One Hundred Thirteenth Congress

Congress of the United States

Committee on Foreign Affairs

Subcommittee on Asia and the Pacific

July 23, 2013

Asia: The Cyber Security Battleground

Chairman Steve Chabot (R-OH)
Opening Statement

Over the course of the last few years, there has been growing acknowledgement of the need for an international cyber security policy. The growing interdependence of the world by way of the internet, and vast frequency and similarity of cyber attacks reported in nearly every corner of the earth, illustrates why.

As they say, cyberspace knows no borders. This implies that cyber security is only as good as its weakest link. In other words, we can work tirelessly to build up the defenses of our critical infrastructure systems and networks here in the U.S., but backdoors could still be found in overseas routing points and links in the global supply chain, for example, through which adversaries can find ways to attack U.S. government systems and private companies. This is why the U.S. must engage its allies around the world to promote the preservation of global network functionality, in addition to establishing confidence building measures that foster trust and reliability with nations that have become Wild West havens for cyber criminals—so that we can close these backdoors.

As an effort to recognize cyber security's growing international attention and importance, the State Department established the Office of the Coordinator for Cyber Issues in 2011 to more effectively coordinate global diplomatic engagement on cyber issues. It was around the same time that the White House issued its international strategy for cyberspace. While we are not here today to discuss the progress or effectiveness of this still relatively new State Department office, I think at the very least it is an acknowledged step in the right direction—even if they could not somehow provide anyone to brief the Subcommittee on its activities before this afternoon. Even so, today's hearing is part of our efforts here in Congress to examine how to advance this strategy in such a critical region of the world as Asia.

Almost every day, U.S. businesses are victims of cyber exploitation and theft by nation-state actors such as China. Theft of intellectual property not only takes away American jobs and hurts innovation and competitiveness, but it costs U.S. businesses somewhere between $2-400 billion a year. In order to ensure American economic prosperity and security, the integrity and openness of our networks must be maintained. And as we discuss this afternoon the evolving threats and growing number of cyber challenges facing our nation, I recognize this will be no easy task.

Asia is a region beset by some of the world's most aggressive cyber actors. I think it's fitting that today's hearing calls the region "the cyber security battleground" because as Asia has become the most economically dynamic region in the world, it has also become the hub of cyber conflict. Alternatively, while Asia is not an actual battleground as we know one to be or in the throes of a drawn out war, this term symbolizes that the region is faced with many serious threats and actors that are unstable, uncertain and volatile. It is unlikely for a real cyber war to start between Asian nations, at this point, but it's critical to note how cyberspace has become a source of great economic and military rivalry, as well as the primary medium for political activism. As we know, in many Asian nations, political dissent via the internet is obstructed by ruling governments and considered a threat. An issue we discuss here frequently, this is a source of great internal conflict and human rights abuses.

Nevertheless, it is the networked interconnection of our lives, information, financial systems and institutions that is enabling global business to expand and thrusting growing Asian economies forward, providing before unavailable economic opportunities to people throughout the region. Competition is growing, and with the growth of competition, has come the growth of malicious activities aimed at stealing economic and military secrets for groups and nations to get ahead. Nearly every military in Asia will eventually have some level of cyber capability, if they don't already, and because of cyberspace's lack of security or established set of norms, the risk of miscalculation only grows. This is why regional engagement on cyber is imperative because building trust, capacity and security is not going to be easy and it will take time.

The "cyber powers" in Asia include the U.S., China, Taiwan, South Korea, North Korea, and Australia. Just like many other issues in Asia, the growth of cyber capabilities in these countries and other Asian nations revolves around China's strength and growing desire for influence. China has been called by numerous high-level officials in the Obama Administration an advanced cyber actor and an aggressive practitioner of economic espionage against the U.S., and no doubt, our allies in Asia as well. The instances in which China was behind cyber attacks or intrusions of U.S. government systems and companies are endless. While I think that opening dialogue with the Chinese about cyber crime, theft and espionage is good, establishing some sort of norms or principles to guide actions in cyberspace that the Chinese can agree to will be incredibly difficult. China will continue to deny accusations and its behavior is unlikely to change.

Similarly, North Korea's behavior has shown its aversion to change; however, the Kim regime is not only unstable, irrational, and erratic, but it is also risk averse. North Korea's growing cyber capabilities present the greatest likelihood of cyber conflict in Asia. Earlier this year, it demonstrated its capabilities in South Korea, where it crippled the operations of banks and news agencies, wiping the hard drives of thousands of computers. While McAfee's report on what is now called Operation Troy does not attribute these attacks to North Korea, it could not be clearer who is responsible. North Korea is not only a nuclear threat, but it is a serious cyber threat as well.

Lastly, we cannot forget the cyber threats emerging from Pakistan that challenge the national security of the U.S. and its neighbor, India. Mutual distrust dominates the relationship, which severely hampers opportunities for bilateral cooperation. As home to numerous terrorist groups, the cyber risks materializing from Pakistan are exceedingly multifarious. Just the other day, the director of the National Security Agency said “Terrorists use our communications devices. They use our networks…they use Skype, they use Yahoo, they use Google…and they are trying to kill our people.” Cyber terrorism is real.

I look forward to hearing the witness’s testimonies today and thank each of you for making the time to be here. The private sector’s role in building cyber collaboration and awareness in Asia is just as important as what our Administration is doing, so I am glad we have a diverse panel here today.

I now yield to my friend from the American Samoa, the Ranking Member Mr. Faleomavaega, for his opening remarks.