Viewpoint: Implementing Japan's New Cyber Security Strategy*

Presented by: The ACCJ's Internet Economy Task Force
Valid Through November 2014

The "2013 Cyber Security Strategy," released in June 2013, and the "International Strategy on Cybersecurity Cooperation", released in October 2013, by the Abe administration are enormous steps forward in Japanese government planning with respect to the mounting cyber security threat. They reflect both the dramatic increase in the external threat situation facing Japan and the government's commitment to take active steps to protect Japanese security and economic interests. The American Chamber of Commerce in Japan (ACCJ) welcomes these strategy documents as the start of what should be a vibrant and open debate on measures Japan will be taking unilaterally and in cooperation with the United States and other nations to protect cyber space. We urge quick implementation of the proposals contained in these documents after broad consultation among domestic and external stakeholders. As this process goes forward, we recommend focusing attention on to the following areas that we believe will further contribute to the successful realization of the new strategies' objectives.

RECOMMENDATIONS

Centralize Cyber Security Planning and Administration in a New Agency

The ACCJ applauds the recommendation to strengthen the role of the National Information Security Center (NISC) and expand its role, but we note the lack of the necessary legal mandate, budget or permanently assigned personnel to accomplish its multi-faceted mission. We believe that fundamental reorganization of the Government of Japan's (GOJ) planning and administrative approach to cyber security is urgently required in the light of the growing existential threat to Japan's economy and the security of its citizens presented by the cyber crime, cyber espionage and cyber targeting of critical infrastructure. Such a reorganization should give NISC or a wholly new agency a clear mandate to oversee (not merely coordinate) the diverse responsibilities and programs of existing ministries, thereby creating a strong and accountable focal point for the protection of domestic infrastructure, the promotion of cyber research, the training of key personnel and the implementation in and out of government of relevant standards. This new agency should also have the deep professional expertise necessary to support and coordinate national and local police forces in countering the cyber crime threats domestically and to allow the Self Defense Forces (SDF) to concentrate their limited resources on responding to national security threats as directed by competent civil authority.

Adopt a Japanese Equivalent Version of the U.S. Federal Information Security Management Act (FISMA)

In addition to an administrative reorganization of the government in responding to the cyber threat, Japan needs to strengthen the legal basis for government information security management. The Federal Information Security Management Act (FISMA) has been part of U.S. law since 2002 and has driven both greater accountability and cooperation across all U.S. government agencies in cyber security related programs. The ACCJ has been on record since 2009 in calling for a consistent procurement guideline without stifling diversity and innovation. Monitoring and enforcement of government-wide cyber security measures are key elements in achieving this goal and would greatly strengthen the hand of the newly named government Chief Information Officer (CIO) in setting a government-wide procurement strategy. A Japanese equivalent version of FISMA can provide a framework for overseeing new rules for the sharing of sensitive information and encourage the rapid deployment of new standards and technologies. Such rules should allow for a "safe harbor" mechanism to ensure that private sector entities are not punished for reporting attacks and include safeguards against "over classification" of information, which can create barriers to sharing.

Establish a Japanese Equivalent of the National Institute of Standards and Technology (NIST)

Any new administrative and legal framework will require a strong, technologically sound base. For that reason, the June cyber security strategy document should have been more explicit in its references to a standards-setting "institute" and should deliver an unambiguous call for the creation of an organization equivalent to the United States' National Institute of Standards and Technology (NIST), which plays a key role in supporting the U.S. cyber security agenda. An internal Liberal Democratic Party (LDP) taskforce in 2012 also called for creating a Japanese version of NIST. We strongly support this position and urge the GOJ to give priority to collaboration with U.S. counterparts to ensure interoperability with relevant NIST standards for cyber security and technology. While common security standards are important, at the same time, it is important that the GOJ also guard against mandating the use of specific technologies for achieving security goals. Technology in the security area is evolving very rapidly and premature standardization can stifle innovation and lead to a lagged response to security threats. We note that the October International Strategy document pledges GOJ cooperation in the creation of international technological standards for cyber security.

Introduce a Japanese equivalent to the FedRamp Program

Finally, we believe that the United States and Japan should consider new ways to work together in developing global "best practices" in the cyber security area. One opportunity is collaboration in building a version in Japan of the U.S. FedRamp program, which can assist government agencies in transitioning to the cloud consistent with world class security standards. Creation of a Japanese version of the U.S. National Cyber Forensics and Training Alliance (NCFTA), which focuses on a public/private partnership to share threat information and cyber technologies, is another example where the two countries working together can do more than they might separately. Both of these initiatives are important not only to improving government performance but also to supporting the GOJ role in providing leadership by example to private sector efforts in Japan to improve cyber security threat readiness.

