Review of the Japan Cybersecurity Strategy

Dr. Yoko NITTA

September 2014

Abstract

Digitization and networking in socioeconomic activities whistles us to create stable cyber security not only for people's lives but also for national security and crisis management, which is a significant challenge. While at the same time, modality of cyber attacks are obvious such as Advanced Persistent Threat (APT) which calculates to exploit sensitive information of government and industries, targeting control system of critical infrastructure directly related to people's lives. Moreover, a massive theft of personal information by smart device has diffused rapidly.

Information Security Policy Conference chaired by chief cabinet secretary launched cyber security strategy in 2013 as a national strategy. It aims at dealing with risks in cyberspace working with coalition to real space, which has got worse.

The Japan Cybersecurity Strategy is supposed to review policy every three years. Based on the outcomes and effort, Japan has worked on since its release, the strategy has been shed light on challenges.

This paper overviews the efforts and challenges of the Japan Cybersecurity Strategy since one year has passed since it was launched.

About ISPSW

The Institute for Strategic, Political, Security and Economic Consultancy (ISPSW) is a private institute for research and consultancy. The ISPSW is objective and task oriented and is above party politics.

In an ever more complex international environment of globalized economic processes and worldwide political, ecological, social and cultural change, bringing major opportunities but also risks, decision-makers in enterprises and politics depend more than ever before on the advice of highly qualified experts.

ISPSW offers a range of services, including strategic analyses, security consultancy, executive coaching and intercultural competency. ISPSW publications examine a wide range of topics connected with politics, economy, international relations, and security/ defense. ISPSW network experts have worked – in some cases for decades – in executive positions and possess a wide range of experience in their respective specialist areas.

Giesebrechtstr. 9
10629 Berlin
Germany

Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06

E-Mail: info@ispsw.de
Website: http://www.ispsw.de

ANALYSIS

Introduction

Internet has firmly established as essential fundamentals for the life of the people as well as social economy activities. On the other hand, continuous cyber attack has never ceased and its target has been at government and government agencies.

Utilizing information communication technology (ICT), cyber intelligence exploits classified information from government and industries which have advanced technologies. Also cyber threats, which could paralyze social operation public safety, will certainly affect national security and crisis management.

Emergency economic projects for Japan's economic recovery has aimed at boosting GDP by two percent and create jobs for more than 600,000 people. In the policy speech by Prime Minister Shinzo Abe to the session of the Diet said "Furthermore, the recent terrorist incident in Algeria has sounded a warning to us once more regarding the importance of crisis management as a nation. We will handle such matters with even greater vigilance under a 24-hour, 365-day system for crisis management responses, including terrorist or cyber attacks as well as large-scale natural disasters and major accidents."

With the diffusion of information communication technology, government agencies as well as industries generally retain information with electronic data. As to the definition of information security, Japan has focused on its confidentiality, integrity as well as availability which are all lined with OECD information security guideline (2012) and U.S. Information Security Management Law (2002) cyber security strategy.

The double budget is allocated for cyber security by 500 million euros for the new fiscal year compared to the one of previous year.

Background

In the past decades, smart phone users and social media (Facebook and Twitter) have increased rather than mobile and personal computers due to the ICT penetration. Also countries which use internet are expanding from developed countries to developing ones, taking shape that internet is connected globally. The measures of cyber attacks are getting more advanced and complex (DDoS) and the aims are worsened from crime committed for fun to economic crime and organized crime. The features of cyber attacks are attribution, invisibility, executing permission beyond borders.

The threat of cyber intelligence was triggered by the fact that the 80 computers of Japanese top defense industry, which manufactures state-of-the-art submarine, missile and nuclear power plant, was virus attacked by outside illegal program which could exploit confidential information in 2011. It followed by the similar modus operandi (MO) as the computers of the House of Representatives. To make the matters worse, ID and passwords of all members run out and they got them stolen at a glance for more than two weeks. Also, the documents of TPP were flowed out in 2013 from the computer of the Ministry of Agriculture, Forestry and Fisheries by virus affected with illegal program.

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

The recent case of cyber attacks is Sony play stations DDoS attacked. The cloud server was damaged and lost mailing list data by five thousand due to the defectiveness updated program, illegal access attacked net banking users ID and passwords, which led to illegal wire transfer. Typical cases of Advanced Persistent Threat (APT) are the one that Mitsubishi Heavy Industry and Stuxnet.

