Center for a New American Security

September 30, 2015

Testimony before the House Foreign Affairs Committee
Cyber War: Definitions, Deterrence, and Foreign Policy

Robert J. Butler, Adjunct Senior Fellow
Center for a New American Security

Mr. Chairman, Ranking Member Engel, and distinguished members of the Committee, thank you for inviting me to speak on the topic of cyber war. I would like to begin by noting that the opinions expressed here today are solely mine and do not reflect the views of any particular organization within or outside the U.S. Government (USG.)

For the last 36 years, my work life has been about Information Technology (IT) and its application across multiple sectors. After graduating with a degree in computer information systems and a focus on quantitative business methods, I began a career in the United States Air Force first as a software developer and then, for the next 26 years, developed or applied information technology as both a computer systems and intelligence officer. Along the way, I was afforded the opportunity to help guide the evolution of information warfare, information and cyberspace strategy and operations within the Department of Defense (DOD) and the USG as a planner and commander. My work in DOD included the stand-up of information operations (IO) organizations, development of IO campaign plans, and serving as the DOD lead in the first USG negotiation with the Russians on cyber arms control in 1998. I was also privileged to serve as the Director of Intelligence at US Transportation Command during Operations Enduring and Iraqi Freedom, just as the Chinese government began aggressive on-line reconnaissance of our critical force projection networks. I culminated my military career by commanding the intelligence operations organization that is now commonly referred to as NSA-Texas.

After retirement from the Air Force, I served as the senior civilian executive for DOD's premiere joint information operations command before joining a US-based global IT services firm as its Director of its Military Intelligence Programs. Returning to government service in 2009, I served as the first Deputy Assistant Secretary of Defense (DASD) for Space and Cyber Policy. My key direction from Defense Secretary Bob Gates and Deputy Secretary Bill Lynn was to get US Cyber Command stood up and write the first DOD cyber strategy. I also had opportunity to provide input and shaping to the first ***International Strategy for Cyberspace***. During my time as a DASD, I witnessed and was appalled at the expansion of the cyber threat from China and Russia, especially the rampant on-line theft of US intellectual property by the Chinese and the continued disruptive Russian cyber attacks which was an ominous signal of what was to come from Russia in the Ukraine. I was also dismayed by our struggles to deal effectively with the Wikileaks intrusion and with STUXNET, the world became aware that another threshold had been crossed into the area of cyber-induced physical destruction.

Since leaving government service, I have spent most of my time in the private sector, helping a leading edge data center company, partnered with a very large New York-based financial services firm, "go global" – to Singapore, London and beyond. As the corporate Chief Security Officer, I had the opportunity to build and implement a "bottoms up" security program, countering foreign threats while courting other foreign customers as partners.

From a public sector perspective, I have served as a non-paid senior government expert to the Air Force, Office of the Secretary of Defense and the Department of Homeland Security (DHS) since leaving full-time government service in 2011. Additionally, I serve as a non-resident fellow at the Center for a New American Security. In sum, I believe my technical training, 30 years of DoD experience – in and outside of uniform and my six years in US-based Multinational Corporations, have given me knowledge and insights to address your questions regarding cyber war, deterrence, the role of diplomacy including business diplomacy, foreign policy implications and US actions to date to reduce cyber conflict.

Before addressing these topics, I wanted to give you my perspective on what is meant by cyberspace operations.

- In DOD, we categorize cyberspace operations as computer network operations (CNO), computer network defense (CND), offensive computer operations (OCO) and computer network exploitation (CNE.) Though we (and other militaries) use these categories as an organizing principle, effective cyberspace operations requires the synchronization of all four categories of activities to meet DOD/USG objectives.

- CNO are the actions we take to enable the flow of data from one location to another location; it includes configuring, operating, monitoring and measuring all hardware – from servers to phones, software – operating systems and applications, and networks – whether they are wired or wireless.

- CND are the actions we take to defend the network and more importantly, the information assets and sensitive data we have on the network. CND includes the deployment of technology like firewalls and intrusion detection systems, but also includes organizing concepts like dividing or segmenting networks. Focus for cyber defenders is on ensuring the continuous confidentiality, integrity and availability of the information flowing within an enterprise.

- OCO involves the use of software, hardware and networks to deliver software (malware) for an intended effect against an adversary – usually to disrupt, degrade or destroy an adversary's capability. Targeting is a very difficult process as data may need to flow across multiple "hops" in a network before arriving at the intended target. Along the way, adversaries have opportunity to watch, intercept and/or re-direct. USG has a very detailed system of "checks and balances" prior to approval of an OCO activity.