Ensure New Security Measures Are Non-Discriminatory

The ACCJ appreciates the recognition in the 2013 strategy of the need to act in ways consistent with Japan's World Trade Organization (WTO) obligations in setting new security standards and rules for procurement and to consult actively with global Internet and cloud services providers in developing measures to protect critical infrastructure and promote industry best practices. U.S. and Japanese companies share concerns in India, China and other markets where new cyber security measures are routinely used to exclude foreign products and services and to undermine intellectual property protections. For this reason, we urge the (GOJ) to avoid actions that may weaken intellectual property safeguards below an appropriate level or make a distinction between cloud services offered from data centers within

Japan and those outside of Japan. Specifically, we are concerned that recent guidelines for cloud computing security drafted by the Office for Information Security Policy at the Ministry of Economy, Trade and Industry (METI) were developed without adequate consultation with relevant stakeholders and could give the impression to domestic consumers that cloud services offered from abroad are inherently unsafe.

Increase U.S.-Japan Cooperation on Cyber Security
We welcome the efforts of the GOJ to support greater research and development of security technologies and to promote investment and employment in this new market sector. However, we are concerned that these programs may not be open and transparent to foreign participation with appropriate safeguards. An urgently important topic for future bilateral consultation should be to create a framework between Japan and the United States to permit this kind of collaboration and the corresponding sharing of sensitive cyber-security information along the lines of similar arrangements with NATO countries. In this context, we support current discussions within the Diet to enact a "secrecy" law to ensure the confidentiality of sensitive government information. We also need parallel efforts to assure that other government data can be made widely available to citizens and for commercial use by business and that any new legislation does not become a barrier to the sharing of information necessary to bidding on government projects. We urge greater cooperation between the U.S. and Japanese private sectors in this area.

ISSUES

The March 20, 2013 cyber attacks on three major banks and the three largest TV broadcasters in Japan's neighbor, the Republic of Korea, were a wakeup call to all of us on the growing nature of the global cyber threat to governments, the private sector and critical infrastructure. As the New York Times has written, the focus of recent cyber attacks is shifting rapidly from "espionage" to "disruption." The South Korean attack, notable in that malware was used to destroy the Master Boot Record – whether Windows or Unix – was a clear escalation of the destructiveness of the threat, going beyond past examples of distributed denial of service (DDoS) attacks.

Japan has not been exempt from such cyber threats. In 2011, user names and passwords were stolen from computers in the Upper House of the Diet, and cyber attacks on eleven companies and research institutes, including Mitsubishi Heavy Industries, may have compromised sensitive data related to nuclear power. In 2012, the renegade hacker organization, Anonymous, defaced the website of Japan's Finance Ministry, and documents related to the Trans-Pacific Partnership (TPP) negotiations were illegally accessed on Ministry of Agriculture computers.

The Abe administration has set responding to the cyber threat as a key priority and is taking steps to increase public awareness and promote greater government collection and sharing of threat information with the private sector. It has also stepped up information exchange with the United States, with the first comprehensive round of cyber security consultations involving multiple ministries taking place in Tokyo during May 2013.

The June 2013 release of a new government planning document, "Cyber Security Strategy" and the October 2013 "International Strategy on Cybersecurity Cooperation (link to English summaries: http://www.nisc.go.jp/eng/) may be the most significant signs of new government activism and determination in this area. The ACCJ welcomes the new and complementary strategies as a significant evolution in GOJ thinking on the cyber challenge and as compelling and persuasive roadmaps, outlining a number of urgent actions needed to guard Japan's cyber space. We urge their rapid implementation in line with the 2015 timetable laid out in the June document.

BACKGROUND

Japan's efforts to protect and promote cyber security date back to 2005 with the creation of the National Information Security Center (NISC) within the Cabinet Office. The Center was charged with coordinating the government response to cyber challenges, although actual legal authority, budget, and staff resided as before with existing agencies, including the Ministry of Defense, the Ministry of Economy, Trade and Industry, the Ministry of Internal Affairs and Communications and the National Police Agency. A key NISC function has been the drafting of national plans, released in 2006, 2009, 2010 and 2013, and yearly updates. A review of the plans shows a gradual evolution in the Japanese government's grasp and response to the challenges in cyber space.

The 2006 and 2009 reports were produced under Liberal Democratic Party (LDP) governments and respectively labeled as the first and second "Information Security Plan." The emphasis in these reports was largely on technical solutions to security concerns and the introduction of preventive strategies. Ensuring information security was seen as critical to the competitiveness of Japanese industry globally and as necessary to alleviate Japanese small business and consumer concerns with the safety of their personal information on the Internet, especially in areas like banking, online commerce, healthcare and education.

