PacNet
Number 41

Pacific Forum CSIS
Honolulu, Hawaii

June 28, 2012

Moving Forward with US-Japan Cybersecurity Cooperation

By Mihoko Matsubara

Mihoko Matsubara [Mihoko@pacforum.org] *is a cybersecurity analyst at Hitachi Systems and a non-resident fellow at the Pacific Forum CSIS. The views expressed in this article are those of the author and do not reflect the official policy or position of Hitachi or Pacific Forum.*

Countering cyber threats demands cooperation among nations, in particular public-private partnerships. The key is the timely exchange of warnings and follow-up information at the governmental, military, and private levels. Without prompt alerts regarding cyber-attacks or espionage methods and targets, all countries will find it difficult, if not impossible, to detect and prevent attacks. Countries, however, are struggling to identify common ground because they have different interests and concerns, as well as different approaches to privacy and regulations – for reasons ranging from national security to impact on economic growth. Thus, it is better to commence cyber collaboration with allies that share interests, economic models, and threat perceptions.

Japan and the United States have the most pressing need to cooperate on cybersecurity. They are the No. 1 and No. 3 economies in the world, and two of the largest military powers. They have and share more sophisticated technology for both civil and military purposes than any other countries. They have more to lose. If cyber-attacks and espionage undermine their economies or military capability, larger geostrategic balances may be affected and the negative consequences may spill over to other countries.

In June 2011, Tokyo and Washington issued a joint statement confirming the importance of cybersecurity cooperation for the first time at the US-Japan Security Consultative Committee. The first Japan-US working-level dialogue on cybersecurity was held in Tokyo in September 2011. The two governments agreed to establish a mechanism to share information on cyber-attacks. Prime Minister Noda Yoshihiko and President Barack Obama then issued a joint statement, which reconfirms the necessity of cybersecurity cooperation and encourages the expansion of public-private partnership, after their summit meeting on April 30.

However, no specific strategy and vision have been provided for the public to show the division of responsibility between the two governments. Ultimately, bilateral cooperation will rest on national-level efforts, which will need to be anchored in public-private partnerships.

Unfortunately, public-private partnerships are weak in Japan due to the lack of strong leadership in unifying information channels and a reluctance to report vulnerabilities. The National Information Security Center (NISC) under the Cabinet Office is responsible for crafting Japan's national cybersecurity strategy. Yet, the center lacks authority or compel the public and private sectors to submit information on cyber threats or to impose recommended countermeasures. Moreover, private companies are hesitant to report their vulnerabilities due to concerns about potential damage to their reputations and benefiting competitors by sharing information on their products.

Within the government and military, robust information assurance is a fundamental prerequisite to exchange intelligence because the information being shared includes potential/actual targets and reveals vulnerabilities in networks and computers. Given the sensitivity of information being exchanged, Tokyo and Washington need confidence in the other's information assurance and security clearance systems. Sadly, Japanese systems are not robust. Ministries and agencies do not have a shared security clearance system that allows them to exchange classified information smoothly. This makes it difficult to prevent and punish cyber espionage. This will discourage the US government from sharing more cybersecurity information.

Moreover, Tokyo does not have an anti-espionage law due to strong resistance from the media, lawyers, and opposition parties that prioritize public access to information and freedom of the press. Given the dark legacy of prewar censorship, they are concerned that the government might arbitrarily use the designation "secret for national defense and diplomacy purposes" and violate the rights of the public and media.

Last October, the Noda administration declared that it would submit a bill for secrecy protection to the Diet in 2012 to stiffen penalties against government officials who leak classified information. The government abandoned that idea in March 2012 because the ruling Democratic Party of Japan decided that the current Diet session has too many bills on its agenda, including reconstruction after the 3/11 triple tragedies. Compounding the reluctance to proceed was the party leadership's belief that the resistance would be too strong.

Yet, if Japan fails to strengthen its information assurance, it will be difficult to bolster relations between the Self-Defense Forces (SDF) and U.S. military – or between the two governments. A cyber-attack on infrastructure could cripple military operations by limiting the electricity for command and control communications, data links, and GPS. Thus, as one measure, Japanese and US forces should start joint exercises on working together in a degraded information environment. Although the US Air Force has already begun such training, insufficient SDF information assurance rules discourage Washington from sharing sensitive lessons learned.

A stronger security clearance system will also require the revision of the court system. Article 82 of the Japanese Constitution requires trials and judgments to be available to the public. The SDF is regarded as non-military under the Constitution and does not have a military court. This means that all cases are sent to open courts and could lead to leaks of sensitive information.

There is another wide-ranging problem: comprehensive partnerships in the private sector hardly exist except for cooperation between individual companies. In March, the Japan Business Federation (Keidanren) and the American Chamber of Commerce in Japan (ACCJ) issued a joint statement that recommends more public-private cooperation to devise countermeasures against cyber-crimes and -attacks. Following up on this, the Federation and ACCJ should take the initiative to launch a company-based collaborative framework to share information. This will constitute a critical part of the public-private partnership to help understand what kinds of information, protection, and regulation companies want and need.

To promote cybersecurity cooperation with the United States, Japan needs to take actions to strengthen the NISC authority, information assurance, and public-private partnership. Timely information sharing is indispensable not only for bilateral cybersecurity but also for a tighter and stronger alliance.

PacNet commentaries and responses represent the views of the respective authors. Alternative viewpoints are always welcomed.