



Committee on  
**HOMELAND SECURITY**  
Chairman Michael McCaul

*Opening Statement*

May 21, 2014

**Media Contact:** Charlotte Sellmyer  
(202) 226-8417

---

**Statement of Subcommittee Chairman Peter King (R-NY)  
Subcommittee on Counterterrorism and Intelligence  
Committee on Homeland Security**

**Assessing Persistent and Emerging Cyber Threats to the U.S. Homeland**

**Remarks as Prepared**

Expanding number of cyber actors – ranging from nation-states to terrorists to criminals – as well as increasing attack capability and the increasing intensity of cyber attacks around the globe have made cyber warfare and cyber crime one of the most significant threats facing the United States. This week the Department of Justice unsealed an indictment against five Chinese individuals working for the Chinese military for hacking into multiple private sector US businesses to steal their sensitive, proprietary information.

Additionally, this week the FBI and international law enforcement arrested over 100 people for using malicious software called Blackshades, which is used to remotely take over a computer, turn on the webcam, and access passwords and other information without the owner's knowledge.

I am encouraged by the DOJ indictment and the recent law enforcement operation and hope it is a signal of more aggressive U.S. actions to address the cyber threat moving forward. This threat is not going away. Cyber attacks have economic consequences, harm our national security, and could be used to carry out attacks in the U.S. homeland.

Over the last decade, the threats facing the United States have become more diverse, as have the tools for conducting attacks and waging war. While the US has made great strides to secure the homeland since 9/11, our enemies have evolved, and we must now consider that a foreign adversary, terrorist network, or a criminal organization will use cyberspace to penetrate America's defenses.

Director of National Intelligence James Clapper featured the cyber threat prominently in his annual threat update to Congress this year. Along with other US officials he painted a sobering picture of the potential fallout from a cyber attack.

Nation states comprise the most capable cyber actors around the globe. Countries such as Russia, Iran, and China have demonstrated a willingness to use cyber space to steal our military secrets, target our critical infrastructure, and even attack our free press and financial sector. Each has invested a great deal in cyber defenses and offensive capabilities, and some have even used cyber-attacks as a proxy to in a physical military confrontation. Many experts have suggested that Russian actors have engaged in offensive attacks in Estonia, to support military forces during their 2008 invasion of Georgia, and again during their recent annexation of Crimea.

In addition to the threat from foreign powers, American citizens and companies lose billions from organized cybercrime every year. Traditional criminal networks have wasted no time in developing their online tradecraft to scam, steal, and destroy valuable data. The recent data breach at Target is a great example of exactly how far-reaching and sophisticated these operations are. The Department of Homeland Security plays a major role in helping private companies keep their networks secure and this will only become more important in years to come.

Finally, though we are accustomed to think of the physical damage caused by terrorist networks to life and property, we must now be prepared to defend against groups like al Qaeda using increasingly sophisticated cyber attacks and cybercrime to their advantage. For many years we have also seen these groups and violent Islamist extremists use the Internet to communicate, radicalize, and spread their hate.

Today, we will hear about these issues from witnesses provided by the FBI and DHS. I am pleased that we will begin this hearing in an open session and subsequently move into a closed, executive session. I am pleased that the Chairman of the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, Mr. Meehan, has joined me in working to further educate the Committee on this issue. Mr. Meehan – along with Chairman McCaul – has led this Committee’s effort to enact serious cybersecurity legislation. With the support of the private sector and privacy advocates, their bill was passed unanimously out of this Committee. That is a testament to their hard work, but also to the importance of these issues.

I welcome those on the ‘front lines’ of this issue and look forward to their testimony.

###