A Comparative Study of the Information Security Policies of Japan and the United States

Yasuhide Yamada,* Atsuhiro Yamagishi** & Ben T. Katsumi***

INTRODUCTION

This article describes the information security policies and institutions of the Japanese government and draws attention to comparable policies and institutions of the U.S. government. We begin with a discussion of Japan's cybersecurity system. In Part II, we examine a particular type of information security policy, namely, cryptography policy, as a special example of how the different systems operate. Japan has implemented a cryptography policy that draws extensively on the Organization for Economic Cooperation and Development (OECD) Cryptography Policy Guidelines. These guidelines are discussed to highlight issues that might emerge in the future in cryptography and merit attention at an international level. Part III analyzes anti-bot policy. Bots, an increasing concern on the Internet, break into an individual user's PC and remotely control it. Bots pose a real problem for many nations, and there is clearly a need for multinational cooperation. This article concludes by suggesting that all involved parties must determine the appropriate extent of lawful access to communications. Moreover, cooperation in eliminating bots provides a good opportunity for Japan and the United States to lead an international effort.

I. JAPAN'S CYBERSECURITY SYSTEM

After studying the overall cybersecurity plans of Japan[1] and the United States,[2] we have concluded that the United States has an advantage over

* Yasuhide Yamada is Director of Information Security Policy, Ministry of Economy, Trade, and Industry (METI), and formerly Managing Director, Information Security Center, Information Technology Promotion Agency (IPA). The views expressed in this article are not necessarily those of the authors' respective organizations or partner organizations.

** Atsuhiro Yamagishi is Group Leader of Cryptography, Information Security Center, IPA.

*** Ben T. Katsumi is Researcher, Information Security Center, IPA.

1. SECURE JAPAN 2009: ALL ENTITIES SHOULD ASSUME THEY MAY BE SUBJECT TO ACCIDENTS, *English version, translated from Japanese, available at* http://www.nisc.go.jp/eng/pdf/sj2009_eng.pdf. The Japanese government announced this cybersecurity policy package on June 22, 2009, midway through the Second National Strategy on Information Security, discussed later in this article. For previous strategies and related documents in English, see the NISC's website at http://www.nisc.go.jp/eng/index.html.

2. CYBERSPACE POLICY REVIEW: ASSURING A TRUSTED AND RESILIENT INFORMATION

Japan in public awareness about national cyber defense, political commitment to national security, and the creation of a government structure for promoting cybersecurity. Japan, by contrast, seems to be superior in protecting personal information and in focusing on information security awareness and awareness-raising programs. This article explores these strengths and other elements in the Japanese context and draws comparisons to the U.S. system.

A. Organizational Structure

Japan's cybersecurity center is the National Information Security Center (NISC), a part of the Cabinet Secretariat. The head of the NISC is one of three Assistant Chief Cabinet Secretaries. This official has dual responsibilities for national security and emergency response systems, including physical security and cybersecurity. Policy questions are decided by the Information Security Policy Council (ISPC),[3] which is chaired by a Chief Cabinet Secretary. Under the ISPC's formal direction and in cooperation with the NISC, policies are carried out by the ministries and agencies. The main ministries that serve under the NISC are the Ministry of Internal Affairs and Communication (MIC), the Ministry of Economy, Trade, and Industry (METI), the National Police Agency (NPA), and the Ministry of Defense (MOD).

The prominence of Japan's NISC and its leadership indicates the extent of its powers. The NISC was established in 2000 as the Information Security Measures Promotion Office, but in 2005, after restructuring, it became the NISC. Its status confers transparency of organizational effects, but this status also suggests a lack of flexibility in prioritization of a cybersecurity agenda. Cybersecurity is not considered a top priority political issue, like the national pension program or a serious earthquake damage recovery program.

Stable organizational structure, continuous empowerment, and consistent service by well qualified personnel have led to a steady evolution of the Japanese information security policy and administration. The "anchor" person at the NISC is the Advisor on Information Security (referred to here as the Advisor). Since the creation of the position in April 2004, the same official, Suguru Yamaguchi, has served as the Advisor. His personal stature has provided significant importance to the NISC, which previously was an assemblage of bureaucrats who were not necessarily cybersecurity specialists. Under the direction of the Advisor, the NISC has assumed responsibility for (1) interpretation of complicated technical

---

AND COMMUNICATIONS INFRASTRUCTURE (2009), *available at* http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

3. Organizationally, the Information Security Policy Council (ISPC) falls under the Information Technology (IT) Strategy Headquarters. The IT Strategy Headquarters is chaired by the Prime Minister and managed by an Assistant Chief Cabinet Secretary.

issues, (2) transformation of technical and managerial issues into policies and directives, and (3) coordination of the political debate concerning emerging cybersecurity measures.

