PacNet
Number 4

Pacific Forum CSIS
Honolulu, Hawaii

Jan. 14, 2015

Cybersecurity cooperation with Taiwan: an opportunity for the US-Japan alliance by Julia Cunico, Nien-chung Chang Liao, Daichi Uchimura, and John K. Warden

Julia Cunico (julia@pacforum.org) is the director of the Pacific Forum CSIS Young Leaders Program. Nien-chung Chang Liao (clnc@alumni.nccu.edu.tw) is a post-doctoral research fellow at the Institute of Political Science at Academia Sinica. Daichi Uchimura (alfred.geopolitik@gmail.com) is a non-resident Sasakawa Peace Foundation fellow with the Pacific Forum CSIS. John K. Warden (jkwarden@gmail.com) is a WSD-Handa Fellow at the Pacific Forum CSIS.

The United States and Japan pushed back the release of the newest version of the US-Japan Defense Cooperation Guidelines – a strategy that outlines common objectives and priorities of the two allies and how each country, and the alliance, can contribute to desired outcomes – until the middle of 2015. The two countries, however, should not allow the document's delay to slow the transformation of the US-Japan alliance, which must move beyond planning for traditional military missions in and around the Japanese archipelago and incorporate efforts to counter nontraditional security threats and to build regional and global partnerships.

From the interim report, we know that the two primary focuses of the updated Guidelines will be, first, the need for a seamless US-Japan response to "grey zone" situations – challenges to Japan's security that fall short of a direct military attack – and second, how the United States and Japan can address China's anti-access and area-denial capabilities. The Guidelines will also stress the importance of reaching out to partners in the Asia-Pacific to address challenges in new areas such as cyberspace. It is in the latter two areas that the United States and Japan have a real opportunity.

The United States remains a global power with global interests and global engagements and, under the Barack Obama administration, has reprioritized the Asia-Pacific. Japan under the Abe Shinzo administration has taken on a greater leadership role in the region, as evidenced by the Prime Minister's frequent visits to regional capitals. Yet despite high-level bilateral coordination, there are few examples of the United States and Japan moving beyond ad hoc engagement to work with a likeminded partner to address a key security challenge. Therefore, when the United States and Japan begin to operationalize their new Defense Cooperation Guidelines, they should work to create an institutionalized mechanism for cooperating with Taiwan, an ally of neither, but a friend of both, to address cybersecurity threats.

The hack of Sony Pictures has refocused attention on cyber threats, showing the significant disruption that can result from even a relatively minor cyber incursion. However, North Korea, who is thought to be behind the hack, is less capable than China, whose military cyber capabilities pose a major challenge for the US and its friends and allies. Actors ranging from nongovernment hackers to People's Liberation Army (PLA) cyber forces frequently use remote infiltration and malware to infect computers, steal information, and monitor websites in Taiwan, affecting the normal operation of the Internet. In the worst case scenario – a conflict in the Taiwan Strait – PLA cyber forces will attempt to cripple Taiwan's command, control, and logistics network. Chinese hackers also, according to reports, use Taiwanese networks to test cyber-attack strategies they plans to use elsewhere and take over Taiwanese computers to use them as springboards to attack more secure networks. In both cases, the common language between Taiwan and China makes the former a convenient target.

For this reason, the United States and Japan, two countries that face frequent cyberattacks originating in China, should have particular interest in cooperating with Taiwan. There is already some cybersecurity cooperation, but it is informal, ad hoc, and focused exclusively on cybercrime. Taiwanese and Japanese firms have informal cyber-focused discussions, and both Taiwan and Japan have separate information exchange and training programs with the United States. The most prominent example of US-Taiwan cooperation occurred in 2014 when Taiwan's leading cybersecurity company, Trend Micro, helped the US FBI arrest and convict members of SpyEye, hackers who produced viruses that affected 1.4 million computers globally. Japan's National Information Security Center has its own "Cyber Security Strategy," which highlights the importance of bilateral policy cooperation dialogues with the United States and several other countries, but makes no mention of Taiwan.

Because cyber threats range across a broad spectrum, there are a number of steps that Taipei, Tokyo, and Washington can take to institutionalize cyber cooperation. The most fruitful area, at least initially, is between law enforcement agencies. The Department of Homeland Security's United States Computer Emergency Readiness Team Coordination Center, the Taiwan Computer Emergency Response Team Coordination Center, the Japan Computer Emergency Response Team Coordination Center, and the Japan National Information Security Center should enhance capacity in each country by establishing a formal partnership to share information about Internet security. Together, the United States, Japan, and Taiwan should establish a data fusion center that functions as an information-sharing pipeline. Working at this center, law enforcement officials could establish a common database on cybercrimes and assist each other with prosecutions.

Eventually, the three countries will move to more politically sensitive areas of cyber cooperation, which would

allow each country to better prepare for cyberattacks, mitigating security risks and preventing economic losses. The United States, Japan, and Taiwan should work together to identify networks and companies that are at risk, develop an early warning and rapid response system, and research new ways of detecting viruses that go beyond identifying signatures from past malware. An agreement on "intelligence sharing" is likely too politically sensitive, but the three countries should be able to establish lower-level and functional agreements on "network safety enhancement" or "joint cybercrime fighting" aimed broadly at cyberattacks and crimes and without specifically targeting a third party. Taipei and Tokyo have signed low-profile agreements in areas such as e-commerce, sea search and rescue, and financial supervision, which provide a model.

An additional benefit of US-Japan-Taiwan cyber cooperation would be shaping China's behavior. First, the three partners could contribute to evolving cyber norms by generating a common understanding of the thresholds between different types of cyber activities; when, for example, does a cyber incursion become an attack? As the norm expands, China's cyber activities would face greater scrutiny and international condemnation. Second, while US-Japan-Taiwan cooperation on offensive cyber weapons is a bridge too far, establishing strong ties in cyberdefense would lay the foundation should offensive cooperation be necessary. This potential alone would signal to Beijing that escalating Chinese cyber activities could have a substantial cost.

Engaging with Taiwan to address cybersecurity would demonstrate that the US-Japan alliance can function as a framework for engaging regional partners to address specific challenges. Cooperation would bring tangible cybersecurity benefits to the United States, Japan, and Taiwan, enhance US-Japan-Taiwan relations, and establish a model for future US-Japan engagement in the Asia-Pacific.

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