Testimony
Subcommittee on Asia and the Pacific
House Foreign affairs Committee
"Asia: The cybersecurity Battleground"
James A. Lewis
Center for Strategic and International Studies
July 23, 2013

I would like to thank the Committee of this opportunity to testify.

Cybersecurity is a volatile issue in Asia. The flashpoints are rampant Chinese cyber espionage and its destabilizing effect on relations with the US and other Asian nations, and the North Korean cyber attacks on the Republic of Korea. China and the U.S., the two major cyber actors in the region, have been careful to keep their activities below the threshold of armed conflict. Even the actions of North Korea against South Korean targets do not clearly rise to the level of the use of force that would justify a military response.

There is a military competition in cyberspace as nations build cyber capabilities, but both China and the U.S. only intend to use these capabilities only in the event of war. The primary problems are political and economic. Spying is not warfare and does not justify the use of force in response by the victim - the U.S. itself should be glad of this. It is not in our economic interest and certainly not in China's economic interest, given the steady weakening of their economy, to see the issue deteriorate into an armed clash. Cybersecurity as an issue for international security is best addressed using diplomatic and trade tools. Our goals should be to prevent escalation into armed conflict and build cooperation in cybersecurity.

There is a risk that we could find ourselves in a conflict, given the deep problems between the U.S. and China and the worsening public perceptions on both sides. Avoiding miscalculation and escalation, where one nation mistakenly assumes that espionage or political action is the precursor to an actual take is a problem for the U.S. and China and for the region. Adjusting to and managing China's rise is the fundamental security problem for the region, a problem with global implications as the Pacific regions displaces Europe as the world's economic engine.

For cybersecurity as with other Asian security and economic issues, the rise of China is the central problem. China's cyber actions are a threat to stability in Asia. Chinese espionage – political, military and economic is rampant. The U.S. is not the only victim. Australia, India, Japan, the Philippines, the Republic of Korea, Russia, Vietnam and perhaps others have been the victims of Chinese cyber espionage. The Chinese are "noisy" in their operations, making them relatively easy to detect. Chinese foreign policy is bumptious. They do not have the experience of the U.S. or Russia in managing security disputes. More importantly, China's cyber activities cannot be divorced for the larger security and political context in Asia, where Chinese actions have alienated many of its neighbors and have increased tensions by attempting to assert its regional authority.

The Chinese would portray things somewhat differently. They are still deeply marked by the "Century of Humiliation," where European powers and Japan carved their country into colonial fiefdoms. The Chinese are suspicious of the United States, particularly in the PLA, which has not shed enough of its Maoist heritage. The Chinese are convinced that we have a "Grand Strategy" to preserve our global political, military and economic hegemony and that part of this strategy is to contain a rising China. They see the discussion of an "Air-Sea Battle and a "Pivot to Asia" as confirmation of U.S. hostile intentions. China's own cybersecurity efforts are hampered by the use of pirated software, which is almost unsecurable, making China one of the easiest countries in the world to hack. Chinese official know how vulnerable they are and this reinforces their suspicions and fears.

The Snowdon revelations, while embarrassing, have not had as much effect on Chinese policy as you might think (although we should not discount the effect on the larger U.S. multilateral effort). In discussions with China they U.S. has always been clear that espionage is a two way street, something that all great powers do, and that espionage against military and political targets is legitimate. What we object to is the economic espionage, the stealing of commercial secrets where there is no national security value. We also emphasize that rampant commercial cyber espionage creates a risk of misperception and miscalculation where a mistake could escalate into a much more damaging conflict. This frankness makes it hard, at least in private, for the Chinese to object too much, although they clearly enjoy our embarrassment wand will see how much diplomatic advantage they can get from the incident.

