Opening Statement on Cybersecurity Policy and Threats
Chairman John McCain
Tuesday, September 29, 2015

The Committee meets today to receive testimony from Deputy Secretary of Defense, Robert Work; Director of National Intelligence James Clapper; and Admiral Mike Rogers, the Commander of U.S. Cyber Command, Director of the National Security Agency, and Chief of the Central Security Service. We thank each of the witnesses for their service and for appearing before the committee.

We meet at a critical time for the defense of our nation from cyberattacks. In just the past year, the United States has been attacked in cyberspace by Iran, North Korea, China, and Russia. Indeed, since our last cyber hearing in March, these attacks have only increased, crippling or severely disrupting networks across the government and private sector and compromising sensitive national security information. Recent attacks against the Joint Chiefs of Staff, the Pentagon, and the Office of Personnel Management are just the latest examples of the growing boldness of our adversaries and their desire to push the limits of acceptable behavior in cyberspace. New intrusions, breaches, and hacks are occurring daily.

The trends are getting worse, yet the Administration still has not mounted an adequate response. They say they will, quote, "respond at the time and manner of our choosing," but then either take no action, or pursue largely symbolic responses that have zero impact on our adversaries' behavior.

Not surprisingly, the attacks continue. Our adversaries steal, delete, and manipulate our data at will, gaining a competitive economic edge and improving their military capability. They demonstrate their own means to attack our critical infrastructure. And they do all of this at a time and manner of <u>their</u> choosing. More and more, they are even leaving behind what Admiral Rogers recently referred to as "cyber fingerprints," showing that they feel confident that they can attack us with impunity and without significant consequences.

Just consider the recent case with China. After much hang-wringing, it appears the President will not impose sanctions in response to China's efforts to steal intellectual property, pillage the designs of our critical weapons systems, and wage economic espionage against U.S. companies. Instead, last week's state visit for the President of China simply amounted to more vague commitments not to conduct or knowingly support cyber-enabled theft of intellectual property.

What's worse, the White House has chosen to reward China with diplomatic discussions about establishing norms of behavior that are favorable to both China and Russia. Any internationally agreed upon rules of the road in cyberspace must explicitly recognize the right of self-defense, as contained in Article 51 of the UN Charter, along with meaningful human rights and intellectual property rights protections. The Administration should not concede this point to autocratic regimes that seek to distort core principles of the international order to our detriment.

Make no mistake, we are not winning the fight in cyberspace. Our adversaries view our response to malicious cyber activity as timid and ineffectual. Put simply, the problem is a lack of deterrence, as Admiral Rogers has previously testified. The Administration has not demonstrated to our adversaries that the consequences of continued cyberattacks against us outweigh the benefit. Until this happens, the attacks will continue, and our national security interests will suffer.

Establishing cyber deterrence requires a strategy to defend, deter, and aggressively respond to the challenges to our national security in cyberspace. That is exactly what the Congress required in the Fiscal Year 2014 National Defense Authorization Act. That strategy is now over a year late and counting. And while the DOD's 2015 Cyber Strategy is a big improvement over previous such efforts, it still does not integrate the ends, ways, and means to deter attacks in cyberspace.

Establishing cyber deterrence also requires robust capabilities, both offensive and defensive, that can pose a credible threat to our adversaries—a goal on which the Congress, and specifically this Committee, remains actively engaged. The good news here is that significant progress has been made over the past few years in developing our cyber force. That force will include a mix of professionals trained to defend the nation against cyberattacks, to support the geographic combatant commands in meeting their objectives, and to defend DOD networks.

This is good, but the vast majority of our DOD resources have gone towards shoring up our cyber defenses. Far more needs to be done to develop the necessary capabilities to deter attacks, fight, and win in cyberspace. Policy indecision should not become an impediment to capability development. We do not develop weapons because we want to use them; we develop them so we do not have to. And yet, in the cyber domain, as Admiral Rogers testified in March, quote, "we're at a tipping point." He said, quote, "we have got to broaden our capabilities to provide policy makers and operational commanders with a broader range of options."

We must invest more in the offensive capabilities that our cyber mission teams need to win on the cyber battlefield. The Fiscal Year 2016 NDAA seeks to address this challenge in a number of ways, including a pilot program to provide the Commander of Cyber Command with limited rapid acquisition authorities.

Finally, we know the Defense Department is in the process of assessing whether the existing combatant command structure adequately addresses the mission of cyberwarfare, and whether to elevate Cyber Command to a unified command. There are worthwhile arguments on both sides of this debate. I look forward to hearing Admiral Rogers's views on this question, and his assessment of how an elevation of Cyber Command might enhance our overall cyber defense posture. I also look forward to hearing from our witnesses what, if any, progress has been made on addressing disagreements within the interagency on the delegation and exercise of authority to use cyber capabilities.

I thank the witnesses again for appearing before the Committee and I look forward to their testimony.