Committee on
HOMELAND SECURITY
Chairman Peter T. King

Opening Statement

April 24, 2012

Media Contact: Shane Wolfe

(202) 226-8417

Statement of Chairman Michael T. McCaul (R-TX)
Subcommittee on Oversight, Investigations, and Management

"America is Under Cyber Attack: Why Urgent Action is Needed"

April 24, 2012
Remarks as Prepared

America's computers and Internet infrastructure are under attack and every American is at risk. The US government, critical infrastructures, American business institutions and our personal data are being compromised by nation states and hacker groups. The intent is to conduct cyber warfare, possibly paralyzing our infrastructure, stealing our intellectual property, conducting espionage, and gaining access to our credit card, bank account and social security numbers.

Richard Clarke, former special adviser on cybersecurity to President George W. Bush, said within the first 48 hours of a cyber attack on the United States we could experience:

- The Department of Defense's classified and unclassified networks collapsing as a result of large scale routers failing to function.
- Reports of large oil refinery fires, as well as lethal clouds of chlorine gas emitting from chemical plants.
- Our financial system dissolving as a result of important financial data being lost with no idea of who owns what.
- Pipelines carrying natural gas exploding.

- Trains and subway derailing.
- A nationwide blackout leaving American cities in the dark.

Unfortunately, this is not a science fiction scenario.There are no shells exploding or foreign militaries on our shores. But make no mistake: America is under attack by digital bombs. There are several things the American public should understand about these attacks:

- They are real, stealthy and persistent and could devastate our nation.
- They occur at the speed of light.
- They are global and could come from anywhere on earth.
- They penetrate traditional defenses.

Who is conducting these attacks and why?

An October 2011 Report to Congress on Foreign Economic Collection and Industrial Espionage states, it is part of China and Russia's national policy to try to identify and take sensitive technology, which they need for their development. China and Russia view themselves as strategic competitors of the United States and are the most aggressive collectors of US economic information and technology.

China's cyber warfare capabilities and the espionage campaigns they have undertaken are the most prevalent of any nation state actor. China has created citizen hacker groups, engaged in cyber espionage, established cyber war military units and laced the US infrastructure with logic bombs.

Russia has advanced capabilities and the intent and technological prowess necessary to carry out a cyber attack anywhere in the world, at any time. Russia has been accused of unleashing a cyber war against Estonia in 2007 and shutting down government websites. Russia has also taken down Georgia's banking and government sites as part of a policy to demonstrate its power during a conflict.

There are of course many other countries developing cyber capabilities and using cyber espionage to steal US trade and technology secrets to bolster their own economic development; and all of them pose a threat.

Besides nation states, there are groups such as Anonymous, LulzSec and AntiSec who indulge in non-state "hacktivism" or hacking and activism. They are largely a sympathizer of "freedom of information," and their agenda is basically to protest what they perceive as violation of freedom of information or violation of privacy.

These attacks are sometimes aimed at individuals but many times used against businesses. Based on the recent arrests here and in the United Kingdom, it appears that the group consists predominantly of juveniles who want notoriety. Non-state hacktivist groups have indulged in denial of service attacks against the likes of Sony, Mastercard and Stratfor, located in my hometown of Austin, Texas, defacing websites, slowing down online accesses on the Internet and stealing sensitive information such as password files, credit card and social security numbers.

These groups, both nation states and non-state hacktivists, present a threat not only to the security of our nation, but also to our personal and business files. We require a robust national effort to counter these attacks against our national interests.

The potential of cyber attacks is frightening. The Stuxnet worm is groundbreaking malware launched against the Iranian nuclear program. It is so devious in its use of computer vulnerabilities with such a multipronged approach that the Iranians had no idea they were attacked. Such a successful attack against the United States with viruses designed to manipulate, bring down industrial control systems could cause devastating human and economic losses.

General Alexander, Director of the National Security Agency, told me that it is not a matter of if, but when a cyber Pearl Harbor will occur. We have been fortunate that up until this point cyber attacks in our country have not caused a cataclysmic event that has brought physical harm to Americans. But that is not for lack of effort on the part of those who mean to destroy our way of life.

Last week, former Secretary of Homeland Security Michael Chertoff said "It doesn't take a lot to understand how an attack on critical infrastructure during a time of tension could seriously undermine the ability of a country to defend itself." The Secretary recalled, “I had the experience of living through an event that occurred after there was a fair amount of warning and four planes were hijacked and we lost about 3,000 people. My message to anybody who's interested in this, particularly in Congress, is let's do something meaningful because it is not a tolerable situation.”

I share the Secretary’s concerns. It is time to do something meaningful.

# # #