# JAPAN’S APPROACH TOWARDS INTERNATIONAL STRATEGY ON CYBER SECURITY COOPERATION

**Yoko Nitta**
Japan Science and Technology Agency (JST) / Research Institute of Science and Technology for Society (RISTEX)
Tokyo, Japan
y2nitta@jst.go.jp

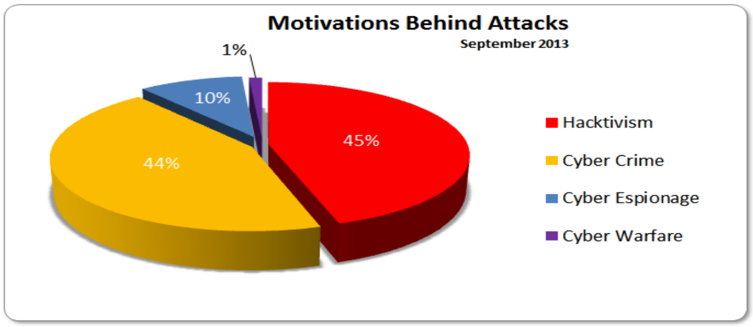
***The analysis contained in this paper is personal to the author and does not reflect the views of the JST/RISTEX**

*Abstract*—The Internet has grown so fast and the world has been interconnected and intertwined. The infrastructure surrounding us: power lines, water and electricity, has been connected by computer networks. Although we obtained this new technology two decades ago, we have been pursuing it without realizing its potential threats. Is the Internet secure enough in the first place? Have we grown accustomed to this new digital growth? Given the so-called ”uncertainties,” the convenvional system is failing while peope still are trying to stick to the traditional framework to pursue their existing interests. We are in middle of a disruption, a balanace shift, and a change in the rules of the game. Many countries call for international collaboration to deal with cybersecurity. International collaboration is based on trust, which is a fundamental element for security.

*Keywords— uncertainty; building trust; cyber attacks; Japan’s new strategy for cyber security, international collaboration; challenges; global governance*

Japan suffered well publicized cyber attacks in the past, such as breaches of parliament and military contractor Mitsubishi Heavy Industries Ltd in 2011. According to the Cabinet Secretariat, which staffs a small, 24-hour cyber-surveillance team, attacks on the Japanese government are continuing constantly. Government networks were hit by some 3,000 attacks a day in 2012, more than double the number in the previous year. The myths of security in Japan are collapsing as well as they are globally.

Figure 1: Motivation Behind Attacks



Source:http://hackmageddon.com/2013-cyber-attacks-statistics/

Following those incidents, the Cabinet Office launched a National Information Security Council in 2012 aiming to strengthen measures against sophisticated threats to companies and organizations handling national security information. Another goal was to maintain a safe and secure 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.

In Japan, four Ministries are responsible for cyber security: National Police Agency (NPA) works on stepping up its fight against cybercrime; Ministry of Economy, Trade and Industry (METI) takes initiatives for Cyber Security Information sharing Partnership Japan (J-CSIP) and deals with infrastructure; Ministry of Internal Affairs and Communications (MIC) is responsible for communication and network policies such as smart phone information security; and Ministry of Defense is in charge of national security and deals with information sharing. Although efforts of the Japanese Government have started bearing fruit, there is still a long way to go. Recent threats to cybersecurity are becoming larger, more advanced and more complicated. Also, threats against government agencies and industries have become a reality.

### *Japan's Cybersecurity Strategy*

On June 10, 2013, the Information Security Policy Council adopted the Cybersecurity Strategy. The Japanese government used to employ the wording, "information security," for its policy and Basic Plans. Since there is an increasing number of cyber threats, which are beyond information security such as sabotage of critical infrastructure, Tokyo decided to use Cybersecurity Strategy in order to address all of these issues for the first time. The strategy aims to develop "world-leading," "resilient," and "dynamic" cyberspace and make Japan a global leader in cybersecurity. The document has four basic concepts to realize the following: Ensure the free flow of information; provide new response to risks that are becoming more serious; responde to cyber threats on a risk basis; and take actions and cooperate with others based on the shared understanding of social responsibility.