- CNE is the use of hardware, software and networks to better understand the adversary through collection and analysis of data. CNE is an intelligence activity, integral and necessary to support both CND and OCO activity.

With this context, let me now provide my thoughts on the topics about which you've asked.

Cyber War.

History, other countries' doctrines and technology trends help us to best envision what a future cyber war would like. First off, I believe the term is not especially helpful. We will likely not be involved in a cyber war, but a war that uses cyberspace tools and capabilities to achieve desired effects. That was certainly the case in Estonia, Georgia and Ukraine as Russia prosecuted its campaign to dissuade local ethnic leaders and reverse outcomes considered detrimental to Moscow. As we saw in these Russian incursions, cyberspace operations – both offensive and defensive – were part of a combined arms campaign.

Importantly, I think we need to better understand how cyberspace capabilities could be used in a run-up to war and what we should do to dissuade a potential adversary nation-state. Carrying out an OCO activity requires exquisite intelligence, derived from CNE and other intelligence activities. Capable nation-states would use all of its intelligence, counter-intelligence and other surveillance resources – both on-line and "off net" – to assure highly successful OCO activity. I commend the Defense Science Board (DSB) 2013 report on resiliency for further detail on this subject.

In the run-up to war, an adversary would likely use CNE to surveil our and our allied on-line capabilities, and acquire the needed intelligence for developing battlespace plans – what we call in DOD parlance the Intelligence Preparation of the Battlespace (IPB). Likely targets for CNE would be our command and control (C2) capabilities – especially in our nuclear, missile defense and force projection mission areas, our other military force structures and our nation's commercial critical infrastructure. Implanting of malware in any of these structures by another foreign nation should be a significant cause for concern and warrant NCA action. In deterring and responding to these threats against the US military and the US more broadly, the United States needs a range of credible options. Offensive cyber is necessary, but not sufficient.

International Law and Norms.

From a policy perspective, the Law of Armed Conflict and other International Law apply to the use of force and armed attack. These provisions include the application of proportionality in response. Beyond these laws, NATO provisions obligate us to render assistance to NATO members that have been attacked in cyberspace – as evidence through sustained disruption, degradation and/or destruction of that member nation's C2, other military and/or critical infrastructure. The Tallinn Manual is a good source for further definition of these treaty obligations.

Though not directly applicable to situations of armed attack, the Budapest Convention could also be invoked to render assistance for on-line criminal activity being prosecuted by a nation or criminal group.

Role of Deterrence.

Deterring bad actors' behavior using our cyberspace capabilities is an important and integral aspect of our defense strategy. More importantly, the use of all means – informational, economic, diplomatic, military -- for deterring malicious acts in cyberspace is a critical component of our ***International Strategy for Cyberspace***, published by the White House in May of 2011. The recently updated ***DoD Cyber Strategy*** clearly describes the components of an effective cyber deterrence strategy. First,

deterrence must include not only a declaration of response, but a display of effective response capabilities such as the projection of force or sanctions from an economic perspective. Secondly, an effective deterrence strategy must include the development and deployment of effective defense capabilities to deny a potential attack from succeeding. The DOD build-out of the Cyber Mission Force, under Cyber Command leadership, is a foundational element of deterrence by denial. Finally, effective deterrence must incorporate provisions to strengthen the resilience of US systems – C2, other military and commercial critical infrastructure – to withstand attack. Also note that attribution is a fundamental part of an effective cyber deterrence strategy and is enabled through strengthening our intelligence capabilities, and our partnerships with both industry and allies.

Diplomacy in Containing Cyber Conflict.

Proactive diplomacy in cyber conflict is essential to containing cyber conflict. As described in the USG's ***International Strategy for Cyberspace***, the USG Executive Branch, under State Department leadership, has been working with other states to build and sustain an open, interoperable, secure and reliable cyberspace environment around the globe, and really creating a new area of foreign policy in the field of cyber diplomacy. The State Department works to meet this diplomatic objective through three activities: bilateral and multilateral partnerships; international and multi-stakeholder organizations; and private sector collaboration. Bilaterally, the US continues to grow capacity building partnerships with the United Kingdom, Australia, Canada, New Zealand, the North Atlantic Treaty Organization, the Gulf Cooperation Council states and allies in the Asia-Pacific region. The USG has been involved for more than a decade in multilateral dialogue with the United Nations' Government Group of Experts to define norms in cyberspace. This year is a notable as there has been consensus among member nations – to include Russia and China – on a small set of norms to include the protection of national critical infrastructure. With the majority of USG critical infrastructure in the hands of US/allied private sector partners, USG collaboration, primarily through DHS, DOD, the Department of Commerce, Department of Treasury, Department of Justice, with US industry – especially US-based MNCs -- is a foundational element of US business diplomacy and deterrence.