This month's meeting of the Security and Economic Dialogue and its Cyber Working Group are an important step that, if it succeeds, will make the situation in Asia more stable, but we are looking at a long effort and the S&ED process will need to be sustained and reinforced. One precedent can be found in the successful effort to engage China on nonproliferation in the 1990s. The U.S. and it allies created international norms that established that responsible states did not engage in proliferation. The U.S., supported by its allies, met regularly with Chinese officials to make this point and providing the Chinese with specific examples of objectionable behavior. Senior U.S. officials and leaders from European countries and Japan made the point that China's involvement in proliferation would harm China's relations with the rest of the world. This multilateral approach was important, as it demonstrated to the Chinese that nonproliferation was not solely an American concern. Finally, the U.S. used or threaten to use sanctions and measures to encourage a change in China's behavior.

The precedent is not perfect because the relationships of power and influence among key nations have changed. China is more powerful and Europe is weaker; China may believe it self to be less dependent, and it is certainly more confident. It is unlikely that many Asian countries will be willing to engage China on cyber espionage and even some major European allies, such as Germany, are unwilling to put business interests at risk even though it has suffered from cyber espionage. This will be a difficult process and cyber espionage has become a flashpoint in Asia and in the bilateral relationship. In this, the U.S. is the only interlocutor that can lead in effectively engaging China to bring its cyber actions in line with global practice.

China will find it difficult to bring cyber espionage under control even if it chooses to do so. Cyber espionage plays an important part in the growth of the Chinese economy and Chinese leaders will be reluctant to put this at risk at a time when their economy is slowing down. Cyber espionage is a moneymaking activity for the PLA and others and President Xi may need to find some way to compensate them they are to get out of the cyber espionage business. There will be a domestic political price for Beijing to bring cyber espionage under control and little incentive for the party's leadership to pay this price absent external pressure and a changed view of what best serves China's own interests.

U.S. and Chinese interests for Asia have much in common when it comes to cybersecurity, are, but cooperation is increasingly blocked by mistrust and competition. U.S. and Chinese interests in cyberspace are symmetric in some areas – reducing the chance of miscalculation that could escalate into military conflict – but diverge widely in others, chiefly over political control of the internet. This is an area of divergence, but unlike political control of the internet, which Beijing sees as essential for regime survival, there is scope for progress in changing China's behavior.

To achieve this, the U.S. will need a long-term diplomatic strategy linked to our larger goals for cyberspace in Asia and the world. The U.S. must manage and reverse Chinese economic espionage while avoiding military or trade frictions. It must modify its existing alliances with Australia, Japan and Korea to make collective cyber defense more than a slogan. It must build a relationship with India on security challenges. All of this must be done as the U.S. helps to lead a global effort to develop norms for responsible state behavior in cyberspace to make it more stable and secure, an effort in which ASEAN nations play an important role.

This is a complex picture with many moving parts. The bilateral U.S.-Chinese relationship is at the heart of the issue, but other Asian nations will consider both their relations with the U.S. and their relations with China. They want to find some way to balance both. China is too important as a market and the U.S. is too important as a guarantor of regional stability. Asian nations would prefer not to have to choose between the two, although there is a growing discomfort with Chinese cyber activities that plays in the U.S.'s favor.

This is not a new Cold War. No Asian country, including any of our allies, is interested in a Cold War with China. Looking to a conflict that ended more than twenty years ago to explain the current situation is a sign of conceptual bankruptcy. China is at the center of Asian markets in a way that the Soviet Union never was. Asian economies are too interdependent for the bipolar separation of the Cold War. This lack of interest in a Cold War among Asian nations also means that China's fears of "containment" are a reflection of its own fears rather than an accurate assessment of the situation.

There are military tensions but this is not a problem where militaries can play a useful role. Each country has elements that define the bilateral relationships in terms of military competition, particularly in the PLA, and Chinese society can be prone to fits of hyper-nationalism, but if China wants to continue to grow and if the U.S. wants to remain a global leader, we have to find ways to cooperate in Asia. It is not in our interest to start a military conflict with China, nor is it in our interest to damage the Chinese economy. Similarly, a trade war between the U.S> and China would damage the global economy - something that could unleash another global recession.

If the problems for Asian cybersecurity are Chinese espionage and North Korean bellicosity, the answers lie in engagement with China, creating international commitments on cyberspace, and in modifying existing U.S. collective defense agreements to apply to cybersecurity.