The Japanese Cybersecurity Strategy was launched in 2013 and its basic missions of NISC (National Information Security Council) is already found in 'Information Security 2012' which NISC released then, which was to strengthen measures for sophisticated threats to companies and organizations handling important national information on security, to maintain a safe and secure user environment for addressing the emerging risks associated with the proliferation of new information and communications technology including the full-fledged widespread use of smart phones, to reinforce international alliances.

In Japan, NISC is the control tower of cyber security of government coordinating government efforts and four key agencies, National Police Agency (NPA), Ministry of Internal Affairs and Communications (MITI), Ministry of Economy, Trade and Industry (METI) and Ministry or Defense (MOD) work closely with businesses and individuals. Agencies in charge of critical infrastructures, Financial Services Agency, MIC, METI, Ministry of Health, Labour and Welfare and Ministry of Land, Infrastructure, Transport and Tourism are in charge of critical infrastructures and they corporate with NISC. They have strengthened its capacity because it was raised awareness by Stuxnet.

For cyber security activities of NPA, whose main mission is to fight cyber crimes, reorganize 'Cyber Force Center' with 140 IT staffs as a control center of all nation's cyber force center sharing information with CCI-designated companies, playing a role as a council to prevent unauthorized communication to counter cyber intelligence with 4,800 companies all over Japan. NPA has improved response capability against cyber crimes and against cyber attacks which threatens state secrets and critical infrastructures, has extended international collaboration, has kept analysis and law enforcement capacities up to date with changing IT technologies and laws.

MIC has mainly been in charge of smart phone information security.

METI has taken initiative for cyber security information sharing partnership Japan (J-CSIP) for sharing information on cyber attacks among partners, building a pool of advanced information security experts such as national security competition, securing control systems such as implementing cyber security exercises, establishing Control System Security Center (CSSC) in 2013 in Tokyo and Tsunami-affected area (Miyagi Reconstruction Park). In this regard, METI has been a hub for security verification and education and worked on information security promotion projects.

The six core approaches of MOD for cyber security are to improve information and telecommunication systems security, to reinforce protection systems, to prepare rules and regulations, to develop human resources, to promote information sharing and to enhance R&D of latest technologies. MOD established 'Cyber Defense Unit' in March 2014 with 100 members, developing network monitoring equipment and has trained through Japan-U.S. joint exercises.

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

First pillar of the Japan Cybersecurity Strategy: Constructing Resilient Cyberspace to strengthen ability of protection and recovery

In order to maintain the sustainability of cyberspace, in addition to reinforcing measures for responding to cyber attacks, Japan aims to construct "resilient" cyberspace and enhance its defensive and recovery capabilities against cyber attacks and other cyber incidents by improving such functions as for recognition and analysis of cyber attacks and for information sharing related to incidents.

1. Highlighted some efforts done by government

For further improvement in information security standards for information and information system, cabinet office strengthens information security of smart phones within government. They need to enforce towards diversified work arrangement.

To toughen inter-government information system, cabinet office and MIC countermeasure towards information threat against system of cloud computing. METI and all ministries enhance the appropriate usage of IT products which is safe and secure software and services promoted by Information Technology Agency (IPA), which is an incorporated administrative agency working closely with METI.

Cabinet office and all ministries promote information security for industries dealing with state secret information. Industries which have contracts with government are enforced to abide by its security policy based upon government procurement guideline.

2. Preparedness for enhancement against cyber attacks

The operational unit of NISC, the GSOC, or the Government Security Operation Coordination team, the authority to deal with threats in a timely manner by cutting through sectionalism among the ministries. In 2012, the GSOC detected 1.08 million illegal access attempts – an average of one every 30 seconds – on government computer systems, up 64 percent from 2010. The radical strengthening of GSOC is required such as drastic review for the capacity for emergency response against cyber attacks. Well-developed sharing information system is aimed at analyzing the overall trend of cyber attacks against government. The collaboration of Cyber incident Mobile Assistant Team (CYMAT) and Computer Security Incident Response Team (CSIRT) is enhanced to response incidents in government.

3. Dealing with critical infrastructure sectors

Cabinet office needs to implement regarding facilitation of safety standards and its reach masses in related businesses. Information sharing system is reinforced and is reviewed within cabinet office and operated by responsible ministries. International collaboration such as bilateral, regional and multilateral is strengthened and best practice cases are provided to related sectors.

