Statement of U.S. Representative Christopher Smith, Cochairman of the Congressional-Executive Commission on China (CECC)

CECC Hearing on "Chinese Hacking: Impact on Human Rights and Commercial Rule of Law"

June 25, 2013, Washington, DC

Excerpts of Remarks by Cochairman Chris Smith (NJ-04)
Congressional-Executive Commission on China
538 Dirksen Senate Office Building
June 25, 2013

In December of 2006 and then again in March of 2007, my Human Rights Subcommittee's computers were attacked by a virus that, in The U.S. House Information Resources Office's words, "intended to take control of the computers." At that time, the IT professionals cleaned the computers and informed my staff that the attacks seemed to come from the People's Republic of China. They said it came through or from a Chinese IP address. The attackers hacked into files related to China. These contained legislative proposals directly related to Beijing, including a major bill I authored, the Global Online Freedom Act. Also hacked were e-mails with human rights groups regarding strategy, information on hearings on China and the names of Chinese dissidents. While this absolutely doesn't prove that Beijing was behind the attack, it raises very serious concern that it was.

Certainly, Chinese agents have not only attempted to target me or my offices. Cyber attacks on Congress are only a small, but not insignificant, part of a much larger pattern of attacks that has targeted the executive branch, the Pentagon, and American businesses.

How do we know this? In recent months, we have seen in-depth reports come out detailing this massive intrusion into our cyber space and massive theft of our cyber data. Chinese agents have stolen our designs for helicopters, ships, fighter jets, and several missile defense systems. They have stolen our innovative technologies, from solar panel designs to biotech research. These thefts appear to have paid off for China. In recent years, the Chinese government has made tremendous jumps in its military capabilities, while boosting the competitiveness of China's "national champions."

While cyber thefts have existed for years, increasingly, we can prove that many of these outrageous thefts—deemed "the greatest transfer of wealth in history"—originate in the People's Republic of China. And these attacks are not random. We now know, with some certainty, that some thefts are being organized by Chinese government agencies.

As we learn about the source of these attacks, we are also learning about the motivations. Talented Chinese Internet users are working day and night to infiltrate our

networks and to steal secrets. China's actions are part of a larger and coordinated state-sanctioned effort to increase China's competitiveness, militarily and commercially.

Today, we will hear more about how the commercial rule of law system in China allows these types of attacks to occur and how these attacks disadvantage American business, innovators, contractors, and government agencies. We will hear about the size and scope of the attacks. And, we will hear how the U.S. government remains unprepared for far too many of these challenges.

We will, also, however, hear about another side of this important topic—one often overlooked during the recent discussions about China's cyber attacks. The Chinese government is not only targeting American business and military organizations, but also targeting ordinary Chinese citizens seeking to advance their most fundamental freedoms. Chinese hackers do not simply look beyond their borders to steal secrets. As we will hear today, Chinese citizens—including those advocating for human rights, free speech and food safety—are also targeted by state-sponsored hackers.

These courageous citizens are also monitored; their private information stolen. The brave pastor seeking to organize a service, the father seeking to raise awareness about toxic foods, the wife of an imprisoned activist, the mother who is made to undergo a forced abortion—all of these citizens realize that, in any instant, the government may be watching. China, of course, also targets those outside of China who similarly wish for human rights and political reform.

Today, we know this system of surveillance and theft occurs. We know that China is organizing these cyber attacks—or is, in the very least, complicit to their existence.

The question we must ask ourselves is why? Clearly, China's rise as a military power requires technology, and China's economy will, no doubt, benefit from the latest innovations from abroad.

But, why is China so concerned about its domestic citizenry—especially those who advocate peacefully for legal and political reforms? Why is China so worried about international NGOs that seek to highlight official abuses and wrongful imprisonments? Why is China so reluctant to provide a fair regulatory environment in China, when commercial laws and regulations will eventually protect all businesses—domestic and foreign—seeking to provide the best services for Chinese consumers?

These may be difficult questions. Thankfully, today we are fortunate to have four guests who are well versed in these issues. They are experts on how China is monitoring our cyber actions and how China is attacking targets globally. I would like to thank them for their participation here today, and I look forward to hearing their insights on these critical issues.