Open Hearing: Advanced Cyber Threats Facing Our Nation

Introduction: The House Permanent Select Committee on Intelligence 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.

- This hearing will focus in particular today on the state of cyber threat information sharing between the U.S. government and private sector, as well as cyber information sharing within the private sector.

- You would be hard pressed to come up with four witnesses better suited to speak on these topics. Our witnesses for today's hearing are:

- Governor John Engler, the former three-term governor of Michigan and currently the President of the Business Roundtable;

- Mr. Ken DeFontes, the President and CEO of Baltimore Gas & Electric;

- Mr. Paul Smocer, the President of BITS, the technology policy division of the Financial Services Roundtable;

- And Mr. Kevin Mandia, the CEO of MANDIANT Corporation, an industry leader in cyber incident response and computer forensics. Mr. Mandia deals with the consequences of advanced cyber espionage against American companies every day, and we look forward to his observations on the threats we face, as well as what we can do to better cope with them.

The Threat

- The United States faces a significant and ongoing cyber security threat today; one that presents grave issues of national and economic security.

- I would like to continue today the conversation we began in our Committee’s open cyber hearing last year, which mostly revolved around China’s pervasive and growing economic cyber espionage campaign against American companies.

- I am sorry to say that China’s economic cyber espionage has not diminished since our last hearing. In fact, it has grown exponentially both in terms of its volume and the damage it is doing to our nation’s economic future.

- The **technological leadership and national security of the United States is at risk** because some of our most innovative ideas and sensitive information are being **brazenly stolen by these cyber attacks**. The Chinese intelligence services that conduct these attacks have little to fear because we have no practical deterrents.

- China’s economic cyber espionage is not the only threat we now face. American financial institutions have been subjected to an intensifying campaign of "distributed denial of service" (DDoS) attacks on their networks over the last year. While DDoS tactic isn't new, the scale and speed with which it happened was unprecedented and made the attacks very difficult to defend against.

- While the U.S. government has not yet publicly attributed these attacks to a particular source, the attacks have been widely attributed in the press to Iran and the Iranian government. When you consider the level of sophistication of these attacks and the level of resources that have been devoted to them, it can only be a nation-state entity.

- Moreover, in our conversations with elements of the private sector that are involved with dealing with these attacks, I have heard nothing to dissuade me from the conclusion that the Iranian government is behind these attacks.

- If you take a step back, and put these Iranian cyber attacks in context, you begin to see a pattern of steady asymmetric, and often lethal, Iranian attacks on the United States.

- Iran's Qods Force, the external operations branch of the Islamic Revolutionary Guard Corps (IRGC), is the Iranian regime's primary mechanism for cultivating and supporting terrorists abroad. The Qods force has provided training to the Taliban in Afghanistan on small unit tactics, small arms, explosives, and indirect fire weapons, such as mortars, artillery, and rockets that has directly resulted in the deaths of American soldiers.

- Since at least 2006, Iran has also arranged arms shipments to Taliban members, including small arms and associated ammunition, rocket propelled grenades, mortar rounds, 107mm rockets, and plastic explosives that that have been used to kill American soldiers.

- The Qods Force supplied Iraqi militants with Iranian-produced advanced rockets, sniper rifles, automatic weapons, and mortars that were used to kill American soldiers, and the Pentagon estimates that the Qods force was responsible for the deaths of at least 170 U.S. troops in Iraq.

- Iran also helped increase the lethality of attacks on U.S. forces by providing militants with the capability to assemble explosives designed to defeat armored vehicles. The Qods Force provided training outside of Iraq as well as advisors inside Iraq for Shia militants in the construction and use of sophisticated improvised explosive device technology and other advanced weaponry.

- Tehran, of course, has a long history of extremely violent acts of terrorism, but the attempted assassination of the Saudi Ambassador in Washington, D.C. in 2011 was shocking even by that standard. The Qods force attempted to set off a bomb that would have killed the Ambassador along with a hundred innocent civilians here in Washington.

- As I look at this pattern of Iran’s asymmetric and often lethal attacks on America, I don’t see any real consequence that Iran has suffered as a result. Of course, Iran is suffering under U.S. and international sanctions for their nuclear program, but where are the consequences for all the American blood they have shed and the cyber attacks on our banks?

- To be clear, Iran’s asymmetric campaign stretches back well before the start of the current President’s administration. In fact, I believe that it has gone on so long that we have become numb to these attacks. We need to wake up and resolve that we have had enough, and that it is time for Iran to suffer significant consequences for these outrageous attacks. Because if there are no consequences, why should they ever stop?

- It’s not hard to imagine what the next wave of Iranian attacks on the U.S. will look like if we do nothing to deter them. A very sophisticated virus called Shamoon infected computers in the Saudi Arabian State Oil Company Aramco last summer. Shamoon has been widely attributed in the press to Iran and the Iranian government.

- Shamoon replaced crucial systems files with an image of a burning U.S. flag and overwrote all the real data on the machine. More than 30,000 of Aramco’s computers that it infected were rendered useless and had to be replaced. There was a similar attack days later on RasGas of Qatar, a major energy company in the region. The Shamoon virus has been described as the most destructive attack that the private sector has seen to date.

- These same tactics can be used by Iran and our other adversaries to degrade or damage American critical infrastructure. At a recent speech in New

York, Defense Secretary Panetta stated that “foreign cyber actors are probing America's critical infrastructure networks. They are targeting the computer control systems that operate chemical, electricity and water plants and those that guide transportation throughout this country. We know of specific instances where intruders have successfully gained access to these control systems. We also know that they are seeking to create advanced tools to attack these systems and cause panic and destruction and even the loss of life.”

Information Sharing

- I would like to have a good discussion today about the advanced cyber threats we face, but just as importantly, we also need to have a good discussion about possible solutions.

- Most elements of the private sector are already working hard to make their networks more secure. They are too often hindered, however, by a lack of information about what attacks other American companies are experiencing and how they are coping with those attacks.

- Too often, companies that would like to share cyber threat information with other parts of the private sector are prevented or deterred from doing so by a range of policy and legal barriers.

- The Intelligence Community also collects valuable information about advanced foreign cyber threats that could dramatically assist the private sector in the defense of their networks. For a variety of legal and policy issues, however, we don’t get the full value of those valuable intelligence insights. Essentially, **the United States is fighting with one hand tied behind its back.**

- Ranking Member Ruppersberger and I reintroduced our cyber threat information sharing bill yesterday to address this problem.

- Our bill provides positive authority to the government to provide classified cyber threat information to the private sector, and knocks down the barriers that impede cyber threat information sharing among private sector companies, and between private sector companies and the government. It does all this with strong restrictions and safeguards to protect the privacy and civil liberties of Americans.

Conclusion

- Whether or not we will ever be able to convince Beijing to voluntarily stop its dirty economic cyber espionage campaign, or deter Tehran from conducting any more cyber terror attacks against our economy, we have a lot of work to do here in the United States to improve our cyber security, particularly improving the sharing of cyber threat information.

- Governor Engler, Mr. Defontes, Mr. Smocer, and Mr. Mandia are excellent resources to help us understand these issues, and I look forward to today’s discussion.

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