIC, MOD, and NPA, continued to push for their own preferred policies, and the amount of energy

they could bring to bear does seem to account for the outcomes during the second two periods. One possibility is that the nature of the institutions created matters: the bureaucrats in NISC are seconded from these other organizations, and therefore likely continue to see themselves as representing their own organizations' interests rather than as members of the same team.

Likewise, the second set of crises in the 2010s did not, as anticipated, lead to the political mode of policy-making. Though these crises did create momentum for the Diet to act, the policy deliberation within the Diet most resembled the cognitive mode, in which persuasion played a key role and consensus was quietly built. The result was a strengthening of existing policy-making structures and the legitimation of existing policies, rather than a fundamental rethinking of cybersecurity policy.

In conclusion, this new theory seems like a step forward, particularly in understanding when ideas matter in policy-making, but requires further refinement. Obvious next steps are to consider the nature of institutions and what effect this has on consensus-building, and whether exogenous shocks are likely to lead to a breakdown in consensus or a reinforcement thereof.

Tables

	Ideas Matters		
Energy Matters		yes	no
	yes	political	artifactual
	no	cognitive	inertial

Table 1: Four sources of policy change, from Campbell, How Policies Change.

Time Period	Shocks	Institutionalized	Mode
1999–2005	yes	No	Artifactual
2006–2013	no	Yes	political to cognitive
2013–2016	yes	Yes	Political

Table 2: Anticipated Japanese cybersecurity policy change over time.

Bibliography

Allison, Graham. *Essence of Decision*. Little, Brown, 1971.

Arimura, Kouichi. "Anti-Bot Countermeasures in Japan," Mar. 2008. Online. Internet. 17 Oct. 2017. Available: http://www.nca.gr.jp/jws2008/WS1-ccc.pdf.

Cabinet Secretariat of Japan. "内閣官房組織令（抄） [order for the organization of the cabinet secretariat (excerpt)]," n.d. Online. Internet. 23 Mar. 2017. Available: http://www.nisc.go.jp/law/pdf/soshikirei.pdf.

Campbell, John Creighton. *How policies change: The japanese government and the aging society*. Princeton University Press, 2014.

Campbell, John L. "Institutional Analysis and the Role of Ideas in Political Economy." *Theory and Society* 27.3 (1998): 377–409.

Cohen, Michael D., James G. March, and Johan P. Olsen. "A garbage can model of organizational choice." *Administrative Science Quarterly* 17.1 (1972): 1–25.

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]," Feb. 2015. Online. Internet. 24 Mar. 2017. Available: http://www.nisc.go.jp/conference/cs/dai01/pdf/01gijigaiyou.pdf.

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

Goldstein, Judith. "The Political Economy of Trade: Institutions of Protection." *The American Political Science Review* 80.1 (1986): 161–184.

Hall, Peter A. "Policy Paradigms, Social Learning, and the State: The Case of Economic Policymaking in Britain." *Comparative Politics* 25.3 (1993): 275–296. Online. Internet. 21 May. 2018.

Ikenberry, G. John. "The Irony of State Strength: Comparative Responses to the Oil Shocks in the 1970s." *International Organization* 40.1 (1986): 105–137.

Information Security Policy Council. "Action Plan on Information Security Measures for Critical Infrastructures," Dec. 2005. Online. Internet. 19 May. 2018. Available: http://www.nisc.go.jp/eng/pdf/actionplan_ci_eng.pdf.

———. “The First National Strategy on Information Security,” Feb. 2006. Online. Internet. 14 May. 2018. Available: https://www.nisc.go.jp/eng/pdf/national_strategy_001_eng.pdf.

———. “The Second National Strategy on Information Security,” Feb. 2009. Online. Internet. 14 May. 2018. Available: https://www.nisc.go.jp/eng/pdf/national_strategy_002_eng.pdf.

———. “新・情報セキュリティ普及啓発プログラム [New Information Security Public Awareness Program],” Jul. 2014. Online. Internet. 14 Feb. 2018. Available: http://www.nisc.go.jp/active/kihon/pdf/awareness2014.pdf.

Information-technology Promotion Agency. “2010 Smart Home Appliance Security Study Report,” Jan. 2011. Online. Internet. 22 Jun. 2018. Available: https://www.ipa.go.jp/files/000014115.pdf.