Here are the main points of Japan's Cybersecurity Strategy:

- The strategy lists the following entities: nation, critical infrastructure-related companies, the industry and academia, individual users, "Small and Medium Businesses" (SMBs), cyberspace-related companies as cybersecurity actors.
- The government plans to give more authority to the National Information Security Center (NISC) in order to enable them to serve as a cybersecurity command and reorganize the NISC into a cyber security center by the end of March 2016.
- Japanese government has to take actions to make cyberspace "resilient": improving the level of information security; raising the security level to minimize supply chain risks; strengthening the capability to counter cyber-attacks; conducting annual exercises and simulations; recruiting and hiring of capable mid-career experts; and enhancing the information assurance system.
- Japan has to take actions to protect critical infrastructure: establishing an institute to evaluate and issue certificates for industrial control systems; adding more categories to critical infrastructure if cyber attacks cause significant impact on the lives of citizens and their socioeconomic activities.
- The academia and industry have to take actions, such as providing information and consultation for SMBs, providing incentives such as lowering taxes so that SMBs can invest more in information security and inviting SMBs to exercises.
- Hygiene for cyberspace is to launch "Cyber Clean Day" to raise awareness among users, create a database regarding malicious websites, and to improve the liability for software quality.
- To counter cybercrimes Japan must establish a version of the National Cyber-Forensics and Training Alliance (NCFTA), which the FBI has, and start discussions on logging, taking the secrecy of communication into consideration under the constitution.

Cyberspace is a new "domain" in addition to the other four—land, sea, air, and space. The Self-Defense Forces (SDF) are responsible for countering cyber attacks when they constitute part of an armed attack and establishing the Cyber Defense Unit under the SDF.

Japan has to take actions to make cyberspace "dynamic": revitalizing the industry; clarifing how much the Copyright Law is applicable to reverse engineering for cybersecurity; and creating advanced services based on big data analysis, research and development, education and training and improvement of literacy. Moreover, Japan has to take actions to develop “world-leading” cyberspace: Diplomacy for studying how international law such as the Charter of the United Nations and the international humanitarian law is applicable to cyberspace; establishing confidence-building to avoid escalation of tensions; and prioritizing cooperation with the United States as an ally, international cooperation for strengthening cooperation with developing countries such as the ASEAN; and strengthening cooperation with foreign law enforcement.

*International Strategy on Cybersecurity Cooperation: Initiative for Cybersecurity’s efforst at Maintaining the Integrity of the Specifications*

Japan needs to break out of security dependency. This has been an ongoing and controversial issue. An urgent task is to authorize the right to collective self-defense to break the siutation in which U.S. protects Japan.

Information Security Center (NISC) of the Cabinet Secretariat summarized a new plan, International Strategy on Cybersecurity Cooperation “J-initiative for Cybersecurity,” which is based on Japan’s Revitalization Strategy and the Cybersecurity Strategy adopted in June 2013. These plans establish international cooperation and mutual assistance in the field of cybersecurity as priority areas. This is the first time when the Japanese government strated collaborating with others in order to tackle cyber attacks as they are getting more sophisticated. Often we cannot defend ourselves against them using systems we currently have in place.

Government’s intention to work on information sharing and technical cooperation with other countries are to be evaluated and various concrete measures are required to be implemented. Given that China is the source of many cyber attacks, Japan invites technical cooperation with ASEAN and South America, among others. Japan can make important contributions to the global community since Japan has developed the world’s top telecommunication infrastructure such as nationwide fiber-optic and high speed wireless networks. Also, Japan has accumulated extensive knowledge and experience responding to cyber threats, development of cybersecurity technology and subsequent steps for its practical application.

Priority areas for the international cybersecurity cooperation strategy includes enhancing multi-layered mechanism for information sharing.  Enhancing cooperation among Computer Security Incident Response Teams (CSIRTs) is crucial to detect cyber incidents, analyze malware and IP addresses and to take response measures. In the strategy, establishing a multi-layered global mechanism for information sharing is imperative. The risk to control systems in terms of cyber attack on factories is becoming a grave concern at the global level. Responding to these urgent issues, Japan’s Control System Security Center (CSSC) has developed simulation enviroments. CSSC operates and improves their testbed and they work to shorten the time to acquire international certificates based on the evaluation criteria by third parties, establish an international recognition scheme for International Classification of Standards (ICS) for security evaluation and certification, promote standardization, and contribute to the enhancement of ICS security at the global level. One of their business milestones is to carry out strategic activities towards international standardization and promote the standards. In terms of international rulemaking for cybersecurity, Japan will institute an evaluation and authentication organization for promoting the use of such technology and will also contribute to activities of industries and organizations participating in the CSSC to propose new international standards using the CSSC. The core mission of CSSC is to protect the critical infrastructure from attacks of cyber terrorism.