In comparing Japan's organizational structure with that of the United States, we find instructive differences. Typically, the U.S. organizational models are dynamic, while the Japanese models tend to be more static, a difference that may reflect the countries' respective historical, cultural, and social identities.

A comparison may be drawn between the NISC with its U.S. counterpart, the National Cybersecurity Division (NCSD) in the Department of Homeland Security (DHS). The administrative function of the NCSD has been in flux since it was created in 2003. In contrast, the role and size of the NISC have been consistently developing. The NISC is more active in the bureaucratic arena, and so far that has been to its advantage. Thus the NISC has managed to handle the potential friction of trying to maintain information technology (IT) convenience, the privacy of IT users, corporate business continuity, and the needs of criminal investigation and national defense.

B. Cybersecurity Strategy

In February 2009, the Japanese government adopted the Second National Strategy on Information Security (NSIS) for the years 2009 through 2011.[4] The three year plan includes four subjects: central and local governments, critical infrastructure, business entities, and individuals.

As part of the NSIS process, the Japanese government adopted "Secure Japan 2009."[5] One-fourth of its 212 policy items are aimed at the improvement of central and local governments. In the areas devoted to critical infrastructure and business entities, private enterprises serve as the subjects of its actions while the government provides support. Like in the United States, the critical infrastructures are owned and operated by members of the private sector, and this public-private partnership is considered very important. Both the MIC and the METI set up grassroots IT security "classrooms" all over the country to leverage efforts of local not-for-profit organizations. These ministries also conduct effective national campaigns to promote security awareness.

By contrast, many of the U.S. policies have focused on enhancement of the federal government's cybersecurity, and few have been employed to work in the private sector. While a full discussion of the U.S. cybersecurity policies is beyond the scope of this article, an example of the U.S. policy balance can be shown by the Comprehensive National Cybersecurity

4. THE SECOND NATIONAL STRATEGY ON INFORMATION SECURITY: AIMING FOR STRONG "INDIVIDUAL" AND "SOCIETY" IN THE IT AGE (2009), *English version, translated from Japanese, available at* http://www.nisc.go.jp/eng/pdf/national_strategy_002_eng.pdf.

5. SECURE JAPAN 2009, *supra* note 1.

Initiative (CNCI)[6] implemented under former President George W. Bush. The CNCI focused on enhancement of cybersecurity capabilities in the federal government, and only a few of the policies were aimed at nonfederal cybersecurity. The Japanese, however, seem more committed to private and civil activities, while U.S. policies promote high level national objectives. A possible reason for the disparity in the United States is that the federal government is focused on federal issues while state and local governments are more directly connected to citizens and corporations. Conversely, the Japanese government tends to be more involved in industry and with the general public.

C. Reporting and Monitoring

In the executive branch, the U.S. National Institute of Standards and Technology (NIST) is an independent standards-dedicated entity. Under the Federal Information Security Management Act (FISMA), the NIST provides standards, rules, and guidelines while the office of Management and Budget does monitoring and reporting. The Inspector General and the Government Accountability Office play independent roles for auditing purposes.

In comparison, Japan assigns all such roles to the NISC, as discussed below. The Japanese relationship between its Congress and Executive body may have a positive effect on consistency and efficiency, but the authors believe that the Japanese government might learn from the U.S. approaches in such areas as segregation of duty, continuous monitoring, and a national auditing mechanism.

In 2005, under the first NSIS, the NISC developed governmental standards for information security measures for the central government computer systems,[7] and distributed these standards to all Japanese national governing bodies. This list of security management and administration objectives and practices has been revised almost every year and is now in its fifth version.

The NISC performs all measuring and reporting from a template that it delivers to ministries and agencies. The template provides thirty-six

---

6. The CNCI designated 12 initiatives, such as (1) moving toward managing a single federal enterprise network, (2) connecting current government cyber operation centers, and (3) developing multi-pronged approaches to supply risk management. Many of these are described as joint efforts by two departments or agencies, and many agencies are involved under the coordination of the Director of National Intelligence. *See* Wyatt Kash, *Details Emerge About President's Cyber Plan,* GOV'T COMPUTER NEWS, NOV. 21, 2008, *available at* http://gcn.com/Articles/2008/11/21/Details-emerge-about-Presidents-Cyber-Plan.aspx?Page=1. A declassified summary was recently released by the White House. *See* Comprehensive National Cybersecurity Initiative (March 2010), *available at* http://www.whitehouse.gov/cyber security/comprehensive-national-cybersecurity-initiative.

