National Cyber Security Strategy: Are We Making Progress? Japan's Efforts and Challenges
Author(s): Yoko Nitta
Source: *Georgetown Journal of International Affairs*, International Engagement on Cyber IV (2014), pp. 89-98
Published by: Georgetown University Press
Stable URL: https://www.jstor.org/stable/43773652
Accessed: 06-05-2020 02:58 UTC

National Cyber Security Strategy

Are We Making Progress? Japan's Efforts and Challenges

Yoko Nitta

No nations' security strategies are currently prepared for cyber attacks. These attacks are advancing dramatically and are increasingly more threatening than cyber espionage, which governments have been typically involved with. Cyber attacks impact individuals and industries, as well as thwart national defense and social order. Cyber warfare refers to offensive exchanges of military, political and diplomatic intelligence, which can target national defense systems and critical social infrastructure. Now, the use of cyber capabilities is a growing trend in warfare, especially to augment other military components. Cyber policy is now an integral aspect of foreign policy issues ranging from human rights to national security.

There is a global increase of cyber-attacks traversing state borders, which makes international cyber security cooperation vital for global security. Cyber-cooperation, however, is not new for Japan, as the Asian state recently signed an agreement with the United States. Moreover, the Japanese cyber industry is constantly advancing and is a strong national resource, which raises domestic demands for international cyber defense cooperation. The demand for international cyber security agreements demonstrates that cyber defense

Yoko Nitta is a senior principal researcher at the Japan Society for Security and Crisis Management, where she focuses on science diplomacy, cyber espionage, information warfare and intelligence. She was a former associate fellow at the Japan Science and Technology Agency (JST), as well as a professional investigator with Japan's Ministry of Foreign Affairs.

is one of the biggest security challenges of the 21st Century. It is apparent that states believe international cooperation is key to increase their ability to solve the challenge.

In this regard, observations of Japan's cyber security strategy and its approach to international collaboration for cyber issues will be laid out.

Risks to Global Commons. The National Security Strategy of Japan, which got approved at the ministry level in December 2013, describes cyberspace as a global common: cyberspace, a global domain comprised of information systems, telecommunications networks and others, provides a foundation for social, economic, military and other activities. Meanwhile, the risks of cyber-attacks that intend to steal classified information, disrupt critical infrastructure and obstruct military systems are becoming more serious. In Japan, the increasing level of interconnected networks of social systems and various other elements makes cyber space valuable for promoting both economic growth and innovation through the free flow of information. Protecting cyberspace from the above-mentioned risks is vital to maintain national security.

The strategy touches upon strengthening and expanding Japan's capabilities and the roles of Japanese cybersecurity contributions overseas.

The strategy also touches upon strengthening and expanding Japan's capabilities and the roles of Japanese cybersecurity contributions overseas: Japan as a whole will make connected efforts in comprehensively proofing cross-cutting measures to defend cyberspace and strengthen its response capabilities against cyber-attacks to protect its networks from malicious activities, ensure the free and safe use of cyberspace, and guard its critical infrastructure, including those in which Japan suspects adversarial state involvement. To this end, Japan will strengthen public-private partnerships to assess the risks of network systems' designs, developments and operations. It will further identify incidents, minimize their damages and their expansion, and analyze their causes to prevent similar incidents in the future. In addition, Japan will comprehensively consider and take necessary measures with regard to expanding the pool of human resources in the security field, protecting control systems, and responding to issues of supply chain risk. Furthermore, Japan will strengthen inter-agency cooperation and define the roles of relevant agencies so that it can reinforce its capabilities to protect cyberspace and respond to nation-wide incidents. At the same time, Japan will promote a range of measures, including enhancing its ability and function to oversee, assess, apprehend, analyze, and internationally coordinate responses to cyber incidents, as well as reinforcing relevant agencies in charge of those tasks. In promoting these measures, strengthening international partnership in a wide range of areas is essential. For this, Japan will take measures at technical and operational levels to enhance collaboration with other countries. Japan will also strengthen information sharing and promote cyber defense cooperation with relevant allies.

There is another challenge; it has become increasingly important for nations to speak with a unique voice and advance a global vision of cyber space, which has produced conflicts among some states. Russia and China have different perspectives from those of the United States and other countries regarding the free flow of information. It is next to impossible that Japan could fill the gap for the time being.

Background. There was motivation for Japan to wake-up from its peaceful past seventy years to the current uncertain and insecure situation. To begin with, Mitsubishi Heavy Industries, one of the biggest Japanese defense corporations, got cyber attacked and information was stolen from their eleven offices in Japan. To make matters worse, Mitsubishi Heavy Industries did not report their attacks to the Ministry of Defense (MOD), even though they are a prominent defense contractor.

