HOMELAND SECURITY
COMMITTEE

Statement of Chairman Michael McCaul (R-TX)
Homeland Security Committee

A Borderless Battle: Defending Against Cyber Threats
March 22, 2017

Remarks as Prepared

Today, I look forward to discussing the borderless battle being waged against us by nation states, hacktivists, and faceless criminals in cyberspace.

Last month I spoke at the RSA Conference in San Francisco. And my message today is the same as it was then: we are in the fight of our virtual lives, and we…are…NOT…winning.

Our adversaries are turning digital breakthroughs into digital bombs.

From Russian and Chinese hackings to brand-name breaches, our cyber rivals are overtaking our defenses. Nation-states are using cyber tools to steal our country's secrets and intellectual property.

Hackers snatch our financial data and lock down access to our healthcare records and other sensitive information. And terrorists are abusing encryption and social media to crowd-source the murder of innocent people.

As our exposure to cyber threats grows, we understand the importance of not only being aware of each individual attack and piece of malware but also the patterns of the sophisticated campaigns and the life-cycle of each threat.

It is clear that cyber-attacks are becoming incredibly personal, and the phones in our pockets are now the battlespace.

Our most private information is at stake. Just last week, the Department of Justice indicted two Russian spies for their involvement in the hack of at least 500 million email accounts at Yahoo.

In 2015, Chinese hackers stole 20 million security clearances—including my own—in a breach of the U.S. government's Office of Personnel Management.

And recently, an alleged hack of the CIA has Wikileaks publishing over 8000 pages of documents with some of the most highly sensitive cyber weapons.

Cyber criminals are targeting our wallets too. One of our witnesses today, General Keith Alexander, said online theft has resulted in the "greatest transfer of wealth in history."

Last year, we also realized our democracy itself was at risk, as the Russian government sought to undermine democratic institutions and influence our elections.

They broke into political institutions, invaded the privacy of private citizens, spread false propaganda, and created discord in the lead up to a historic vote.

The conclusion from all of this chaos is clear: our digital defenses need to be strengthened—and our attackers must feel the consequences of their actions. Unfortunately, the U.S. government is fighting 21st century threats with a 20th century mindset and a 19th century bureaucracy.

Bigger federal agencies are not necessarily the answer. We need to better tap into private sector innovation—and more quickly. But government does play a critical coordinating role.

When it comes to domestic cybersecurity, it is important that our efforts are led by a civilian department. Not by the military. And not by intelligence agencies.

Just as we do not allow soldiers to police our city streets, we should not have organizations like the military or intelligence agencies patrolling domestic networks. That is why in both 2014 and 2015 Congress passed legislation I championed that better defined interagency cyber responsibilities.

Those bills put DHS in the lead for operationally securing the so-called "dot gov" domain, helping to better protect critical infrastructure, being the hub for cyber threat information sharing, and providing voluntary assistance to the private sector.

At the end of last year, the Department announced it was providing cybersecurity services to 93 percent of the executive branch's civilian workforce.

But perimeter detection is only one tool in our tool box. We need defense-in-depth strategies and a talented cyber workforce on the frontlines.

Unfortunately, we are not attracting top cyber talent because morale is poor on the inside and the money is better on the outside.

I have proposed the creation of a stronger, consolidated cybersecurity agency at the Department of Homeland Security. This will help us step-up our cyber defense efforts and attract top talent.

And we have already begun to work with the Trump Administration and others to make that a reality in the near future.

Finally, winning battles in cyberspace depends on our ability to deliver consequences. As a former federal prosecutor, I know that if you don't make the costs outweigh the benefits bad behavior will continue.

This requires strong leadership, a willingness to track down rogue hackers, and a determination to hold hostile countries accountable.

###