Training for initial response to large-scale cyber attack is implemented and the new budget is allocated for this by four million euros. Also, cyber information sharing initiative is enhanced by METI to deal with this issue. METI supports to establish the assessment and certify body for control system equipment of CSCC, also strives to launch the body based on international standard of control security system.

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

4. Improving cognition of incident and its analysis capacity

NPA and Ministry of Justice reinforce rapid understanding of prior warning against cyber attack and collection of information and its analysis for this situation. Also they work on information analysis for assessing the current status of cyber attacks. Ministry of Internal Affairs and Communication (MIC) promotes preventive and early countermeasures against cyber attacks collaborating with universities as well as United States based on the consensus at Japan-US Cooperation on the Internet Economy. MIC continuously proceeds discussion with EU for collaboration research to smooth attack on network. Also MIC promotes cooperation by Japan ASEAN Security Partnership, JASPER, which is a collaborated project with ASEAN counties.

5. Crime countermeasure in cyberspace

NPA strengthens preparedness within cyber attack analysis center and cyber force center against cyber attacks. They promote crime prevention with Special Troops located in 13 prefectures in Japan. Also NPA considers the establishment of Japan version National Cyber-Forensics & Training Alliance (NCFTA). They work on further collaboration between public and private to deal with cyber terrorism against critical infrastructure, also to deal with cyber intelligence. NPA implements environmental arrangement for safety usage of smart phone, which is getting a big concern, and they tackle cyber crimes targeting smart phone users.

6. Defense in cyberspace

MOD put in place the equipment for information gathering, system design for cyber protection analysis for next version, functional enhancement for equipment for cyber protection analysis, preparing Defense Information Infrastructure (DII), research for building technology for environment of cyber drill, strengthening of network monitoring, information gathering on cyber attacks related overseas, promoting human resource development and enhancing cooperation with overseas as well as industries.

Cabinet office, NPA, MIC, Ministry of Foreign Affairs (MOFA), METI, MOD and related agencies toughen countermeasures to deal with national sponsored attacks.

Second pillar of the Japan Cybersecurity Strategy: Constructing Vigorous Cyberspace to strengthen knowledge and creativity

In order to maintain the expansion of cyberspace, Japan aims to construct "vigorous" cyberspace through the activation of industry which plays a central role in responding to cyber attacks, developing advanced technologies, carrying out training and fostering of human resources and literacy, and other measures, and aims to strengthen the creativity and knowledge which will allow it to independently respond to the risks surrounding cyberspace.

1. Industrial vitalization

METI promotes research and develop (R&D) for high security semiconductor device to address diffusion in smart community, check list of cloud service level, efforts for international standardization working with MIC and trade of security products based on international rule. The budget for this project, METI is allocated.

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

2. R&D

MIC operates research infrastructure to promote R&D for cyber security through NICT, National Institute of Information and Communication, which is the cyber security laboratory conducts highly practical and macroscopic security research to promptly grasp, closely analyze, and provide effective countermeasures against evolving cyber attacks and carries out R&D regarding visualization for smart phone. Also MIC runs R&D for analysis and detection against cyber attacks and construct R&D center of excellence. METI promotes R&D for control system security.

3. Improving literacy

As to deal with smart phone, MIC promotes to utilize safe and secure WLAN and works on information security of smart phone with METI under the cooperation between public and private sectors. Also MIC reviews filtering of smartphone with METI, promotes personal information of smart phone as well as information security resulting from social media.

Third pillar of the Japan Cybersecurity Strategy: Constructing World-leading Cyberspace to strengthen ability in contribution and outreach

In order to keep up with a global cyberspace, "world-leading" cyberspace shall be constructed and attempts shall be made to strengthen contribution and outreach capabilities in the global strategic space by strengthening ministerial level dispatches, active participation in the international rule-makings, active outreach into overseas markets, capacity building support and confidence building measures.

1. Diplomacy

To strengthen building multilateral partnership with countries which share basic common values, high government officials of cabinet office, MOFA and related ministries develop a strategic approach. To enlarge discussion regarding application of exited international law for cyberspace, ministries get invoked in drafting code of conduct. Also cabinet office MOFA and related ministries participate expert meeting of the United Nations.

Convention on the Use of Electronic Communications in International Contracts to build trust and capacity building. To continue and expand dialogues on the basis of bilateral and multilateral countries, cabinet office, MIC, MOFA, METI and other related ministries enhance face-to-face dialogues regarding cyber security policy. Also they consult with U.K. and organize internet security forum with EU as well as launch national cyber security dialogues with Russia, Estonia, France and EU. All ministries intensify cooperation with U.S. based upon Japan U.S. security agreements.