This was followed by an unconfirmed information leakage at the Japan Nuclear Energy Safety Organization (JNES), an attack case on TPP-related information at the Ministry of Agriculture, Forestry and Fisheries of Japan (MAFF), external unauthorized access to servers at the Japan Aerospace Exploration Agency (JAXA), a zero-day attack causing particular entities to be infected by web browsing at government agencies, and the possibility of an information leakage by a virus infection at the Japan Atomic Energy Agency (JAEA). Later, the National Information Security Center (NISC) aimed to coordinate and take charge of particular ministries and agencies. NISC was launched under the Cabinet Office in April 2005 as a control tower of Japanese information security policies.

Additionally, Big Data has high economic potential and has been discussed at the ministry level for its use as a driver for economic growth. Corporations have already incorporated it as their competitive tool. Big Data is a common platform for information sharing and its data is regarded as a service because open data, initially stored knowledge, M2M (streaming data) and personal data can be collected and replaced with Big Data. On the other hand, the characteristics of cyber space may cause Big Data to increase the severity of risks, dissemination of risks, and the globalization of those risks. Unfortunately, the method of compiling data is impossible to predict in advance so that it is difficult to know the potential risk in advance. Japan may be overlooking the challenges that Big Data poses—including the way companies interpret the information, manage the politics of data and find the necessary talent to make sense of the flood of new information.

Big Data, in other words, introduces high stakes into the data-analytics game. There is a greater potential for privacy invasion, greater financial risk exposure in fast-moving markets, greater potential for mistaking noise for true insight, and a greater risk of spending lots of money and time chasing poorly defined problems or opportunities. Unless

Japan understands and deals with these challenges, it risks turning all that data from something that has the potential to benefit Japanese organizations into a diversion, an illusion or a paralyzing turf battle.

The Defense Posture Review Interim Report published by the Ministry of Defense (MOD) has shown the new integrated mechanism of the Self Defense Forces (SDF), combining the forces of Air, Marine and Land to combat cyber attacks. This new task force, the Cyber Defense Unit, was launched at the end of March 2014. The report serves as a basis for the new National Defense Program Guidelines that motivates Japan's medium and long-term defense policies.

The Japanese government will also redesign the National Defense Program Guidelines, which will be published at the end of 2014, which will be a trigger for a big leap. The new guideline should be pragmatic and promote mutual interests between the United States and Japan.

Analysis for Japan Cybersecurity Strategy. The Japanese Cybersecurity Strategy covers diverse areas. The three main pillars are: (1) a resilient cyberspace to strengthen ability of protection and recovery among all stakeholders, (2) a vigorous cyberspace to strengthen creativity and knowledge through developing technology, capacity building, and increasing public literacy, and (3) a world-leading cyberspace to strengthen the ability of contribution and outreach through diplomacy, global outreach and international cooperation.

The National Information Security Council (NISC) is responsible for managing the ministries working on cyber attacks. This conglomeration is going to be redesigned as a Cyber Security Center with strengthened authority by the end of 2015. The Center has laid out a mid-term goal by Fiscal Year 2015 to increase cyber security information-sharing among government agencies and critical infrastructure providers, decrease malware infection rates and citizen concerns, and improve international incident coordination, as well as a long-term goal by 2020 to double the size of the domestic information security market and increase the proportion in security professionals in the marketplace.

1)*Is the strategy focused towards a particular type of threat?*

The strategy is focused on attacks against our critical infrastructure, such as critical industry information, which is our source of global competitiveness and benefits corporations, academia, and research and development institutions that deal with intellectual property and piracy information. A significant threat is also cyber attacks toward state secrets. There is a need to strengthen the ability to recognize and to respond to cyber attacks against these critical assets.

2)*Has Japan outlined the necessary steps, programs and initiatives that must be undertaken to address the threat?*

The Control System Security Center (CSSC) is at ethnology research association to conduct R&D to handle cyber attacks and ensure the security of control systems of critical infrastructures that support people's lives, such as gas and power plants. In order to ensure the security of control systems of impotent infrastructures, CSSC conducts various thorough operations including research and development, international standardization, certification, human resource development, and the security verification of each system. On 17 May 2013, eighteen corporations joined the association to contribute to control systems security research, edification, education, training, authentication and international collaboration. It is a critical issue for the national security and risk management complex to deal with cyber attacks against control systems of important infrastructures, such as gas and power plants.

Another Japanese technology project to deal with cyber attacks is a cyber attack alert system, which the National Institute of Information and Telecommunication Technology (NICT) developed. Termed the "NICT Daedalus Cyber- attack alert system", this project views the state of an attack on networks visible in "3D" real-time graphics. Daedalus, which stands for "Direct Alert Environments for Darknet and Livenet Unified Security," visualizes large groups of computers from multiple perspectives to track any suspicious activity as it moves through the network. Today's cyber attacks breach boundary defenses of organizations internally and externally, which includes spreading malware via USB memory sticks (this could be most lethal weapon in the twenty- first century), mail attachments, as well as zero-day exploits. Therefore, using Daedalus along with conventional boundary systems is expected to improve organizations' network security. NICT also provides the system free of charge to educational institutions.