The change in government with the Democratic Party of Japan (DPJ) victory in the 2009 election was the proximate reason for the issuance of a new plan in 2010, but the naming of the report and its contents departed in important ways from that of the previous two plans. The "Information Security Strategy for Protecting the Nation" was released against the background of large-scale cyber attacks against targets in the United States and the Republic of Korea and embarrassing leaks of personal data from Japanese firms. The economic dimensions of Internet security were still a motivating concern, but there was also growing recognition within the government of the threat posed by transnational cyber crime.

The "2013 Cyber Security Strategy" represents a further step down this path. Gone is the reference to "information security" in the title of the report. Gone, too, is the largely economic focus of previous plans. The emphasis in the new document is squarely on the national security implications of the threat. The report also takes up for the first time the topic "Internet of Things," indicating a keen awareness that Japan's highly advanced information and communications technology (ICT) infrastructure and the sensor networks it depends on may be more vulnerable to cyber disruption than in any other country.

The new plan is based on the concept of "risk management," recognizing that security is not an absolute. In the new threat environment, security is a dynamic and moving target, with informed trade-offs required to preserve the "openness" that is so vital to continuing innovation and competition on the Internet. The new strategy recognizes that cyber security is the business of all “stakeholders,” not just the GOJ. These stakeholders include not just traditional domestic infrastructure operators in areas like transport, energy and communications, but also a whole new group of direct and indirect Internet service providers, including many global providers of services to Japan -- among them prominent members of the ACCJ.

Most importantly, this strategy along with its companion document, “International Strategy on Cybersecurity Cooperation,” released in October 2013, include a number of significant and actionable proposals for strengthening Japan’s cyber security and improving international coordination against the cyber threat:

- Affirmation of NISC as lead agency for cyber strategy in Japan and its renaming as the “Cyber Security Center”
- Organization of a “cyber defense” unit within the Self Defense Forces (SDF) and legislative changes to set “cyber space” as a national security domain on par with land, air, sea and outer space
- Creation of an “institution” or “process” to set cyber standards for government and industry
- Government sponsorship of annual cyber threat simulation exercises for industry
- New measures for the handling of sensitive information to share cyber threat-related information within government and with the private sector
- Provision of incentives to support small business investment in and management of cyber security technologies
- Launch of “Clean Cyber” days and months to drive public awareness of the threat and solutions
- Clarification of the permissible range of “reverse engineering” for cyber security purposes in the Copyright Law
- Measures to promote research and development of cyber security technologies to support international competitiveness of Japanese industry
- Strengthened partnership with the United States and other countries that share similar values and interests with regard to cyber space
- Cooperation with Association of Southeast Asian Nations (ASEAN) member states for regional capacity building against cyber threats and to promote cooperation in dealing with cyber crime

CONCLUSION

Over the past decade, the cyber threat has expanded dramatically beyond the activities of a few individual hackers and criminal organizations to become a matter not just of business and economic security, but of national security. ACCJ members include companies that offer a wide range of ICT products and services to Japanese enterprises and consumers and have innovative technologies and deep experience directed to meeting the cyber challenge. We look forward to sharing this expertise with our Japanese business partners and to bringing new investments and technology to Japan in the cyber security area. We believe that Japan and the United States are natural partners in the area of cyber security and are strongest when we can work together as partners. The ACCJ appreciates the GOJ’s engagement on cyber security concerns with the U.S. government and welcomes opportunities through the U.S.-Japan Internet Economy Dialogue and other bilateral and domestic policy mechanisms to support this process.

Balancing the common interest in a robust legal framework with the free flow of information and freedom of speech and expression is a continuing challenge. The cyber threat challenge is difficult because it is multi-faceted, coming not just from cyber crime or espionage, but the growing ability of sophisticated adversaries to target and destroy critical infrastructure such as energy and communications networks. In this regard, a close partnership between the public and private sectors is essential in responding to the cyber threat and a broad national discussion on the appropriate balance between securing information and while allowing it to be freely shared is required. The ACCJ welcomes the GOJ's commitment to assuring the free flow of information and its recognition that freedom of speech, privacy protection and the promotion of innovation and growth also need to be core objectives for an effective cyber security policy.

Viewpoint: Implementing Japan's New Cyber Security Strategy*

*Note: This Viewpoint is not a standard ACCJ Viewpoint. Standard ACCJ Viewpoints are presented in both English and Japanese in a branded format (for other ACCJ Viewpoints, please visit: http://www.accj.or.jp/en/advocacy/viewpoints). This document, however, does represent the ACCJ's official position and will form the English portion of a forthcoming standard ACCJ Viewpoint.