

Oral 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 thank the Committee for the opportunity to testify.

Cybersecurity creates instability in Asia. In cybersecurity, as in so many other issues, China’s behavior is the central strategic issue. North Korea’s cyber actions are worrisome, but have been confined to the Korean peninsula. China’s actions have a destabilizing regional and global effect.

The U.S. response should have four elements: (1) engage with China to reduce cyber espionage and the risk of a cyber incident escalating into armed conflict; (2) modify existing alliances with Australia, Japan and Korea to make collective cyber defense a reality; (3) build formal cooperation with ASEAN countries and India on cybersecurity; and (4) make Asia a central part of the global effort to develop norms for responsible state behavior in cyberspace.

The most important thing we can do to increase stability is to reach agreement on norms for responsible behavior – the rules, practices and obligations that states observe in their dealing with each other and with the citizens of other states.

In June, a fifteen nation UN Group of Government Experts on Information Security that included the U.S., China, India, Indonesia, Australia, Japan, and Russia, agreed that the UN Charter, international law, the principle of state responsibility, and national sovereignty apply to cyberspace. This UN agreement is a significant step forward in defining international norms for cybersecurity.

China reluctantly accepted this agreement. Cybersecurity is a

fundamental test of China's willingness to "play by the rules" and will establish if its rise will be peaceful. China can choose to play the game and amend international understandings and agreements that it believes do not serve its national interests, or it can choose to ignore them. This choice will determine future relations with China. The U.S. can influence China's decision, however, with persistence and the right strategy. We have done this before, and while China is more powerful, we can again persuade it to change its behavior to fit global norms.

Military competition between the U.S. and China is increasing, but there is no military solution for cybersecurity. Military conflict is not in our interest. No Asian country, including any of our allies, wants a Cold War with China.

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.

Political issues will complicate efforts to reach agreement on cybersecurity. Many Asian nations want to regulate content, citing pornography and online gambling as examples of web services that they would like to block. It is also too early to measure the effect of Snowden's revelations on U.S. efforts to build international agreement on cybersecurity.

Making sure that Asia does not become a "cybersecurity battleground" will require sustained engagement on cybersecurity with China and cooperative agreements on cybersecurity. Reaching agreement will not be easy nor will it be quick, but it is the best way to advance U.S. interests.

I thank the Committee and look forward to your questions.