## JAPAN’S PROMOTING INTERNATIONAL COLLABORATION

As to the Asia Pacific region, on October 2013 Japan and ASEAN made an agreement for raising awareness as a specific cooperation issue. American and Japanese defense chiefs made an agreement to establish a bilateral framework to discuss the means to counter cyber attacks on government branches and other organization. In addition, both countries will enhance network security through activities such as information sharing, technical cooperation for security through activities promoting the exchange of technical expertise. The United States and Japan have built a cooperative relationship to promote various efforts in the area of policy consultation, information sharing and cyber incident response through such platforms as the Japan-U.S. Cyber Dialogue and the Japan-U.S. Policy Cooperation Dialogue on the Internet Economy. Japan will continue to deepen this partnership. As for European countries, Japan has also built cooperative relationship to promote various efforts with shared values. For instance, Japan held the bilateral Japan-UK Cyber Dialogue and the Japan-EU Internet Security Forum. Japan also ratified the Convention on Cybercrime adopted by the Council of Europe. Japan will continue to strengthen these partnerships. Japan has worked within the framework of international legislative responses and cooperation such as Group of Eight (G8), United Nations, Organization for Economic Co-operation and Development (OECD) and Asia-Pacific Economic Cooperation (APEC).

With respect to policies for critical infrastructure protection and rapid incident response, global initiatives have also been undertaken at the Meridian and the IWWN (International Watch and Warning Network), as well as meetings as the FIRST (Forum of Incident Response and Security Teams) and the APCERT (Asia Pacific Computer Emergency Response Team). Sharing common values, Japan and NATO now seek to establish pragmatic collaboration on global challenges, including cyber, through NATO Science and Peace Security program in response to Prime Minister Abe's visit to NATO Director General in April 2013.

## CHALLENGE FOR TRANSFORMATION IN JAPAN

Japan has taken certain steps to step up its cyber defense such as establishing Cyber Security Group at the Defense Ministry, which is expected to be operational next year. In order to urge cooperation with other countries, Japan should strengthen domestic cooperation through information sharing. All theories aside, Japanese laws do now allow victims to hack back in retalliation against cyber attackers. Japan cannot even investigate who is doing the hacking under the current law. A law on secrecy and security clearances is a must to work on cyber terrorism and information sharing, which is the fundamental condition for international collaboration. The new law on secrecy has becomecontroversial in Japan because it still lacks important provisions including independent reviews what can be called in secret and a clear limit on the period of confidentiality. The Japanese government is responsible for explaining to its citizens the necessity of sharing information on the methodology of cyber-attacks and alert the public on the current threats so that Japan can minimize damages in a timely manner.

