Testimony to the House Armed Services Committee

Ian Wallace

Senior Fellow, International Security Program & Co-Director of the Cybersecurity Initiative,

New America

September 29, 2015

Chairman Thornberry, Ranking Member Smith, distinguished committee members, thank you for inviting me to testify on the Department of Defense (DOD)'s Strategy for Cyberspace. Let me first make clear, that I am testifying in a personal capacity and my comments should not be taken to reflect those of my former employer, the British Ministry of Defence.

OVERVIEW

The DOD's Strategy for Cyberspace, published in April this year, is a welcome and necessary update to the DOD's 2011 Strategy for Operating in Cyberspace, which was at the time an important and timely document. But the public conversation has evolved and it was, for example, becoming increasingly untenable for DOD's extant strategy not to acknowledge the United States' offensive cyber capability.

Cyber capabilities will undoubtedly play a major role in the future of war, and international relations more generally. The strategy demonstrates the considerable progress that the DOD has made in responding to the new challenges. That said, this still remains an emerging area in which no one yet has all the answers. Therefore, this exercise in opening up the DOD's thinking for public discussion should be welcomed and encouraged.

Nevertheless, despite the progress that the Department of Defense (DOD) has made, the Strategy is not perfect. There is more work to do particularly in establishing the exact role that the DOD should play in defending against cyber threat to the rest of Government and the private sector; and in preparing for the future operating environment. Against that background, and in the spirit of constructive criticism, I offer the following concerns that I believe warrant further inquiry.

WHAT IS THE ROLE OF THE DOD IN CYBERSPACE, ESPECIALLY IN 'DEFENDING THE NATION'?

My first major concern relates to second of DOD's self-appointed missions: 'conducting cyber operations to counter an imminent or on-going attack against the U.S. homeland or U.S. interests in cyberspace'[1]. It is relatively easy to infer what 'success' would look like when it comes to defending DOD's own networks: even if it is not possible to keep all attackers off those systems, early identification of intrusions and the removal of the intruder will be as important for DOD as for any major organization. Equally, ultimate success in terms of supporting the warfighter will be success on the battlefield. I have some concerns about the depth and breadth DOD thinking on how to achieve that goal (see below), but not in the goal itself.

On the other hand, the DOD's exact responsibilities for defending of the U.S. homeland are less clear. The Strategy talks of being 'prepared to defend the U.S. homeland and U.S. vital interests from disruptive and destructive attacks of significant consequence.' And the Strategy goes on to emphasize that use of DOD assets should be the exception. It is clear that this has been a topic of discussion within

[1] The DOD Cyber Strategy, U.S. Department of Defense, April 2015, p5

the Administration. It might also and reasonably be argued that it would be unhelpful to give potential attackers too clear an indication on when DOD would engage in a public document.

Nevertheless, particularly in the absence of a wider, up-to-date U.S. Government Strategy for Cyberspace (a major problem for the Strategy, although not the fault of DOD itself) how much the U.S. Government will depend on the DOD remains unclear. In an effort to provide reassurance that such DOD intervention in support of the private sector will be rare, Principal Cyber Advisor to the Defense Secretary Eric Rosenbach told the emerging threats and capabilities subcommittee of the Senate Armed Service Committee in April this year that the DOD would only act in the 'top 2%, the most serious'[2] of cases. In doing so, however, he only raised more questions about what that really means.

Why does this matter? For two reasons: first because a fundamental aspect of good strategy is prioritization. There are opportunity costs related to the establishment of the National Mission Force: in relation of other DOD cyber missions, in relation to other non-cyber defense capabilities, and in relation to wider non-defense priorities. And second because the way in which this mission is described in the Strategy assumes that the DOD's main role in defending the U.S. homeland from cyberattack is likely to be in cyberspace.

It is not that this mission is wrong in itself. As the Strategy points out, the DOD is 'in concert with other agencies … is responsible for defending the U.S. homeland and U.S. interests from attack'[3]. It therefore needs to ensure that it has the capability to fulfill that responsibility. It might even be argued that the very existence of the National Mission Force represents part of a credible deterrence strategy. My concern, however, is that bureaucracies have a tendency to 'do their thing', and military bureaucracies doubly so. Once the National Mission Force become established and has proven its worth, it will be tempting for others to take it for granted. My contention is that the aim should for the use of DOD capabilities to 'defend the nation' from bad actors in cyberspace to be seen as a failure of wider government policy, not the normal course of events.

Neither should we think of the National Cyber Force as the Department of Defense's only contribution to defending the U.S. homeland or vital interests from cyberattack. As set out in the 2011 International Cyberspace Strategy[4], the United States reserves the right respond 'by all necessary means' to a cyberattack, i.e., including outside of cyberspace. I believe that there is a good case to be made that one of the reasons that we have not so far experienced a very serious level of disruption or destruction is that potential attackers understand that to do so would risk a significant military response. To put it another way, there are plenty of people in the world who would like to do harm to the United States, and the tools to cause trouble in cyberspace are widely proliferated. However, given the prospect of a military response, even nation state actors have kept their actions at a level below which would justify a military response. Such threats are not easy to manage, but they do not have to be the responsibility of the DOD. Such logic does not negate the need for a National Cyber Force. It could have a major role to play when deterrence has already failed – for example with a war, or when states feel their existence is under threat and they have nothing to lose.