———. “IPA Information-technology Promotion Agency, Japan: IPA: Business Outline,” n.d. Online. Internet. 24 Mar. 2017. Available: http://www.ipa.go.jp/english/about/outline.html.

———. “IPA Information-technology Promotion Agency, Japan: IPA/ISEC： Vulnerabilities： ‘MyJVN Security Configuration Checker’ released,” Dec. 2009. Online. Internet. 22 Jun. 2018. Available: https://www.ipa.go.jp/security/english/vuln/200912_myjvn_cc_en.html.

———. “JVN iPedia - Vulnerability Countermeasure Information Database / What is JVN iPedia?” n.d. Online. Internet. 22 Jun. 2018. Available: https://jvndb.jvn.jp/en/nav/jvndb.html.

———. “Outline of Information Security Benchmark (ISM-Benchmark),” 2007. Online. Internet. Available: https://www.ipa.go.jp/files/000011798.pdf.

Ito, Yurie, Greg Rattray, and Sean Shank. “Japan’s Cyber Security History.” In *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, edited by Jason Healey. Cyber Conflict Studies Association, 2013.

Japan House of Representatives. “衆法 第186回国会 35 サイバーセキュリティ基本法案,” 2014. Online. Internet. 24 Jun. 2018. Available: http://www.shugiin.go.jp/internet/itdb_gian.nsf/html/gian/keika/1DBB2DA.htm.

Johnson, Chalmers. “MITI, MPT, and the Telecom Wars.” In *Politics and Productivity: How Japan’s Development Strategy Works*, edited by Chalmers Johnson, Laura D’Andrea Tyson, and John Zysman, 177–240. Ballinger Publishing Company, 1989.

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],” n.d. Online. Internet. 16 Apr. 2017. Available: http://www.jpcert.or.jp/about/05.html.

Katzenstein, Peter J. “Conclusion: Domestic structures and strategies of foreign economic policy.” *International Organization* 31.4 (1977): 879–920.

———. “Same War: Different Views: Germany, Japan, and Counterterrorism.” *International Organization* 57.4 (2003): 731–760.

Kingdon, John W. *Agendas, Alternatives, and Public Policies*. vols. 2nd ed. HarperCollins College Publishers, 1995.

Kingston, Jeff. “Japan’s cybersecurity upgrade — too little, too late?” *The Japan Times*, May. 2016. Online. Internet. 15 Nov. 2016. Available: http://www.japantimes.co.jp/opinion/2016/05/21/commentary/japans-cybersecurity-upgrade-little-late/.

Kitahara, Munenori. “Information society law in japan.” *US-China Law Review*1 (2011): 21–40.

Krebs, Brian. “Talking Bots with Japan’s ‘Cyber Clean Center’ — Krebs on Security,” Mar. 2010. Online. Internet. 16 Oct. 2017. Available: https://krebsonsecurity.com/2010/03/talking-bots-with-japans-cyber-clean-center/.

March, James G., and Johan P. Olsen. “The new institutionalism: Organizational factors in political life.” *The American Political Science Review* 78.3 (1984): 734–749.

March, James G., and Herbert Alexander Simon. *Organizations*. Wiley, 1958.

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

Matsubara, Mihoko. “How Japan’s Pacifist Constitution Shapes Its Approach to Cyberspace.” *Council on Foreign Relations*, May. 2018. Online. Internet. 15 Jul. 2018. Available: https://www.cfr.org/blog/how-japans-pacifist-constitution-shapes-its-approach-cyberspace.

Ministry of Defense. “Establishment of the Cyber Defense Unit.” *Japan Defense Focus*52 (2014). Online. Internet. 16 Apr. 2017. Available: http://www.mod.go.jp/e/jdf/sp/no52/sp_activities.html#article03.

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)],” 2010. Online. Internet. 18 Nov. 2017. Available: https://www.mof.go.jp/tax_policy/tax_reform/outline/fy2010/explanation/PDF/08_P350_420.pdf.

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]*, November 2016. Online. Internet. 21 Nov. 2016. Available: 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 [cyber security strategic headquarters]," n.d. Online. Internet. 16 Jul. 2018. Available: http://www.nisc.go.jp/conference/cs/index.html.

———. "サイバーセキュリティ戦略本部　名簿 [cyber security strategic headquarters, register of names]," Apr. 2016. Online. Internet. 24 Mar. 2017. Available: http://www.nisc.go.jp/conference/cs/pdf/meibo.pdf.

