USCC.gov
444 North Capitol Street, N.W. - Suite 602, Hall of the States - Washington, DC 20001
Phone: (202) 624 - 1407 - Email: contact@uscc.gov
U.S.-China Economic and Security Review Commission

FOR IMMEDIATE RELEASE **March 08, 2012**

The U.S.-China Economic and Security Review Commission was created by Congress to report on the national security implications of the bilateral trade and economic relationship between the United States and the People's Republic of China. For more information, visit www.uscc.gov.

REPORT: Chinese Capabilities for Computer Network Operations and Cyber Espionage

Today the U.S.-China Economic and Security Review Commission released a report entitled: ***"Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage."*** The report details how China is advancing its capabilities in computer network attack, defense, and exploitation and examines issues related to cybersecurity, China, and potential risks to U.S. national security and economic interests.

"The United States suffers from continual cyber operations sanctioned or tolerated by the Chinese government" said Commission Chairman Dennis Shea. "Our nation's national and economic security are threatened, and as the Chinese government funds research to improve its advanced cyber capabilities these threats will continue to grow. This report is timely as the United States Congress is currently considering cybersecurity legislation, and the Commission hopes that this work will be useful to the Congress as it deliberates on how to best protect our networks."

"The report highlights China's extensive development of cyber tools to advance the leadership's objectives" said Commissioner Michael Wessel. "It's getting harder and harder for China's leaders to claim ignorance and innocence as to the massive electronic reconnaissance and cyber intrusions activities directed by Chinese interests at the U.S. government and our private sector. The report identifies specific doctrinal intent as well as financial support for government-sponsored cyber espionage capabilities. There's clear and present danger that is increasing every day."

This report was prepared for the U.S.-China Economic and Security Review Commission by Northrop Grumman Corp, and is a follow-up to a 2009 report prepared for the Commission by Northrop Grumman on the *"Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation."*

The following is the Commission's synopsis of the report:

Report Conclusions

Among other things, the report concludes that:

- Chinese capabilities in computer network operations have advanced sufficiently to pose genuine risk to U.S. military operations in the event of a conflict;
- Chinese commercial firms, with foreign partners supplying critical technology and often sharing the cost of the R&D, are enabling the PLA to receive access to cutting edge research and technology; and
- The Chinese military's close relationship with large Chinese telecommunications firms creates an avenue for state sponsored or state directed penetrations of supply chains for electronics supporting U.S. military, government, and civilian industry – with the potential to cause the catastrophic failure of systems and networks supporting critical infrastructure for national security or public safety.

The Chinese Military Is Targeting Sensitive U.S. Defense Systems

Chinese capabilities in computer network operations have advanced sufficiently to pose genuine risk to U.S. military operations in the event of a conflict.

People's Liberation Army (PLA) leaders have embraced the idea that successful warfighting is based on the ability to exert control over an adversary's information and information systems. The PLA has placed computer network operations in a unified framework broadly known as information confrontation and seeks to integrate all elements of information warfare, electronic and non-electronic, offensive and defensive, under a single command authority.

PLA analysts consistently identify logistics and C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance) infrastructure as U.S. strategic centers of gravity, which they would almost certainly target in the event of the conflict, likely in advance of actual combat to delay U.S. entry or degrade capabilities.

Currently, no policy exists to easily determine appropriate response options to a large scale attack on U.S. military or civilian networks in which definitive attribution is lacking. Beijing, understanding this, may seek to exploit this gray area in U.S. policymaking and legal frameworks to create delays in U.S. command decision making.

The Chinese Military Is Developing Cyber Capability with Commercial & Academic Partners

The PLA is tapping the talent and resources found in China's commercial IT sector and the academic talent in its military and civilian university system. As part of this effort, the Chinese government funds grant programs to support offensive and defensive cyber research, including research related to information warfare, at civilian and military universities.

The PLA also collaborates with Chinese companies and universities in order to receive access to cutting edge research and technology, including dual-use and military-grade microelectronics and telecommunications. This work is often carried out by Chinese commercial firms, with foreign partners supplying critical technology and often sharing the cost of the R&D.

U.S. Critical Infrastructure and Global Supply Chains Are Vulnerable

The Chinese military's close relationship with large Chinese telecommunications firms creates an avenue for state sponsored or state directed penetrations of supply chains for electronics supporting U.S. military, government, and civilian industry. Globally distributed supply chain networks mean that virtually every sector of private industry has the potential to be impacted; either from upstream manufacturing channels or downstream distribution channels.

Successful penetration of a supply chain such as that for telecommunications industry has the potential to cause the catastrophic failure of systems and networks supporting critical infrastructure for national security or public safety. Potential effects include providing an adversary with capabilities to gain covert access and monitoring of sensitive systems, to degrade a system's mission effectiveness, or to insert false information or instructions that could cause premature failure or complete remote control or destruction of the targeted system.

The technical and logistical challenges associated with hardware supply chain compromises make these types of attacks feasible for only extremely well-resourced organizations, such as state intelligence organizations, which have the expertise and access to technical personnel to penetrate a supply chain with sophisticated technology.

Visit www.uscc.gov for transcripts of previous hearings, research reports, the Commission's annual reports to the Congress, and other information about the Commission's activities.

Follow the Commission on Facebook to get the latest news and announcements from the USCC.