[2] Eric Rosenbach, Principal Cyber Advisor to the Defense Secretary, Hearing to Receive Testimony on Military Cyber Programs and Posture in Review of the Defense Authorization Request for Fiscal Year 2016 And the Future Year Defense Program, emerging threats and capabilities subcommittee of the Senate Armed Services Committee, April 14, 2015

[3] The DOD Cyber Strategy, U.S. Department of Defense, April 2015, p2

[4] The International Strategy for Cyberspace, The White House, May 2011, p14

Put simply, therefore, the ‘defend the nation’ mission will require careful and ongoing oversight to ensure that it remains properly sized to meet the need, as well as ensuring that others in Government and in the private sector do not come to depend too heavily on DOD for activities that do not need to be carried out by uniformed personnel.

DOES THE STRATEGY PROPERLY PREPARE THE DOD FOR THE FUTURE?

Another important question to ask of the Strategy is: Does it prepare DOD for the future challenges the military will face? One of the opportunity costs of an over-emphasis on the ‘defend the nation’ mission is that we risk crowding out time and resources for imaginative thinking about the ways in which cyber capabilities will affect the way in which future wars will be fought, and what that means for the United States military. My second concern is that the Strategy focuses so closely on preparing the Department for the challenges of today that it risks overlooking the need to prepare for the cyber challenges of tomorrow.

While the Strategy document acknowledges the need to respond to the actions of potential rivals, it is less clear from the document that the DOD has fully internalized the effect of the globalization of information technologies and its implications. Yet good strategy is inherently competitive and potential rivals are not standing still.

Other initiatives, such as the so-called ‘Third Offset Strategy’, show that there are some within the Pentagon who appreciate the future challenge. However, it is less clear from reading the Strategy for Cyberspace how much impact that thinking is having on cyber policy. This is not the place for a full discussion of the future operating environment, but there are several trends that will affect the way in which the United States uses its cyber capabilities that the Committee might like to ensure that the DOD is addressing.

a. Technology – While the importance of research and development is highlighted in the Strategy, there is relatively little focus on the extent to which the technology, to date an important contributor to the United States’ competitive advantage on the battlefield, will increasingly become a leveler in global affairs. This is particular true with regards to cyber capabilities for which the barriers to entry are relatively low (especially as much of the technology is commercially sourced) and through which other, increasingly networked, military capabilities can be attacked. The United States may well find plenty of ways to maintain a technological edge, but the DOD’s plans to do that with regard to cyber capabilities will be key to future military success (even if not part of the unclassified Strategy document).

b. Organization – while the Strategy does go into detail in the way in which the DOD has reorganized itself to deliver the three cyber missions, we should not expect that this will be the last reorganization. And nor should it be. Historically militaries who adapt successfully to new technology often do so by changing the way in which they organize to fight. While the Strategy focuses on the Cyber Mission Force, the true organizational challenge will be in adapting the wider U.S. Forces. This does not mean that every Service member needs to become a ‘cyber warrior’, but existing organizational constructs are unlikely to be perfectly suited to the changed operating environment. The implications of that will be difficult for the institutions affected, but to ignore that is to risk a future adversary exploiting that unwillingness to adapt.

   Just as in the Interwar years, the U.S. Navy applied some of their finest minds to classroom wargames and live exercises in order to find the right organizational concepts to incorporate

carrier aviation (leading to the replacement of the battleship with the aircraft carrier at the center of the fleet), operational experimentation will be key. This time, however, to be truly successful, such experimentation will need to be properly Joint, and – given the strength of Service interests – that means actively supported from the top of the Department.
The Committee should not expect that DOD will already have all the answers on future force structures, but it should expect senior DOD leaders to display a commitment to explore new ideas.

c. Allies – One of the best features of the Strategy is its recognition of the importance of Allies to the United States' future military edge. As potential rivals develop increasingly sophisticated technology, it will be the United States' ability to build and maintain alliances that will ensure its military edge. While the proposed actions in the Strategy make sense, the challenges in refreshing old alliances (and building new ones to take advantage of the new opportunities offered by cyberspace) and the time and work required should not be under-estimated.
The support and the encouragement of the Committee to such efforts will be important, especially as such efforts are likely to take time and considerable commitment.

d. People - The biggest opportunity for the United States military to maintain its competitive advantage in the 21st century will likely come from the quality of its people. While the Strategy acknowledges the importance of the workforce by making its development part of its first Strategic Goal, the Strategy tends to focus on the Cyber Mission Force. While that is understandable in the short to medium term, it raises questions about the capacity of the wider force to appreciate the constraints and opportunities created by the new technology and therefore the ability of the force to fully adapt. While it is understandable that DOD does not yet have all the answers to what the arrival of cyber capabilities into the battlespace means for the wider force, the Committee should expect them to be asking these questions.

To summarize: the Strategy offers a good road map to achieving the DOD's own sense of what it needs to do to achieve its responsibilities in cyberspace. I believe that that the analysis is largely correct, but that the DOD will require outside support in several key areas, most obviously in calibrating the military's role in defending the United States from cyberattack and ensuring that the significant near term challenges do not crowd out thinking about how to remain competitive on the wars of the future.