National Institute of Information and Communications Technology. "About NICT NICT Charter NICT-National Institute of Information and Communications Technology," n.d. Online. Internet. 24 Mar. 2017. Available: https://www.nict.go.jp/en/about/charter.html.

National Police Agency. "警察庁　総合セキュリティ対策会議　概要 [National Police Agency - Coordinated Security Measures Council - Summary]," 2001. Online. Internet. 11 Jul. 2019. Available: http://www.npa.go.jp/cyber/csmeeting/h13/pdf/h13gaiyou.pdf.

Office of the Prime Minister of Japan. "情報セキュリティ関係省庁局長等会議の設置について [About the Establishment of the Conference of Ministries and Agencies Related to Information Security]," n.d. Online. Internet. 19 Jun. 2018. Available: https://www.kantei.go.jp/jp/it/security/taisaku/0917kyokutyou.html.

Ostrom, Elinor. "Institutional rational choice: An assessment of the institutional analysis and development framework." In *Theories of the policy process*, 21–64. 2nd ed. Cambridge, MA: Westview Press, 2007.

Sabatier, Paul A., and C.M. Weibel. "The advocacy coalition framework: Innovations and clarifications." In *Theories of the policy process*, 189–220. 2nd ed. Cambridge, MA: Westview Press, 2007.

Schaede, Ulrike. "From developmental state to the 'New Japan': The strategic inflection point in Japanese business." *Asia Pacific Business Review* 18.2 (2012): 167–185.

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

Skocpol, Theda, and Kenneth Finegold. "State capacity and economic intervention in the early new deal." *Political Science Quarterly* 97.2 (1982): 255–278.

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?" n.d. Online. Internet. 16 Oct. 2017. Available: https://www.telecom-isac.jp/ccc/en_index.html.

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," Jun. 2014. Online. Internet. 1 Aug. 2018. Available: https://www.trendmicro.com/vinfo/au/threat-encyclopedia/web-attack/3141/vawtrak-plagues-users-in-japan.

Weatherford, M. Stephen, and Haruhiro Fukui. "Domestic Adjustment to International Shocks in Japan and the United States." *International Organization* 43.4 (1989): 585–623.

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.

Wildavsky, Aaron. "Choosing preferences by constructing institutions: A cultural theory of preference formation." *The American Political Science Review* 81.1 (1987): 4–21.

Zachariadis, N. "The multiple streams framework: Structure, limitations, prospects." In *Theories of the policy process*, 65–92. 2nd ed. Cambridge, MA: Westview Press, 2007.

"82,000 PCs in Japan, worldwide infected with virus harvesting banking passwords." *RT International*, Apr. 2015. Online. Internet. 1 Aug. 2018. Available: https://www.rt.com/news/248673-japan-vawtrak-bank-infect/.

"サイバーセキュリティ基本法 [cyber security basic law]," Apr. 2016. Online. Internet. 23 Mar. 2017. Available: http://law.e-gov.go.jp/htmldata/H26/H26HO104.html.

情報セキュリティ対策推進会議 [Council for the Promotion of Cybersecurity Measures]. "情報セキュリティ対策推進会議について [About the Council for the Promotion of Information Security Measures]," Jul. 2005. Online. Internet. 18 Jul. 2019. Available: https://www.nisc.go.jp/conference/suishin/ciso/pdf/konkyo.pdf.

———. “重要インフラのサイバーテロ対策に係る特別行動計画　[Special Action Plan for Responding to Cyberterrorism on Critical Infrastructure],” Dec. 2000. Online. Internet. 18 Jul. 2019. Available: https://www.nisc.go.jp/active/sisaku/2000_1215/pdf/txt3.pdf.

総合セキュリティ対策会議 [Coordinated Security Measures Council]. “情報セキュリティ対策における連携の推進について [About the Coordinated Promotion of Information Security Measures],” Mar. 2002. Online. Internet. 11 Jul. 2019. Available: http://www.npa.go.jp/cyber/csmeeting/h13/pdf/pdf13a.pdf.

———. “第 1 回総合セキュリティ対策会議　発言要旨　[The First Meeting of the Coordinated Security Measures Council - Summary of Remarks],” Dec. 2001. Online. Internet. 11 Jul. 2019. Available: http://www.npa.go.jp/cyber/csmeeting/h13/pdf/h13youshi1.pdf.