Ranking Member Adam Smith

Opening Statement

3/1/2017

Cyber Warfare in the 21st Century

I thank the witnesses for appearing before us today. Each of our witnesses possesses a wealth of experience and knowledge of the cyber domain, in addition to broader expertise that should be applied to this topic.

Lawmakers and other leaders in government tend to take narrow approaches to assessing the cyber domain, which may have the effect of limiting our ability to effectively employ cyber capabilities and to counter adversaries. Cyber threats can be sweeping in scope. For example, the Russian Federation’s reported cyber activities during the recent U.S. election did not comprise an isolated cyber-attack; they were part of a broader Russian influence campaign designed to undermine democracy and to legitimize the autocratic Russian regime. They were also carried out in a way that blurred the lines between soldier and spy.

ISIL’s use of the cyber domain to recruit, command and control forces, and disseminate its twisted narrative is only one part of its broader strategy to establish a caliphate. Much of the dialogue surrounding ISIL’s campaign is focused on the United States ramping up our own cyber efforts in response. Although we would all agree that offensive and defensive military operations in cyberspace are critical lines of effort to countering adversaries, they are not the only means that we should employ. For this reason, our deterrence strategies and responses to malicious cyber activities must take into account the broader set of activities that we are trying to deter and then leverage all instruments of power to counter our adversaries.

We must also accept that while some of our adversaries will operate in the cyber domain the same way that they do in the conventional domain - without regard to international law and without laws and policies restraining their activities - we are a country that will continue to adhere to international law. We will remain a country that carefully considers the impact that military operations in the cyber domain may have when crafting governing authorities and policies. Like a Navy ship, cyber tools can be used for deterrence, but they can also be used as deadly weapons. The esoteric and ambiguous nature of the cyber domain will continue to offer challenges, but it will not compromise our values.

That said, there is ample opportunity to strengthen the United States’ position in the cyber domain. Refinement of the Department of Defense’s roles and authorities in the cyber domain for deterrence, response, offensive action and homeland defense will further enable effective employment of the force. Agility and speed must be key ingredients to cyber strategy, authorities, and policies, and the use of cyber tools and methods. These ingredients are especially critical when it comes to high-level decision making for necessary military operations, development and acquisition of cyber capabilities, and management of the cyber force structure.

Additional funding alone will not solve the challenges we face in the cyber domain. Investment must be coupled with the development of carefully considered, comprehensive strategies, authorities, and policies to bring us “left of click.”