7. STANDARDS FOR INFORMATION SECURITY MEASURES FOR THE CENTRAL GOVERNMENT COMPUTER SYSTEMS (2005) *English version, translated from Japanese, available at* http://www.nisc.go.jp/eng/pdf/full1_sism_g_eng.pdf.

questions and a check-list of items in ten subcategories divided into four areas: planning, knowledge-sharing, execution, and evaluation and improvement. The template includes items such as education for IT security supervisors, compilation and maintenance of information asset lists, and incident handling manuals. The NISC then rates the reported activities with single, double, and triple stars.[8] In comparison, the United States has a multilevel grading system that government branches use to self-report.

The NISC has identified several "best practice" areas.[9] Using the NISC's template, ministries and agencies report their best practices annually to Japan's IT Strategy Headquarters. Thus through reporting and monitoring and consistent application of standards, government bodies have made tremendous improvements in overall security levels of Japanese government systems.

D. Summary

There are many similarities between Japan's cybersecurity system and that of the United States in terms of setting standards, monitoring, and reporting. Both governments apply almost the same bases for their government's cybersecurity but, interestingly, under very different systems. Below are some specific observations.

The NISC has been consistent in its commitment to improve the security measures of Japan's ministries and agencies, but challenges lie ahead. The NISC has performed rulemaking, orders, monitoring, and performance evaluations. Its efforts have resulted in an increase in productivity in just four years of work. However, the NISC will be tested when the government considers lawful access to private communications for purposes of cryptography and anti-bot policies.

Japan and the United States can learn from each other's contrasting approaches and experiences. Japan has enacted many policies and measures, but may be weak on strategy. Some may argue that the government has enacted so many, extremely precise policies that it will have difficulty implementing them in a reasonable period of time. On the other hand, some may say that U.S. policies are not precise enough; the U.S. cybersecurity approach is dominated by strategy, but its policies are so broad that they are difficult to implement. Thus Japan may learn about

8. The summary table appears (in Japanese) on the NISC's website at http://www.nisc.go.jp/conference/seisaku/dai21/pdf/21siryou0403.pdf.

9. The best practice list is available (in Japanese) at http://www.nisc.go.jp/conference/seisaku/dai21/pdf/21siryou0402.pdf. As an example of a best practice, the Ministry of Finance conducts weekly consultations with its IT staff with the objective of developing their knowledge of IT security.

strategy and vision from the United States. The United States may learn from Japan about effective grassroots programs to promote cybersecurity.

Japan can also learn from the United States about research on cybersecurity. Japan does not have funds allocated to this specific purpose. The U.S. government has traditionally been effective in using R&D funding to stimulate innovation and has established effective ways of technology expansion. The Japanese government needs to be more committed to its domestic cybersecurity industry and can learn how to do so by studying the U.S. experience.

II. CRYPTOGRAPHY POLICY

Neither the United States nor Japan has a written cryptography policy, although it is an important part of information security. In fact, the U.S. Cyberspace Policy Review does not even discuss cryptography policy.

Japanese cryptography policy is based primarily on the principles set out in the Guidelines for Cryptography Policy recommended by the OECD in 1997.[10] It was not until the 1990s that cryptography policy came to be discussed in Japan, because scientific research on cryptography was interrupted from 1945 to the mid-1970s due to Japan's recovery efforts after World War II. Electronic commerce was activated by the advent of the Internet, and with e-commerce came concern about unlawful access to the Internet. Modern cryptography research started in Japan with the the DES (Data Encryption Standard), the principle of the public key cryptosystem, and RSA, an algorithm for public key cryptography. In other words, cryptography policy was triggered by discussions regarding key recovery and key escrow and by the OECD Cryptography Policy Guidelines.

A. Cryptographic Methods (OECD Principles 1-4)

The cryptograph algorithms used by the Japanese government's online services system were selected between 2000 to 2003. This selection was conducted by the Cryptography Research and Evaluation Committee, or CRYPTREC.[11] Like the U.S. NIST, CRYPTREC adopted an open selection policy by announcing evaluation criteria, and forty-eight proposals from around the world were introduced. These proposed cryptograph algorithms and other de facto standards were evaluated by CRYPTREC. As a result,

10. For the OECD's Guidelines for Cryptography Policy, including its eight principles, see http://www.oecd.org/document/11/0,3343,en_2649_34255_1814731_1_1_1_1,00.html. The eight principles are listed in the appendix to this article. The OECD assumes that the guidelines document is read widely and practiced by both private companies and public organizations. The guidelines do not address protection of information related to national security.