The challenge is that if Japanese critical infrastructure gets attacked, it is difficult for the Ministry of Defense (MOD) and Self Defense Forces (SDF) to adequately respond, since the new cyber response unit only consists of 90 people as of today. While its structure will be strengthened, the response unit's main mission is to protect the network system of MOD and SDF. Furthermore, it is a quite challenging to determine who attacks via attribution, and whether we can respond. Plus if the attacker is a single person, it is uncertain whether the military should respond. The upcoming Japan-U.S. Guidelines will address these issues.

3)*Has a responsible entity or competent authority been identified in Japan's Cybersecurity Strategy? Is that entity or authority empowered?*

Critical infrastructure industries interact with the Cyber Security Information Sharing Partnership of Japan (J-CSIP, pronounced JAY-sip), which takes initiative for cyber security information-sharing partnership between Ministry of Education, Science and Technology, Culture and Sports (MEXT) and private sector. The Information-Technology Promotion Agency (IPA) operates this cyber-security partnership. IPA collects information on cyber attacks that are detected at member companies and their group companies, anonymizes the information source (the member company who provided the information), obscures or deletes sensitive information, adds its own analysis, makes the information sharable with the authorization from the information source, and shares the information with member companies. Additionally, Japan's Computer Security Incident Response Team (CSRIT) works on detection, triage and response. Its mission is quite similar to that of firefighters. CSIRT is a critical operations model and its daily training and accumulated knowledge is an asset.

Japan has also sent SDF to the United States to train their cyber defense skills and bring their cyber security knowledge back home. Japan and the United States held the first working level meeting over cyber defense to prepare for launching the project in 2015. The two nations confided in each other that cyberspace cooperation would require constructing a working-level panel over the issue. The panel intended to discuss cyber attack training and considered dispatching commander-class officers from cyber-related units to one another's instructors in each country.

The NISC has the Government Security Operation Coordination Team (GSOC) to monitor computer systems of ministries, collect information on incidents, and analyze them on a 24/7 basis. Each ministry in the Japanese government has a Computer Security Incident Response Team.

There are no laws in place to effectively collect communication records, even though countries overseas possess those laws and regulations.

4) *Are the laws adequate?*

The National Policy Agency (NPA) has been doing everything they can to deal with cyber attacks under the current law. However, the current legal framework to promote robust Japanese cybersecurity is inadequate. Article 21 of Japanese Constitution and article 4 of Telecommunication Business Act protect the secrecy of telecommunications. Due to these articles, telecommunications cannot be traced down nor analyzed without contractual agreements between users and carriers, even if illegal correspondences are found in the telecommunication network. As a result, it is difficult and time-consuming to block or cease those illegal telecommunications. A recent example is a computer that was remotely attacked with a virus last year. NPA's response to the incident was inadequate, and eventually NPA arrested the wrong person for the attack. This indicates that there are no laws in place to effectively collect communication records, even though countries overseas possess those laws and regulations. It is also quite difficult to identify the criminal with a surveillance camera. In order to bolster Japan's attribution and tracking of cyber-threats, it is necessary to develop a legal framework that grants certain governmental institutions the authorities to inspect and analyze network data. It is therefore essential that articles of the Japanese constitution and Japan's telecommunications business law be changed. Because Japan is an island nation and connected through submarine cables via landing points, the country should be able to tap into these network lines to watch malicious communications.

5) *Has funding been set aside to address the*

cyber security shortfalls? What are the highest priorities and why?

The Japanese government does not collect enough information on cyber attacks since there is no sufficient information-sharing mechanism based on trust similar to what the United Kingdom has. Japanese corporations are rather reluctant to report to government due to fears of publicizing their gaps in cybersecurity. Exposing institutional weakness could result in profit-losses from falling stock prices and investor uncertainty. Accordingly, Japan needs to define beforehand which information should be confidential and solely for government, as well who can access their corporate network data.

Another concern is that most of the software used to combat cyber attacks in Japan is manufactured overseas. If a new, domestically made system can be created for monitoring communication activity, it would be a huge leap for Japanese cybersecurity.

More importantly, Japan needs to foster human resources and put them on well-established positioning to advance Japan's cyber security strategy. Providing adequate funding and incentives for all these requirements is essential to attain this goal.

