NOT FOR PUBLICATION UNTIL RELEASED BY THE SUBCOMMITTEE

Statement by

Dr. Kaigham J. Gabriel

Acting Director
Defense Advanced Research Projects Agency

Submitted to the
Senate Armed Services Committee
Subcommittee on Emerging Threats and Capabilities
United States Senate

March 20, 2012

NOT FOR PUBLICATION UNTIL RELEASED BY THE SUBCOMMITTEE

The Defense Advanced Research Projects Agency's (DARPA) role in the creation of the Internet means we were party to the immense opportunities the Internet created and share in the intense responsibility of protecting it. While national policymakers, not DARPA, will determine how cyber capabilities will be employed to protect and defend National Security interests, the Agency has a responsibility to explore the outer boundaries of such capabilities so the United States is best prepared for future challenges.

The following comments are unclassified. To understand the complete picture of the DoD cyber challenges and DARPA's contributions, classified discussions at the special access level are essential. DARPA's bottom line: DoD is capability limited, both defensively and offensively. We need to fix that.

Chairwoman Hagan, Ranking Member Portman, and members of the Subcommittee, my name is Regina E. Dugan. I am the Director of the Defense Advanced Research Projects Agency. I appreciate the opportunity to discuss DoD's cybersecurity research and development activities at DARPA.

DARPA has a multidecade history in cyber. Agency activities across the full spectrum of conflict have significantly changed the Nation's toolbox of capabilities.

In today's unclassified discussion, we can focus on the challenges of cyber defense, informed by our analytic framework. These challenges include:

- Attackers can penetrate our networks: In just 3 days and at a cost of only $18,000, the Host-Based Security System was penetrated.
- User authentication is a weak link: 53,000 passwords were provided to teams at Defcon; within 48 hours, 38,000 were cracked.
- The Defense supply chain is at risk: More than two-thirds of electronics in U.S. advanced fighter aircraft are fabricated in off-shore foundries.
- Physical systems are at risk: A smartphone hundreds of miles away took control of a car's drive system through an exploit in a wireless interface.
- The United States continues to spend on cybersecurity with limited increase in security: The Federal Government expended billions of dollars in 2010, but the number of malicious cyber intrusions has increased.

After months of original data collection and analysis, DARPA's conclusion is that the U.S. approach to cybersecurity is dominated by a strategy that layers security onto a uniform architecture. This approach is taken to create tactical breathing space, but it is not convergent with an evolving threat.

DARPA's recent testimony before Congress highlighted how cyber threats jeopardize National Security to the point of keeping the Agency leadership awake at night. Malicious cyberattacks are not merely an existential threat to DoD bits and bytes; they are a real threat to physical systems—including military systems—and to U.S. warfighters. The Unites States will not prevail against these threats simply by scaling our current approaches.

That's the defensive picture. With respect to cyber offense; DARPA's belief is that the Department must have the capability to conduct offensive operations in cyberspace to defend our Nation, Allies, and interests. To be relevant, DoD needs cyber tools to provide the President with a full range of options to use in securing our national interests. These tools must address different timescales and new targets, and will require the integrated work of cyber and electronic warfare at unprecedented levels.

Modern operations will demand the effective use of cyber, kinetic, and combined cyber and kinetic means. The shelf-life of cyber tools and capabilities is short— sometimes measured in days. To a greater degree than in other areas of Defense, cybersecurity solutions require that DoD develops the ability to build quickly, at scale, and over a broad range of capabilities. This is true for both offensive and defensive capabilities. To be sure, the list of needed capabilities is long.

Specifically, the tasks required for military purposes are sufficiently different so that we cannot simply scale intelligence cyber capabilities and adequately serve the needs of DoD. Rather, cyber options are needed that can be executed at the speed, scale, and pace of our military kinetic options with comparable predicted outcomes.

A great deal of time is spent on determining the cyber governance structure, rather than resolving the inevitable question that follows: "What now?" The lack of capability is the overwhelming issue. Further oversight strategies must be updated and be at pace with the threat.

DARPA activities are part of a larger whole within National Security at the National Security Agency, the newly formed US CYBERCOM, the Services, the private sector, universities, nonprofits and, as appropriate, the Department of Homeland Security.

Clearly, the challenges of cyberspace require the concerted efforts of many. We all must be protectors of and operate within cyberspace.

The Agency is ready to meet a continuing responsibility in advisory roles during the formation of policy and legal frameworks, because new policies and laws—domestic and international—must be executable, enforceable, and sustainable.

To be of use, such policies and laws will demand evaluation and adjustment on timescales that correspond to the dynamic nature and compressed evolutionary timescales of advances in cyberspace. That means moving faster than accustomed.

The complete picture of the cyber threat should inform such policies and laws. Truly understanding the threat, however, cannot come from unclassified discussions.

DARPA's engagement in cyber is not new. The Agency's expanded effort builds on an existing foundation and continuing contributions to cyber. DARPA-developed technologies are widely prevalent in military, intelligence, and commercial use today. But there is still much to do.

Thank you.