11. *See generally* Cryptography Research and Evaluation Committee, http://www.cryptrec.go.jp/english/index.html.

the e-Government Recommended Ciphers List was completed in March 2003. The selection process was announced officially in its annual report to ensure transparency.

Thus the processes of cryptograph algorithms selection in the United States and Japan are similar with regard to transparency and openness. There is, however, a notable difference between Japan and the United States. Japan has not designated the selected cryptograph algorithms as the government standard cryptograph, while the United States has. Although in the U.S. government it is mandatory to use the Federal Information Processing Standard (FIPS) cipher, the Japanese government recommends selection and use of a cipher from a recommended cipher list. This different approach might simply reflect the fact that the NIST is authorized under the FISMA to select a cipher, while CRYPTREC lacks such authority under Japanese law. CRYPTREC is a "private committee" that is managed by the MIC and the METI.

Neither Japan nor the United States has compelled its private sector to use the government evaluated cryptograph. But treatment differs with respect to the use of the cryptograph within the government. The U.S. government requires that all agencies use the Federal Information Processing Standard (FIPS) cryptograph. By contrast, Japan's e-Government Recommended Ciphers List is merely an advisory reference for government offices; the list is respected, but officials may select other cryptographs.

Japan's approach to R&D in encryption technology differs from U.S. practice. In Japan, universities and companies have played a role in R&D. However, although the level of the research relating to encryption technology is high in national research institutions such as the National Institute of Advanced Industrial Science and Technology (AIST), national institutions have not reached the level of promoting R&D throughout the country. In Japan, a university, a telecommunications company, and a vendor restarted research in cryptography, stimulated by the appearance of DES and the public key cryptosystem. Therefore, one might say that there was neither political guidance nor promotion by the Japanese government in cryptography R&D.

In the United States, the federal government has taken the lead and promoted R&D because encryption technology is connected with national security. It is difficult to say that such R&D in the United States is completely driven by the market. The cryptographic hash function and key deposition cryptography were developed by the National Security Agency.

Turning to standards, U.S. practices can be contrasted with Japanese ones. The U.S. NIST creates a federal standard, and the United States proposes this federal standard to international bodies, such as the International Organization for Standardization (ISO). In Japan, the international standard for cryptography technology was adopted for the e-Government Recommended Ciphers List after CRYPTREC had evaluated

security aspects. However, since cooperation between CRYPTREC and international standards bodies is not close, Japan has been less effective in this area than the United States.[12] Another factor is that there are many academics handling Japanese cryptography and security mechanisms, but the government is barely included. Therefore, it is difficult to reflect the will of the whole industry or to define a government plan.

B. Privacy Protection, Lawful Access, and Liability (OECD Principles 5-7)

Privacy protection and lawful access are inherently in tension. The privacy protection law in Japan was enacted as the "Act on the Protection of Personal Information" in 2003. The Act defines its basic principle as follows: "In view of the fact that personal information should be handled cautiously under the philosophy of respecting the personalities of individuals, proper handling of personal information must be promoted."[13]

The law also describes the responsibilities and measures to be taken by state and local governments, administrative agencies, and business operators in handling personal information. This law is based primarily on the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.[14]

Regarding lawful access, Japan enacted the Act on Wiretapping for Criminal Investigation in 1999.[15] This law established requirements for monitoring electronic communications as well as various other procedures with the intent of protecting the secrecy of communications. However, electronic communications – for criminal or other purposes – are not monitored in any systematic indexed way, so elucidation of truth is difficult.

In Japan, interception of communications to support judicial investigations is legal, whereas interception to obtain intelligence is not. Academics have begun to discuss the latter.[16] However, Japan will have difficulty when it tries to enact measures allowing interception of

---

12. Japanese international standardization activity has been guided by efforts of the "Cryptography and Security Mechanism" working group of the "Security Techniques" subcommittee, which is one of the technical committees within the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) framework. This working group is also known as "JTC1 SC27 WG2."

13. Act on the Protection of Personal Information, Law No. 57, 2003, art. 3.

14. *See* OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA, *available at* http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00 .html.