The Challenge of Cyberspace: Living and Working in a Digital Society. Humankind has taken for granted the pervasiveness of computerization and the equally ubiquitous connectivity of what we have come to call cyberspace. In just over twenty years, society has become massively dependent on the benefits of what has grown into a vast and complex global information and communication system. The system that allows us to effortlessly withdraw cash anywhere in the world, video chat with loved ones on the other side of the globe, or connect to the office while traveling in the wilderness is one aspect of cyberspace, while Edward Snowden's leaking of the National Security Agency's details of United States global surveillance operations, and the widespread use of cyberspace by criminal organizations and ordinary individual criminals is another. Yet there are divergent views on whether to prioritize or ignore the dark side of the contemporary communications revolution. Humanity not only produces vast amounts of information, but it also routinely allows that information to be accessed by others, sometimes for good and sometimes for malign purposes.

On the positive side, "data analytics" (often describe as "Big Data") is facilitating major strides in improving productivity and efficiency in areas as diverse as "smart" electricity grids, genomic medicine and personal digital assistants. Massive Open Online Courses (MOOCs) offer a fundamental shift in the democratization of education and its outreach to those in emerging economies.

On the negative side, there is the widespread criminal use of cyberspace and a burring of the boundaries between state and non-state actors in activist attacks and old-style espionage, but with constantly evolving tools. Similar abuses of the privacy of personal data, especially in sensitive areas such as medical records, could fundamentally undermine trust between a government and its citizens.

Further Implications. Governments use cyberspace for a variety of purposes, both defensive, to counter the exploding number of cyber attacks on government agencies, and offensive, such as the Stuxnet worm attacks on the Natanz facility in Iran in 2010. The increasing tendency to see cyberspace as a battlespace and computers as weapons can be best seen in the October 2012 statement by the then-Secretary of Defense, Leon Panetta, who declared that cyber warfare- conflict between states or non-state actors using attacks on, with, and by computers- is the greatest threat facing the United States.

Even though we have not yet developed many of the capabilities that are being bruited, there are nonetheless those who worry about a "cyber Pearl Harbor" that will attack infrastructure targets built in the pre-computer age. Trying to provide security against the possibility of a cyber attack seems to be a constant challenge by government agencies charged with providing their citizens with protection. The creation of a Cyber Command by the United States in 2010 is one such measure.

Abusing the privacy of personal data, especially in sensitive areas such as medical records, could fundamentally undermine trust between a government and its citizens.

Yet it is not just the "weaponization" of cyberspace that has engaged governments and security agencies. In many countries, governments use the Internet and their citizens' apparent addiction to cyber-connectivity to deepen the control of governing elite. Similarly, these deeply interconnected and interdependent elements have a tendency to form "accidental systems" whose characteristics are poorly understood and may weaken both technological and social resilience through potential cascades of failure.

Conclusion. While the technologies underpinning cyberspace have been through some forty years of continuous exponential growth in performance per unit price, humans remain linear beings; they do not adapt well on the same timescale. This points to a key area where more work is required. The growing impact on individual citizens and organizations by these developments is poorly understood. Good security is a holistic balance of personnel security, physical security and electronic security. In many organizations, excessive testing in the (nonetheless important) technological approaches to cybersecurity has led to neglect of the other areas with potentially disastrous results. Some organizations, by focusing too much on the technological approaches to cyber security, were neglecting some of the basics of physical security and personal security. Failing to hire new staff and failing to cheek the authenticity of biographies in job applications is one such example. There is also a poor understanding across general pollutions of the basics of "cyber hygiene." Even the fundamental tools of business lag behind. As a consequence, we fail to apply many tried and tested corporate disciplines to these new challenges. The increased use of social media continues to transform politics in countries around the world, posing challenges to long-established political institutions.

In the one year since the cybersecurity strategy was passed, Japan has been successfully developing its cyber capabilities as well as struggling to implement certain crucial provisions. With adequate support, resources, and clearly established policy and legal frameworks, Japan will achieve new heights in cyber security for years to come.

NOTES

[1] National Information Security Council "Japan Cybersecurity Strategy"

June 13, 2013 http://www.nisc.go.jp/active/kihon/pdf/cybersecuritystrategy-en.pdf

[2] National Information Security Council "International Strategy on Cybersecurity Co-operation ~ J-initiative for cybersecurity" October 2013 http://www.nisc.go.jp/active/kihon/pdf/InternationalStrategyonCybersecurityCooperation_e.pdf

[3] The Government of Japan "National Security Strategy of Japan " December 2013 http://www.cas.go.jp/jp/siryou/131217anzenhoshou/nss-e.pdf

[4] Defense of Japan 2013 'White Paper' http://www.mod.go.jp/e/publ/w_paper/2013.html

[5] Richard A. Clarke and Robert K. Knake's "Cyber War: The Next Threat to National Security and What to Do About It" (Harper Collins, 2010)