PacNet
Number 84

Pacific Forum CSIS
Honolulu, Hawaii

Dec. 13, 2012

Public-private partnership programs are key in cyber collaboration agreements in the Asia-Pacific region

by Ria Baldevia

Ria Baldevia (riabaldevia@gmail.com) is a Hawaii-based web & digital strategist for small businesses.

The Obama Administration's strategic rebalance toward the Asia-Pacific region presents an opportunity for the United States to establish and strengthen strategic cyber alliances. The basis of this effort should be a private-public partnership program to address cyber defense and cyber intelligence sharing. A multi-pronged approach to cyber security that promotes military relationships, diplomacy and public-private investments in India, South Korea, and Japan is a smart move considering economic relationships, political alliances, and an existing dialogue focused on cyber security in the region. These alliances should comprise three separate bilateral agreements between the US and its Asian counterparts.

Bilateral cyber intelligence sharing agreements with India, South Korea, and Japan is an essential component of US foreign policy as the country pivots toward Asia, but that is not enough. Identifying areas where both the US and Asian countries can implement public-private partnerships is also essential.

The US has frameworks for both cyber intelligence sharing and public-private partnership components that can be used as guidelines for these cyber collaboration pacts. An example of intelligence sharing agreements is the Five Eyes Agreement, also known as the UKUSA Agreement. This memorandum of understanding among the United States, United Kingdom, New Zealand, Australia, and Canada operationalizes the sharing of communications intelligence. Furthermore, the current US-India Strategic Dialogue fosters cyber intelligence sharing. This needs to be replicated in separate cyber collaboration pacts with South Korea and Japan.

The US public-private initiative in cyber security exemplifies how private industry can be part of the solution, especially in identifying talent. The National Board of Information Security Examiners' US Cybersecurity Challenge (USCC) offers opportunities to identify talent at home. Under the USCC, the United States Air Force Association (AFA) and Northrop Grumman have sponsored an initiative in US high schools to begin to recruit talent to address our cyber security needs. The UK's similar Cyber Security Program includes a competition or "hackathon" that is sponsored by GCHQ, the British signals intelligence agency. Winners represent potential talent to be recruited. Applying these types of public-private efforts to the Asia region would help strengthen our cyber collaboration with the region.

Asia is home to the most highly Internet-penetrated societies in the world: 44.8 percent of all Internet users live in Asia. India, South Korea, and Japan have a total of nearly 300 million Internet users. India has the second greatest number of Internet users in Asia (second to China); and South Korea and Japan have Internet penetrations of 83 percent and 79.5 percent, respectively. The likelihood that the digital infrastructure rests primarily in the hands of private industry is high in countries with high Internet penetration.

Industry and government agencies ranging from banking, electricity, trade, medical care, and education are inextricably linked through digital networks. This interconnectivity in cyberspace leaves these countries' entire infrastructure vulnerable to attack. If even one element of a private or public agency is attacked, disruption of multiple systems could result, with potentially disastrous consequences.

India

The Indian government has recently been more open and receptive to US cyber security policies and objectives. In September, the United States and India engaged in their second cyber drill that focused on phishing, malware attacks, spam, and other cyber security issues. The US needs to capitalize and build upon that political will and burgeoning cyber alliance. The US-India cyber cooperation pact needs to go further and address public-private partnerships in India. Such partnerships will highlight the need for private firms, who control most of the country's information infrastructure, to become part of the cyber security dialogue and influence policy that will promulgate India's cyber security.

South Korea

South Korea has already been the target of multiple North Korean cyber attacks. Last year, South Korea's Nonghyup Bank was reportedly hacked by North Korea. This was one of several distributed denial of service (DDoS) attacks North Korea launched against its southern neighbor. Additionally, North Korea was caught attempting to hack South Korea's Incheon International Airport digital infrastructure in 2012 but was caught by the Seoul Metropolitan Police Agency. The DDoS attack against Nonghyup Bank highlighted the detrimental effects a cyber attack could have on individuals, their daily lives, businesses, and other assets. With the highest Internet penetration in the world and a flourishing economic relationship with the US, it is important for South Korea's private industry to be involved in the cyber security dialogue. A US-South Korea cyber collaboration agreement that includes fostering a private-public partnership, to ensure a stable South Korea cyberspace, as a supplement to military and diplomatic cooperation, is a win-win solution.

Japan

Japan has plans to establish a cyber defense network in 2013 under the defense ministry. Japan considers its cyber defense strategy the fifth area of defense along with land, sea, air, and space. Japan's cyber defense network aims to identify viruses, defend against cyber threats and attacks, and strategize counterattacks in cyberspace. The US has an opportunity to establish a cyber cooperation pact with Japan as the country finalizes its cyber strategy. One area that can be addressed is the training and retention of skilled cyber security specialists in the country. Currently, Japan is having trouble staffing its 100 member cyber defense network due to a lack of skilled cyber security specialists. A US-Japan cyber collaboration pact can lay the foundation for military and diplomatic cooperation, but can also address the country's cyber defense human resource needs by encouraging private local industries to invest in identifying and training talent.

Creating a strategic cyber alliance that includes public-private partnerships in addition to military and diplomatic collaboration represents a proactive policy of defense in cyber security, something that is critical in today's digitally interconnected world.

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