15. Act on Wiretapping for Criminal Investigation, Law. No. 137 of 1999, *available at* http://hourei.hounavi.jp/hourei/H11/H11HO137.php (in Japanese).

16. MOTOHIRO TSUCHIYA, POLICY ISSUES ON WARRANTLESS WIRETAPPING BY THE BUSH ADMINISTRATION: CHANGES IN INTELLIGENCE COMMUNITY BY DIGITAL TECHNOLOGIES AND NETWORKS (2007) (study available in Japanese), *available at* http://officepolaris.co.jp/icp/2006paper/2006007.pdf.

communications for intelligence purposes because citizens groups and the general public are concerned about the emergence of a surveillance society.

Turning to policies affecting data confidentiality, including key escrow and key recovery policies, the authors observe pros and cons. The United States was eager to introduce such a key escrow/key recovery policy in the first half of the 1990s. The Clinton administration dispatched an ambassador-rank official responsible for cryptographic matters to various countries, asking them to align their key management policies with those of the United States. Japan also held many discussions about key escrow/key recovery. This was in the context of Japan's enactment of its Act on Wiretapping for Criminal Investigation a few years ago. No Japanese company has adopted a key escrow/key recovery policy other than as a countermeasure against the lost key problem.

Key management, which is concerned with requirements for minimum security levels, evolves into self-responsibility, with governments and organizations choosing from a range of options. Under Principle Seven of the OECD Cryptography Policy Guidelines, the OECD offers a possible solution to establish liability of individuals and organizations for confidentiality consistent with national legislation and international agreements. This might be seen as the OECD's answer to U.S. key management policy.

C. International Cryptography Policy (OECD Principle 8)

International cryptograph policy includes regulation of exports under the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies. Both Japan and the United States are participating states and thus their respective national regulations governing exports of encryption technology are the same, with one exception. The United States implemented a unique regulation called "re-export control." This rule applies to U.S. goods and foreign produced goods that are made using technology or technical data originally produced in the United States. The restriction applies regardless of whether the exporter is a U.S. entity. While a detailed discussion of this rule is beyond the scope of this article, it should be noted that now many countries beyond the United States also conduct R&D in cryptographs, and cryptograph technology has become more widely available. For this reason, it might be time that the United States reconsiders the rationale for subjecting cryptograph technology to re-export controls.

III. POLICY AGAINST BOTS

Bots are an increasing concern on the Internet. They break into an individual user's PC and remotely control it. Bots can make a PC perform actions such as sending spam emails,[17] engineering phishing or distributed denial of service (DDoS) attacks[18] against specific targets, and enabling the theft of information from targets. The majority of users owning bot-infected PCs are forced to become unwitting intermediaries for crimes and therefore become not only victims but also victimizers without realizing what is happening in their PCs. Bot-infected PCs are automatically connected to command and control (C&C) servers under a network called a botnet.[19] Under a botnet, a malicious commander known as a "herder" remotely manipulates infected PCs. About 2 to 2.5 percent of all Internet broadband users in Japan, which means 400,000 to 500,000 PCs, were estimated to be infected with bots,[20] and in the world, approximately 1.2 million PCs are reportedly infected with bots.[21]

Disinfecting bots using conventional methods, however, has become increasingly difficult because: a) many bot programs are frequently updated and released in greater volume and b) attacks by bots are performed in limited portions of programs and use stealth techniques. The bot problem remains a huge concern.

A. Japanese Model or American Model?

Japan and the United States follow very different policies concerning bots. Facing threats derived from bots, the Japanese government launched a project under the Cyber Clean Center (CCC)[22] in 2006.

---

17. IBM GLOBAL TECHNOLOGY SERVICES, INTERNET SECURITY SYSTEMS, X-FORCE®, 2008 TREND & RISK REPORT 65 (2009), *available at* http://www-935.ibm.com/services/us/iss/xforce/trendreports/xforce-2008-annual-report.pdf.

18. In 2003, Estonia fell victim to a large-scale DDoS attack, and in 2008, Georgia was victimized.

19. Notorious botnets include Asprox, Bogus, Donbot, Mega-D, Rustock, Srizbi, Rustock, Storm Worm, Warezo, and Zeus.

20. Telecom-ISAC Japan and Japan's Computer Emergency Response Team Coordination Center conducted the study in 2005. *See generally* https://www.telecom-isac.jp/.

21. MCAFEE AVERT LABS, MCAFEE THREATS REPORT: FIRST QUARTER 2009, at 4, *available at* http://resources.mcafee.com/content/AvertReportQ109.

