Opening Statement of U.S. Senator Jack Reed
Ranking Member, Senate Armed Services Committee

Room SD-G50
Dirksen Senate Office Building
Tuesday, September 29, 2015

To receive testimony on U.S. cybersecurity policy and threats:
(As prepared for delivery)

Thank you, Mr. Chairman. I commend you for scheduling this hearing. This is an appropriate time to discuss a number of important cyber issues with our witnesses, especially in light of the cyber agreements announced last Friday between President Obama and the President of China. I want to thank Director Clapper, Deputy Secretary Work, and Cyber Command Commander Admiral Rogers for their testimony today.

Let me start with the series of cyber agreements with China. The apparent commitment by China to cease stealing U.S. intellectual property for economic gain is notable, and I expect we will have a robust discussion about China's compliance and our course of action if it does not. China's leaders must be aware that its reputation and standing in the eyes of the American people will continue to decline if this piracy does not stop, which ultimately will have a tremendously negative impact on our relations. I would also emphasize the potential importance of China embracing a set of international norms in cyberspace developed by the United Nations, which includes a commitment to refrain from attacks on other nations' critical infrastructure.

Next I would highlight that we are facing the recurring issues of whether or when to elevate Cyber Command from a sub-unified command to a full unified command, and whether to sustain the current "dual-hat" arrangement under which the Commander of Cyber Command also serves as the Director of NSA. I understand that the Department may be nearing a recommendation to the President that the next Unified Command Plan elevate Cyber Command to a unified command.

The Committee in the past has questioned whether Cyber Command is mature enough to warrant elevation to a unified command, and whether the dual-hat arrangement should continue when a decision is made to elevate the Command. Put simply, if Cyber Command is so reliant on NSA that common leadership is still necessary, is the Command ready to stand on its own as a unified combatant command?

Historically, combatant commanders have been drawn from the ranks of officers from what the Army and Air Force call the "combat arms" and the Navy calls "officers of the line," and not from supporting arms, such as intelligence. The Committee has expressed concern about the prospect of an intelligence specialist serving as a combatant commander, as well as, in the alternative, a broadly experienced combat arms officer serving as the Director of a technically complex intelligence agency such as NSA. I look forward to the perspectives of our witnesses on this matter.

Directly related to the question of the maturity of Cyber Command is the status of the military cyber mission units that the Department only began fielding over the last two years. Commendably, the Department is meeting its schedule for standing up these units with trained personnel, but by its own admission the equipment, tools, and capabilities of these forces remain limited. Indeed, the Committee's FY16 National Defense Authorization Act includes a mandate that the Secretary of Defense designate executive agents from among the services to build the so-called "Unified Platform," "Persistent Training Environment," and command and control systems that are necessary for these forces to operate effectively. It will take a number of years to build these capabilities.

We are behind in developing these military capabilities for our cyber forces because the Defense Department was persuaded that the systems and capabilities that NSA already has would be adequate and appropriate for use by Cyber Command. This is an important example

of an assumed critical dependency on NSA, and an assumed commonality between intelligence operations and military operations in cyberspace, that has turned out to be wrong.

For a number of years, this Committee has been urging the executive branch to work diligently to identify all practical methods to deter malicious actions in cyberspace, and to articulate a strategy for implementing them. Some believe that retaliation in kind in cyberspace is a necessary and effective component of such a strategy. I look forward to hearing the views of our witnesses on this matter. While I share the concern and frustration over the many large-scale acts of espionage, theft of intellectual property, and even destruction that we have suffered, I would simply note that: one - few nations, including our own, forsake opportunities to spy on potential adversaries; and two - committing crimes ourselves, and damaging property, in cyberspace does not strike me as a winning strategy for a nation as singularly exposed to cyber-attack as ours.

As my colleagues and our witnesses are well aware, the Senate went into recess for the August break having reached an agreement for bringing the cyber information sharing bill to the floor for debate. I know the Chairman is in full agreement on the need to debate, amend, and pass that legislation this year in the interest of national security.

I would be remiss, Mr. Chairman, if I failed to note the impact that sequestration will have on the cybersecurity and counter-terrorism capabilities of the civilian partner agencies of NSA, Cyber Command, and the Defense Department, and will ask Admiral Rogers in particular to comment on that.

Finally, I think it is important that we hear from our witnesses on the subject of encryption. Post Snowden, U.S. technology companies, fearful of losing business at home and abroad, are encrypting communications, and offering encryption services, for which even the companies themselves have no technical capability to unlock. FBI Director Comey has given multiple speeches warning that law enforcement agencies and intelligence agencies will be "going dark," with serious consequences for public safety and national security.