Foreign Policy Implications.

The Internet is a global platform shared by all states and non-state actors for commercial, humanitarian, defense and other security purposes. As such, the ability to operate in open, interoperable, secure and reliable cyberspace environment is a critical national interest. To achieve that goal, the US must build and sustain an environment in which norms of responsible behavior guide states' actions, sustain partnerships and support the rule of law in cyberspace.

Assessment of US Administration Actions to Date.

The Administration has taken some effective steps in countering and anticipating the threat of conflict in cyberspace facing this nation, but much more needs to be done. The ***International Strategy for Cyberspace*** and other Departmental Strategies have been good blueprints for what needs to be done and provide the right messaging to the rest of the world for what we should do to effectively operate in cyberspace and reduce cyber conflict. **However, the scale and speed of strategy implementation are lacking and lagging, creating a significant "deterrence deficit" and unacceptable risk exposure for the nation.**

- In order to have credible and effective deterrence of cyber attacks on critical infrastructure by well-resourced adversaries, the U.S. needs to ensure the resilience not only of our nuclear strike capabilities, but of a broader range of non-nuclear capabilities such as conventional strike, missile defense and offensive cyber. In short, we need to do more.

- As noted by the OPM breach, our deterrence by denial across USG systems is not credible. We need to do more.

- As noted in the 2013 DSB report on resiliency and other studies of our grid infrastructure, our resilience, especially in our commercial critical infrastructure, is not at a level to withstand a high-end attack from a determined and resourced adversary. The DSB and other Executive Branch-sponsored reports point to a worsening threat environment which portends for even more trouble. We need to do much more.

So, what should be done?

- The President himself needs to work with you – the Congress – to drive cybersecurity as a national priority --- on level with health care, immigration and the nuclear treaty with Iran.

- We need to back priority with resources and authority to Departmental stakeholders, and hold Departments accountable for rapid action.

- DHS needs resources and authority to autonomically apply "best practice" cyber hygiene across USG agencies.

- DOD needs additional resources to more rapidly build out cyber mission forces and associated infrastructure.

- The White House needs to lead USG efforts to update all cyber-related laws (which are being exploited by adversaries) and to create new statues that enable us to rapidly close risk exposure.

- Related to the previous point, we need to update Critical Infrastructure Partnership Advisory Council (CIPAC) authorities to incentivize the private sector to do more. Where these incentives do not suffice, dictate rules of security and safety to protect commercial critical infrastructure and make it more resilient. Exercise business and government continuity together.

Proposed Role for the House Foreign Affairs Committee.

The Committee should have a critical role in this subject area by first requiring a comprehensive review of the ***USG International Strategy for Cyberspace*** – what has been the result of actions taken thus far, what's not been done, and why. This will require the Administration to provide measures of effectiveness for the strategy. The Committee should ensure implementation measures address the worsening threat environment since the strategy was published in 2011.

Secondly, the Committee should ensure the Administration leads the rapid build-out of international public-private sector partnerships as an integral component of an effective deterrence strategy. In doing

so, the State Department should be required to provide regular updates to the Committee on implementation status and to highlight to this committee any impediments to full implementation by the end of 2016. Further to this end, the Committee should work with the State Department to acquire authorities and/or resources to overcome impediments to strategy implementation.

Complementing and helping to enable the Administration's efforts on the international stage, the Committee should solicit regular updates from US-based Multinational Corporations on what else should be done to further US national interest in working with foreign nations to create an open, interoperable, secure and reliable cyberspace environment. This should include obtaining industry perspective on the effectiveness of current and proposed amendments to international trade and arms control agreements, such as the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies.

Finally, the Committee should set up a "table top" exercise that would help members to better understand different conflict scenarios which would involve cyberspace capabilities and highlight the role the Committee has in establishing mechanisms for prevention and response.

Thank you again for the opportunity to share these thoughts. I stand ready to help the Committee as we seek to better protect and grow our nation.