22. The CCC project was established by the MIC and the METI, and then the Information Technology Promotion Agency (IPA), Computer Emergency Response Team Coordination Center, Telecom-ISAC, Internet Service Providers, anti-virus vendors developing bot disinfection tools, and other related entities joined as partners. *See* https://www.ccc.go.jp/en_index.html.

The primary objectives of the project are to:

- Collect bot analytes, the constituent elements, using decoy PCs, or "honeypots."
- Identify users' computers infected by bots.
- Provide users with disinfection tools (after notifying them that they were infected by bots).
- Provide the collected bot analytes to anti-virus vendors.

By the end of April 2009, the total number of collected analytes was 13,788,232. Among these, the total number of unique analytes was 886,144. To date, 382,968 emails to alert about bots were sent to 80,647 infected users. The CCC project has succeeded in reducing bot infection in Japan. Anti-virus vendors in their commercial release software have discovered bot analytes in their virus pattern files. This user-based approach was introduced as one of the best practices throughout the world.[23]

Protection against bots in the United States seems to differ significantly from practices in Japan. Exposure of herders and blocking off of C&C server communications are standard U.S. measures against bots. According to the FBI's website, the agency successfully unmasked herders in 2007. A network of the Internet Service Provider (ISP) Atrivo/Intercage, which hosted a C&C server, was shut down by a higher ISP in September 2008. Thereafter, the botnet disappeared. In November, networks of another ISP, McColo, which was hosting several C&C servers used for sending spam emails, were blocked off. Thereafter, evidence of bots and spam emails decreased throughout the world, including in Japan. Apprehension of herders offers the best means to eliminate the root cause of threats derived from bots, and the shutdown of a C&C server hosting a botnet is significant.

However, the detection of herders is becoming more difficult because they do not always send programs directing bot-infected PCs from or within the same country where the C&C server is located. Actually, McColo operated outside of the United States. Another headache is the quick recovery by botnets. In McColo's case, only two weeks after the shutdown, it was observed that bots and spam had resumed, presumably due to a switch to new C&C servers.[24] It is quite simple for bot criminals to resume their attacks because millions of bot-infected PCs exist, even after C&C servers have been shut down.

While law enforcement reports have a significant deterrent effect on botnet herders and criminals, the Japanese approaches to shutting down

23. MICROSOFT SECURITY INTELLIGENCE REPORT, VOL. 7 (Jan.-June 2009), at 40-47, *available at* http://blog.seattlepi.com/microsoft/library/20091102sirv7.pdf.

24. *See, e.g.*, IBM GLOBAL TECHNOLOGY SERVICES, *supra* note 17, at 80.

C&C servers also may deter by increasing the costs of attacking and holding botnets. Researchers have reported that:

> [W]e illustrate in detail how honeypots can be deployed to change economic motivations of illegal Internet practitioners. In this sense, we are in line with these researchers by claiming that botnet-related crimes will dramatically decrease if botnet masters give up on it – that is, when maintaining botnets becomes more troublesome than they are worth.[25]

In our view, the Japanese approach is better from the standpoint of decreasing the C&C server operators' economic motivation. However, the Japanese experience tells us that its approach is not necessarily the best. The CCC also faces an obstacle; only about thirty percent of infected users download the disinfection tool from the CCC web site, even though the CCC notifies users that they are being infected by bots.[26] This is primarily because bots do not cause damage directly to the infected users, so the users do not have a strong motivation to download the tool.

Japan's Information Technology Promotion Agency (IPA) has conducted a basic study to enlighten users by applying the science of social behavior.[27] The role of the media is also important. When the television news reported CCC activity, massive numbers of users checked the CCC web site to request the bots disinfection tool. The result caused the equivalent of a denial of service (DoS) attack – but in a good sense.[28]

B. Looking Toward the Future – A Comprehensive Approach

More effective methods are needed to mitigate the bot threat. Specifically, nations should adopt a comprehensive approach to the bot problem. A comprehensive approach is necessary not only because each nation's approach is not very effective on its own, but also because bot attackers tend to use stealth techniques.

As recorded by the CCC, herders and attackers now employ methods aimed at making PC users sequentially download limited portions of malicious programs from seemingly legitimate websites that have been cracked beforehand by herders or attackers. These methods of attack make detection more difficult. The web technology that facilitates information

---

25. Zhen Li, Qi Liao & Aaron Striegel, *Botnet Economics: Uncertainty Matters*, at 3 (presented in the Workshop on the Economics of Information Security (WIES) (June 2008)), *available at* http://weis2008.econinfosec.org/papers/Liao.pdf.