The U.S. has collective defense arrangements with Japan, Korea, and Australia. All are being modified to include cooperation on cybersecurity. One issue for collective defense comes from the differing capabilities of the partners. Another involves the difficulty of sharing sensitive information with partners whose ability to protect it may be less effective than we would wish. The U.S., in modernizing collective defense, must avoid the impression that it is building a regional alliance to contain China. The largest problem involves defining what collective cyber defense means and what actions would be required under our treaty commitments, particularly because most malicious cyber actions fall below the threshold of an armed attack that would clearly trigger collective defense.

The U.S. and Australia have a special relationship and they agreed to add cybersecurity cooperation to the existing defense treaty in 2011. Australia faces extensive Chinese espionage efforts and has made considerable progress in developing its national cybersecurity programs - in some areas, it is ahead of the U.S. The relationship with the U.S. makes an important contribution to Australia's national cybersecurity effort. Australia must take into account its close economic ties with Beijing as it strengthens security ties with the U.S., but in cybersecurity, there is a strong existing relationship between the U.S. and Australia and a large commonality of interests in defense cooperation and in the creation of a stable international order for cyberspace.

Japan, like Australia and the U.S., has suffered from extensive Chinese cyber espionage. Japan has in the last year undertaken a number of actions to improve cybersecurity. These include the publication of a new cybersecurity strategy, the creation of a cybersecurity unit in the JSDF, and plans to create a governmental coordination cybersecurity center by 2015 (which will be an expansion of the existing National Information Security Center in the Cabinet Secretariat). Japanese and U.S. share similar economic and security interests in cybersecurity, and while progress in defining collective defense has been slow as Japan works through constitutions issues related to the definition of self-defense in cyberspace, but discussion with the U.S. are underway and Japan has been an important partner in the efforts to build international agreements for cybersecurity.

The situation in Korea differs from that in Japan and Australia because, in addition to Chinese espionage, the ROK faces an erratic and active opponent in cyberspace. North Korea is a source of turbulence and an irritant to both the U.S. and China. So far, most North Korean activity seems to have been directed against the ROK. Since other witnesses will discuss North Korean capabilities, I will note that confirmable intelligence is sparse. There are also disputes about the role for China in the North Korean activities and the extent to which China is witting, supportive, or opposed to the North Korean activities.

North Korea's motives for cyber attack, to the extent they can be discerned are a complex and irrational mix of objective. The North has been developing cyber capabilities for many years and uses them not only for espionage but also for clumsy attempts to sway opinion in the South. Some South Korean analysts believe that the recent cyber attacker could have been a murky diplomatic signal from the North about direct negotiations. They could have been a demonstration for the North's new leader by a cyber attack unit of their capabilities against a media target that had attracted his displeasure. The problem with this is the stability of North Korean decision-making and the ability of North Korea's leaders to accurately calculate the risk that a cyber attack could entail. This is a country that does not mind shelling villages or sinking patrol boats, but a miscalculation in the use of cyber weapons could have much broader and perhaps escalatory effects. The ROK, in response to the North's actions, has increased the amount of resources devoted to cyber security. As with Japan, the U.S. has begun discussion with the ROK on cybersecurity cooperation and collective defense.

North Korea will be an anomaly and an outlier in the efforts to make cyberspace more secure and stable in Asia. Progress, as with the nuclear issues, will be a captive of internal North Korean politics, but it would be helpful to embed the issue of North Korea's use of cyber attacks in a larger international framework, especially a framework that China accepts. This means that U.S. strategy must pursue three interconnected goals simultaneously. The first is sustained, high level dialogue with China. The second is close coordination with allies. The third is multilateral engagement to create international norms of responsible behavior in cyberspace.

