
**November 20, 2014** **Contact:** **Susan Phalen**
**Susan.Phalen@mail.house.gov**

# House Intelligence Committee
# Open Hearing on Advanced Cyber Threats Facing Our Nation
# Chairman Rogers Opening Statement
# November 20, 2014

*(as prepared)*

"The House Intelligence Committee meets today in open session to convene a hearing on the advanced cyber threats facing the nation, as well as the ongoing efforts to protect our nation and our economy from these dangerous threats.

"Our witness for today's hearing is Admiral Mike Rogers, the Commander of U.S. Cyber Command and the Director of the National Security Agency. Admiral Rogers, we appreciate you appearing before the committee today.

"As this Congress comes to a close, I wanted to take this opportunity to talk with the American people one more time about one of the most significant national security threats we face.

"I was a member of the HPSCI for several years before I became Chairman, and I had seen the cyber threats grow in volume and complexity over that time. As I took the gavel as committee Chairman in 2011, I was determined to do what I could to help American companies deal with these threats.

"I started talking publicly in as great a detail as possible about the countries like China and Iran that were preying on American companies. I wanted to raise awareness among companies being targeted, and also advance the debate about what the U.S. government needs to do to address those threats.

"The highlight of that effort for me was the Committee's October 2011 open hearing on cyber where I called out the Chinese government for its industrial-scale campaign of cyber economic espionage against American companies.

"This brazen Chinese government campaign was no secret in the U.S. government or in the private sector cyber security community, but no one was talking about it publicly. The U.S.

government was unwilling to call Beijing to account and U.S. companies feared that the Chinese government would punish them with crushing cyber attacks for speaking out.

“After we opened that debate here and called China out, we were able to have an honest conversation with the American people about the cost of this Chinese campaign and what needs to be done about it.

“China’s economic cyber espionage has certainly not diminished in that time. In fact, it has grown exponentially in terms of volume and damage done to our nation’s economic future. The Chinese intelligence services that conduct these attacks have little to fear because we have no practical deterrents to that theft. This problem is not going away until that changes.

“China’s economic cyber espionage is not the only threat we now face. Iran launched very challenging "distributed denial of service" (DDoS) attacks on our banks’ networks in 2012. While the DDoS tactic isn't new, the scale and speed with which it happened was unprecedented and made the attacks very difficult to defend against.

“A sophisticated virus widely attributed in the press to the Iranian government also wiped out more than 30,000 computers at the Saudi Arabian state oil company Aramco.

“There has been a lot of talk over the years about the hypothetical dangers of a “cyber pearl harbor” and it has become a bit of cliché in cyber security circles. I would argue, however, that threat of a catastrophic and damaging cyber attack on U.S. critical infrastructure like our power or financial networks is actually becoming less hypothetical every day.

“The Iranian attack on Saudi Aramco is a clear example that our adversaries have the intent and capability to launch damaging attacks. Moreover, there are growing reports of attempts to breach the networks and industrial control systems of our electrical power operators and other critical infrastructure operators. Foreign cyber actors are probing America's critical infrastructure networks and in some cases have gained access to control systems.

“Trojan horse malware that has been attributed to Russia has been detected on industrial control software for a wide range of American critical infrastructure systems throughout the country. This malware can be used to shut down vital infrastructure like oil and gas pipelines, power transmission grids, and water distribution and filtration systems.

“I’m not aware of a case yet where a hacker has gained access to one of these systems and used it to cause damage to American critical infrastructure, but I wouldn’t take too much comfort from that.

“I believe our advanced nation state adversaries have the ability to cause such damage. These nations lack a strong motive at this moment to conduct such an attack and are deterred only by the fear of U.S. retaliation.

“Our critical infrastructure networks are extremely vulnerable to such a damaging attack, and we can’t count on deterrence if we’re already in a shooting war with a nation like China or Russia.

"It's not hard to understand how difficult it would be if the power or water was shut off, but imagine if one of our adversaries were able to shutdown key American financial transactions. Our economy would grind to a halt.

"Even worse, imagine if a foreign cyber attacker altered or deleted key financial transaction data so that we couldn't verify bank account balances or what companies owe each other from one day to the next. It would be chaos.

"Most of our critical infrastructure providers are doing their best to better secure their networks, but if they get attacked by an adversary with the resources and capabilities of a nation state like China, it's not a fair fight. The U.S. government has an obligation to help the private sector by sharing threat information about known potential attacks before they happen.

"I'm glad we have this opportunity to talk with the American people about this vital issue. I am hopeful that this hearing can help focus members' attention on this issue and the need to pass cyber threat information sharing legislation before the end of 2014. We must be ready for a damaging cyber attack against our critical infrastructure.

"If the Senate does not act swiftly, both houses of Congress will have to start from scratch next year moving new bills. Given the cyber threats we face, this would be an unnecessary and dangerous delay when we are so close to an agreement that protects privacy and our economy.

"I now turn to the Ranking Member for any remarks he would like to make."

*-30-*