26. *See* CCC activity reports, *supra* note 22.

27. *See generally* http://www.ipa.go.jp/english/about/outline/security/02.html.

28. In our view, the role of the media should be carefully examined in such cases. There is a tension between informing the public about security incidents and protecting national security. There are also tensions as regards reporting personal information leaked via peer-to-peer (P2P) networks and protecting the privacy of people affected by leaks.

sharing, called "Web 2.0," such as P2P search engines, also increases the challenge posed by bots.

The international information security community should make provisions to protect data centers, or "cloud computing," from bot attacks. Evildoers may utilize clouds available to the general public – "public clouds" – as C&C servers. Researchers recently cautioned that:

> Another availability obstacle is Distributed Denial of Service (DDoS) attacks. . . . Such attacks typically use large "botnets" that rent bots on the black market for $0.03 per bot (simulated bogus user) per week.[29]

Beyond the obstacle of cloud computing, we are concerned about development of a new bot attack technique using computation resources of cloud computing. Further, botnet herders may perform a DDoS attack to clean out a cloud computing system as an attractive target. Waves of cloud computing can give the evildoers opportunities for cost reduction, creation of new attack methods, and easy targets. The evildoers may thus be able to enjoy the taste of cloud computing three different ways.

From information security points of view, security practitioners may encounter difficulties in analyzing, predicting, and discovering bot attacks electronically should herders use cloud computing, because information is processed and stored in cloud computing servers that are unknown to users and even to cloud computing providers. To quote a saying from the ancient Chinese Sun Tzu's *Art of War*, "One who knows the enemy and knows himself will not be endangered in one hundred engagements."[30] We are moving into an age when it is difficult to know our enemies.

Laws should be harmonized internationally to establish a comprehensive approach. A law authorizing interception of telecommunications for the purpose of information security needs to be considered.

Secrecy of communication in Japan has been dealt with rigorously in the country's Telecommunications Business Law.[31] Some practitioners, however, have advocated that the secrecy principle should be applied

---

29. MICHAEL ARMBRUST ET AL., ABOVE THE CLOUDS: A BERKELEY VIEW OF CLOUD COMPUTING 14-15 (2009), *available at* http://www.eecs.berkeley.edu/Pubs/Tech Rpts/2009/EECS-2009-28.pdf.

30. SUN TZU & SUN PIN, THE COMPLETE ART OF WAR 179 (Ralph D. Sawyer trans. Westview Press 1996).

31. Telecommunications Business Law, Law No. 125 of 2003 (amending Law No. 86 of December 25, 1984), art. 4, states: (1) The secrecy of communications being handled by a telecommunications carrier shall not be violated. (2) Any person engaged in the telecommunications business shall, while in office, maintain the secrets of others that have come to be known with respect to communications being handled by the telecommunications carrier. The same shall apply even after this person's retirement from office. An unofficial English translation of the law is available at http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/Resources/laws/2001TBL.pdf.

flexibly. Some researchers have proposed reexamining the extent of protection of communications secrecy, and suggest that the original drafter of Article twenty-one of the Constitution of Japan regarding secrecy of communication did not intend it to be interpreted so broadly.

There are some architectural features of the IP network that allow a network operator and a law enforcement agency to intercept IP network information in the United States and Europe under specific cases.[32] To fight bot attacks, international agencies of information security should be challenged to promote standardization of practices related to telecommunications interception around the world.

It is anticipated that the U.S. government will make government-private sector partnerships, including relevant ISPs and anti-virus vendors, a priority. The Obama administration's *Cyberspace Policy Review* suggested that:

> The President's cybersecurity policy officials should work with relevant departments and agencies and the private sector to examine existing public partnerships and information-sharing mechanisms to identify or build the most effective models.[33]

The *Review* does not touch specifically on anti-bot measures. The Japanese experience suggests that private companies are motivated to implement anti-bot measures as part of corporate social responsibility (CSR) programs.[34]

The *Cyberspace Policy Review* also emphasizes effective partnership with the international community, and states that:

> The United States needs to develop a strategy designed to shape the international environment and bring like-minded nations together. . . . In addition, differing national and regional laws and practices – such as those laws concerning the investigation and prosecution of cybercrime; data preservation, protection and privacy; and approaches for network defense and response to cyber attacks – present serious challenges to achieving a safe, secure, and resilient digital environment.[35]

---

32. 18 U.S.C.A. §2511(2) (West 2000 & Supp. 2010) allows operators of network providers and investigators to monitor the content of telecommunications. For the European Telecommunication Standards Institute (ETSI) model, see Aqsacom Document No. 04050 (040451), *Lawful Interception for 3G Networks: White Paper* (Nov. 2005), *available at* http://www.aqsacomna.com/us/articles/LI3GWhitePaperv4.pdf.