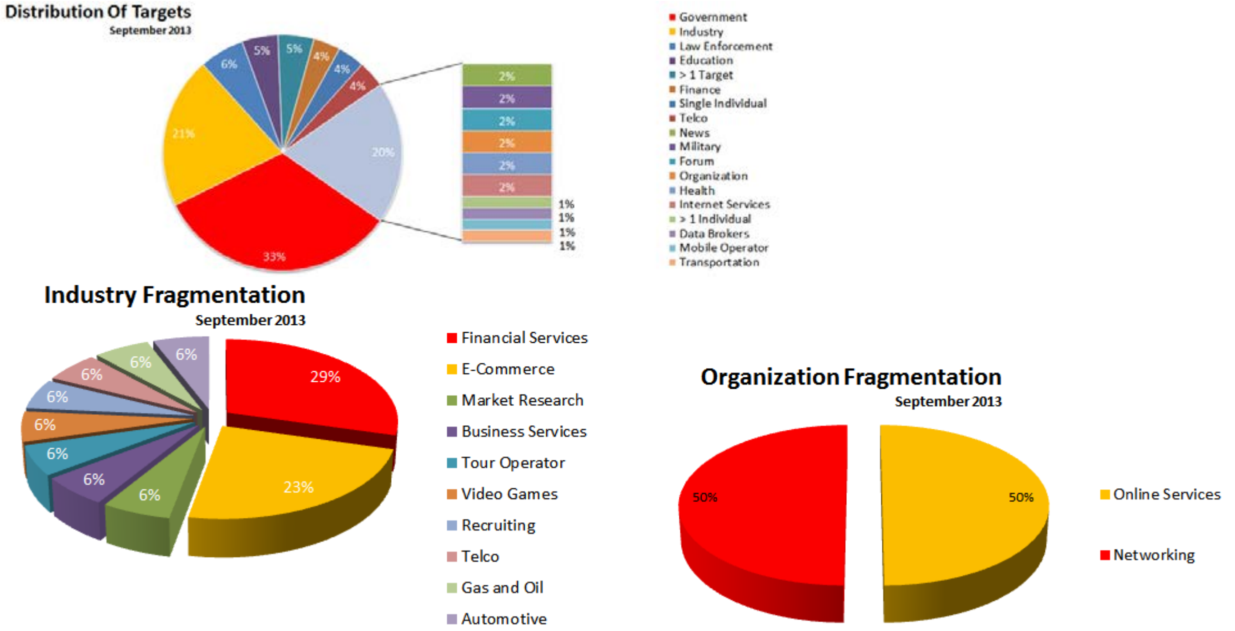
## IMPLICATIONS FOR FUTURE

While emerging countries believe that they should have a vote in the global structures of the 21st century, their voices are frequently not heard. Additionally, China has been advocating for a new world order, one that reflects America's declining influence in global affairs. This leads to global instability which has already resulted in fricitions. In this context, existing international security mechanisms are inoperative. Each day we cannot help but feel that we are losing ground—morally, if not phisically. We need to build new mechanisms to address the fundamental issue of growing distrust and bring our behavior in line with our rhetoric. Problems of cybersecurity are transnational; they cannot be solved uniletarally. Many countries and alliances are starting to realize this and have designated cybersecurity as one of the core national security intersts. Now that the Japanese government began addressing cybersecurity in earnest, the situation is moving in the right direction. However, it will be difficult to achieve success without coordinating operations of the various ministries involved.

Information sharing is a fundamental mechanism to respond to global cyber incidents. Establishing multi-layered response consisting of technology, law enforcement, policy and diplomacy is required. For cyber defense, support for emerging countries, where the Internet has been expanding rapidly, is crucial. Disseminating security technology is essential in Africa, in particular, where China is enjoying great influence. Also, training security technology experts is necessary to protect the Japanese government and industries from malicious cyber attacks which are getting more advanced daily. Domestic human resources training should be hastened for enhancing technical cooperation with other countries.

Japan has the good structures in place, but it needs more situational awareness. Do the current cybersecurity approaches bring peace and relief? The foremost characteristic of the new globalized world is the lack of trust, which makes us feel insecure. Strategies for overhauling the global governance system need to be reviewed and discussed. We also need to take international collaboration into consideration. This whole scenario has presented us with a world full of "complexities."

Figure 2 2013 Cyber Attacks Statistics



Source: http://hackmageddon.com/

REFERENCES

[1] National Information Securiyt Center (NISC) (2013)
[2] Cybersecurity Strategy - Toward a world-leading, resilient and vigorous cyberspace - (June 2013) Available at : http://www.nisc.go.jp/active/kihon/pdf/cybersecuritystrategy-en.pdf
[3] National Information Securiyt Center (NISC) (2013)
[4] Japan international collaboration for cyber security – j-initiative. Available at :http://www.nisc.go.jp/active/kihon/pdf/InternationalStrategyonCybersecurityCooperation_j.pdf
[5] National Information Securiyt Center (NISC) (2013)
[6] Critical Infrastructure Committee Available at : http://www.nisc.go.jp/conference/seisaku/ciip/dai33/pdf/33sankousiryou03-1.pdf

[7] By Tyler Roney The Diplomat , October 9, 2013
[8] With Obama MIA, China Touts Multipolar World (Available at : http://thediplomat.com/china-power/with-obama-mia-china-touts-multipolar-world/)

[9] North Atlantic Treaty Organization (NATO)
[10] NATO and Japan explore opportunities to cooperate on emerging security challenges , 5 Jun. 2013 – 29 Jun. 2013 (Available at :http://www.nato.int/cps/en/natolive/news_102417.htm )
[11] North Atlantic Treaty Organization (NATO)
[12] Sicnece for Peace and Security (SPS) (Available at: http://www.nato.int/science/about_sps/framework.htm. )

[13] 2013 Cyber Attacks Statistics (Available at: ) http://hackmageddon.com/2013-cyber-attacks-statistics/

[14] JOINT MINISTERIAL STATEMENT OF THE ASEAN-JAPAN
[15] MINISTERIAL POLICY MEETING ON CYBERSECURITY COOPERATION Tokyo, 13 September 2013 (Available at
http://www.meti.go.jp/press/2013/09/20130913005/20130913005-5.pdf