In June 2013, the U.S., China, Australia, India, Japan and Indonesia, as part of a fifteen nation Group of Government Experts (GGE) on Information Security established by the UN endorsed the application to cyberspace of the UN Charter, international law, the principle of state responsibility, and national sovereignty. This included agreement that States would not use "proxies" for malicious cyber actions. We know that there are many steps between agreement and implementation when it comes to international practice, but at a recent Track II discussion in Beijing a Chinese official said in a reference to the GGE, "China's position was evolving in the light of international experience." The U.S. has been working with other nations to build on the success of the GGE to create norms and agreement on responsible state behavior in cyberspace. As this effort progresses and there is international consensus on responsible behavior in cyberspace, China's cyber espionage will be difficult to sustain.

The U.S. has been working with other nations to build on the success of the GGE, to create norms and agreement on responsible state behavior in cyberspace. Singapore, Vietnam, Thailand, New Zealand, the Philippines, and Indonesia, all have active cybersecurity efforts at varying levels of maturity. The most important venues for this in Asia are APEC, ASEAN and the ASEAN Regional Forum (ARF). APEC focuses on law enforcement and technical cooperation at the CERT level. The ARF, in its larger effort on terrorism and transnational crime, has begun work with the U.S. on cybersecurity confidence building measures.

The focus of the global effort to develop agreed norms of state behavior in cyberspace will take place this fall in Korea. Seoul will be the venue for a third meeting of a global process started by the UK's Foreign Minister William Hague, to be held in October of this year. Previous meetings have been held in London and Budapest. Korea, as the host, will build on the work done in the ARF and in the GGE. The content of any norms emerging from this meeting will resemble and build upon those agreed at the UN GGE.

The fundamental decision is whether to continue to pursue an effort to obtain universal agreement among all states on norms and responsibilities for states in cyberspace or whether to move to seeking agreement first among like-minded states, as was the case with nonproliferation, while leaving the door open for other nations to join later.

Like-minded nations would almost certainly not include China. In part to forestall any criticism at the first meeting in London, Russia and China introduced their Code of Conduct to shift the terms of debate in their favor and provide an easy riposte to charges that they are not serious about state responsibilities for cybersecurity. The Code reflects their view of how international commitments developed in a bipolar era when they were largely “outside” should be restructured to increase the rights of the state vis-à-vis the rights of citizens. The Code would amend international law in this direction. It reflects a larger dispute over “universal” values. The Chinese position on the Code is more rigid than that of Russia, but it has become largely untenable after failing to win broad support.

Any like-minded effort cannot be a transatlantic initiative. Important “fence sitters” like India and Indonesia – both of which are at early stages in their work on cybersecurity - must be engaged from the start. While some ASEAN nations share to a degree Russia and Chinese concerns about the “U.S.-centric” nature of the internet, it should be possible to build a partnership with them, but building partnerships with the new powers may require flexibility and concessions on issues like internet governance. Several Asian nations, not just China, have expressed a desire to be able to regulate content consistent with the national laws (citing pornography and online gambling as examples of web services available from the U.S. that they would like to block).

This political issue may complicate efforts to reach agreement on cybersecurity norms. It is also too early to measure the effect of Snowdon revelation on US diplomatic efforts to build international agreement on cybersecurity. Making sure that Asia does not become a “cybersecurity battleground” will, however, require regional and perhaps global agreement on the norms, practices and obligations that states observe in their dealing with each other and their dealings with the citizens of other states. This is the essential requirement for making cyberspace stable and more secure.

The common element is the need to address the destabilizing effect of Chinese cyber espionage. Cybersecurity is a fundamental test of China’s willingness to “play by the rules” and whether its integration into the international “system,” will be peaceful. China can choose to amend rules that it believes do not serve its national interests or it can choose to ignore them, but the outcomes from these different choices will be very different for Asia, the U.S. and the world. Cybersecurity in Asia is not a problem that can be resolved by force or coercion, and our engagement with China will be reinforced if there is multilateral agreement on norms. Our goal should be sustained engagement on cybersecurity, globally, in Asia and with China, to build the cooperative agreements that will make cyberspace more secure for all nations. This will not be an easy process nor will it be quick, but it is the best way to advance U.S. interests.

I thank the Committee for the opportunity to testify and look forward to you questions.