33. CYBERSPACE POLICY REVIEW, *supra* note 2, at 18.

34. Notably, as of June 2009, the number of ISPs participating in Japan's CCC has reached 77, which represents about two-thirds of all contracting broadband users in Japan. ISPs indicate that they are motivated by CSR and an expectation that participation will improve their corporate public relations. For more on ISPs participating in the CCC, *see* https://www.ccc.go.jp/en_ccc/.

35. CYBERSPACE POLICY REVIEW, *supra* note 2, at 20.

Now is the time to cooperate on a worldwide basis to address bot attacks. Clearly, although bot attacks have already been conducted globally, international protection and defense schemes remain divided and disorganized. In July 2009, the DDoS attack on the United States and South Korea via botnets, in which bot-infected PCs all over the world were used as delivery and attack points,[36] is very fresh in our minds.

To eliminate threats posed by bots and to stop these global DDoS attacks, comprehensive countermeasures should include apprehension of herders (including attackers and C&C server renters), shutdown of C&C servers hosting botnets, cleanup of C&C servers worldwide, periodic monitoring of viruses in a balanced and cooperative manner, and creation of legal frameworks and a capability to investigate herders. The international community must act collaboratively on these measures.

CONCLUSION

National information security policy must achieve a balance between post-incident measures, criminal investigations, business continuity, national security, and communications secrecy. To be effective, the policies also must win public trust. Thus far, Japan's cybersecurity system – including its control center, the NISC, and its cryptography and anti-bot policies – is well managed and effective. The same can be said of the U.S. cybersecurity system, though it sometimes operates under contrasting approaches.

Global society, however, is now seeing cyber threats different from those of the past in terms of method and quantity. Cyber espionage and crime through malicious and secretive techniques, potentially massive cyber disruption, and terrorism are emerging. Consequently, strong political leadership is crucial to protect critical information infrastructures from innovative attacks.

Facing these threats, all involved parties – international and domestic – should investigate the appropriate extent of lawful access and enforcement. In addition, governments should establish systematic means for coordinating with the public in their decisionmaking processes to promote public understanding and trust.

Moreover, anti-bot cooperation provides a good opportunity for Japan and the United States to lead an international cooperation effort. It also provides a perfect case study where security and secrecy issues can be extensively discussed and resolved.

---

36. *See, e.g.,* Shadow Server, http://www.shadowserver.org/wiki/pmwiki.php/Calendar/20090710.

APPENDIX

OECD Guidelines for Cryptography Policy: Principles[*]

Principle 1: TRUST IN CRYPTOGRAPHIC METHODS. Cryptographic methods should be trustworthy in order to generate confidence in the use of information and communications systems. . . .

Principle 2: CHOICE OF CRYPTOGRAPHIC METHODS. Users should have a right to choose any cryptographic method, subject to applicable law. . . .

Principle 3: MARKET DRIVEN DEVELOPMENT OF CRYPTOGRAPHIC METHODS. Cryptographic methods should be developed in response to the needs, demands and responsibilities of individuals, businesses and governments. . . .

Principle 4: STANDARDS FOR CRYPTOGRAPHIC METHODS. Technical standards, criteria and protocols for cryptographic methods should be developed and promulgated at both the national and international level. . . .

Principle 5: PROTECTION OF PRIVACY AND PERSONAL DATA. The fundamental rights of individuals to privacy, including secrecy of communications and protection of personal data, should be respected in national cryptography policies and in the implementation and use of cryptographic methods. . . .

Principle 6: LAWFUL ACCESS. National cryptography policies may allow lawful access to plaintext, or cryptographic keys, of encrypted data. These policies must respect the other principles contained in the guidelines to the greatest extent possible. . . .

Principle 7: LIABILITY. Whether established by contract or legislation, the liability of individuals and entities that offer cryptographic services or hold or access cryptographic keys should be clearly stated. . . .

Principle 8: INTERNATIONAL CO-OPERATION. Governments should co-operate to co-ordinate cryptography policies. As part of this effort, governments should remove, or avoid creating in the name of cryptography policy, unjustified obstacles to trade. . . .

---

[*] *See supra* note 10.