This dialogue follows the first Japan-U.S. Cyber Dialogue held in Tokyo in May 2013, which inaugurated a whole-of-government approach between Japan and the United States on cyber policy. Officials from relevant ministries and agencies of the two governments have discussed wide-ranging bilateral cooperation on cyber issues, including critical infrastructure protection, capacity building, cybercrime, national security issues in cyberspace, and our common approach in relevant international venues. This dialogue is expected to deepen Japan and U.S. shared understanding of our respective organizations, policies, and operational architectures, as well as identify opportunities to strengthen bilateral cooperation mechanisms going forward.

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

2. International collaboration

Cabinet office, MIC, MOFA and METI promote cooperation between Japan and ASEAN for information security as well as cyber crime countermeasures. Japan also supports ASEAN for capacity building in terms of information security. METI promotes information sharing for early stage warning in Asia Pacific region in the framework of TSUBAME, which is a packet traffic monitoring system to observe suspicious scanning activities in the Asia Pacific region. It aims to promote collaboration among CSIRT in Asia-Pacific region by using the common platform and enhance capability of global threat analyses by incorporating 3D visualization features.

3. Promotion systems

NISC enhances its capacity as authority and reorganize to establish a Cyber Security Center around 2015 fiscal year. NISC has developed a framework that promotes the sharing information related to cyber attacks between government agencies and critical infrastructure providers. Specifically NISC increases the coverage of cyber attack related information sharing network in government agencies and decreases malware infection rates and citizen concerns, and increase the number of such nations as participating in national incident coordination. Also, NISC doubles the size of domestic information security market and to decrease the lack of proportion in security professionals.

Further Implications

Mainly, NISC has enhanced information security policy in Japan. Based on the escalation of risks that surround cyberspace and needs for strengthening response capacity for Olympics and Paralympics which will be held in 2020, further enhancement for NISC function is essential as a control tower.

Reviewing the efforts since the Japan Cybersecurity Strategy has been launched in June 2013, points at issues have been conducted discussion to bolster up the improvement systems of our cyber security strategy:

First, building system to utilize the knowledge of NISC for ministries and agencies as well as taking the lead form at government level to deal with immense cyber threat for Olympic and Paralympic Games in Tokyo. Therefore, it is crucial to strengthen the function of GSOC, post-survey for thorough investigation to determine serious incidents. Furthermore, deployment and training experts for research and analysis for cyber security situation and its foreign policy are essential.

Secondly, cross-functional paradigm should be beefed up and NISC needs to contribute to improve the security standards among ministries. Also implementing cross-cutting viable efforts for security policy among ministries are in demand.

Thirdly, intensifying information sharing and international collaboration for preparing globalization of cyber threats are necessary. Increasing capacity for summarizing information on cyber security incidents between government agencies and crucial infrastructure businesses. Coordinating some international contact points among public and private and enhancing manpower in terms of the perspectives are necessary to discuss.

Also the strategy could be revised depending on changing come out with the cyber security environment and taking measures against the Tokyo Olympics and Paralympics.

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

I have not referred in details regarding R&D for cyber security, public awareness and situation of cyber espionage and cyber intelligence. I would like to save it for another day.

***

Remarks: Opinions expressed in this contribution are those of the author.

Notes

1. Speech of Prime Minister Abe
   http://www.extremetech.com/extreme/188583-hackers-take-down-psn-with-ddos-and-sony-presidents-plane-with-a-bomb-threat
2. Japan Cybersecurity Strategy
   http://www.nisc.go.jp/active/kihon/pdf/cybersecuritystrategy-en.pdf
3. National Information Security Council
   http://www.nisc.go.jp/eng/
4. Japan-US Cooperation on the Internet Economy
   http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/Releases/NewsLetter/Vol21/vol21_04/vol21_04.pdf
5. National Institute of Information and Communications Technology
   http://www.nict.go.jp/en/index.html

About the Author

Dr. Yoko Nitta is a senior principal researcher at Japan Safe and Security Crisis Management. She has been researching foreign policies and has a keen interest in facilitating global cyber security among EU, US, Russia and Japan at an official policy level. Currently she focuses on cyber espionage, information warfare and intelligence. She has global responsibility of shaping its agenda and broad responsibilities for developing global bridges through her mission.

Dr. Nitta can be reached by e-mail: ynitta6666@gmail.com

Yoko Nitta

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de