NOT FOR PUBLICATION UNTIL RELEASED BY THE COMMITTEE

Statement by

Dr. Bob Leheny

Acting Director
Defense Advanced Research Projects Agency

Submitted to the

Subcommittee on Technology and Innovation
and
Subcommittee on Research and Science Education

Committee on Science and Technology

United States House of Representatives

June 16, 2009

NOT FOR PUBLICATION UNTIL RELEASED BY THE COMMITTEE

Mr. Chairman, Subcommittee Members and staff: I am Bob Leheny, Acting Director of the Defense Advanced Research Projects Agency (DARPA). I am pleased to appear before you today to discuss DARPA's ongoing work in cybersecurity, or what we in the Department of Defense (DoD) call "information assurance."

I'd like to set the context for my remarks today by briefly describing DARPA's mission and how we work.

DARPA's mission is to prevent technological surprise for us and to create technological surprise for our adversaries. DARPA conducts this mission by searching for revolutionary high-payoff ideas and sponsoring research projects that bridge the gap between fundamental discoveries and their military applications. Stealth aircraft, developed at DARPA more than 25 years ago, is one among many important examples of how we create technological surprise.

To understand DARPA's role in DoD's science and technology (S&T) establishment, consider an investment timeline that runs from "near" to "far," indicative of the time required for an investment to be incorporated into an acquisition program. The "near side" represents investments that characterize much of the work of the Department's other S&T organizations, which tend to gravitate to the near term because they emphasize investments in capabilities required to meet today's mission requirements. These investments are excellent S&T and are crucial to DoD because they continuously hone U.S. military capabilities, e.g., improving the efficiency of jet engines and making existing radios more reliable. This S&T is usually focused on known systems and problems.

At the other end of the investment timeline—the "far side"—are the smaller basic research investments made by various Federal agencies and the Military Services that support fundamental discoveries, where new science, ideas, and radical concepts typically first surface. Investigators working on the far side generate ideas for entirely new types of devices or new ways to put together capabilities in a revolutionary manner, but often find that obtaining funding is difficult, if not impossible.

DARPA was created to bridge the gap between these two groups. The Agency finds the people and ideas on the far side and accelerates those ideas to the near side for transition to the DoD S&T and acquisition communities as quickly as possible. DARPA's work is high-risk and high-

payoff precisely because it bridges the gap between fundamental discoveries and their military use.

DARPA's success depends heavily on the freedom of its program managers to pursue the far side ideas that other S&T organizations overlook or, for a variety of reasons, decide not to consider. DARPA hires program managers for limited terms of 4 to 6 years, which ensures a steady input of new energy and ideas. Given their relatively short tenure, these program managers focus their time on quickly generating ideas and starting new programs. DARPA's senior leadership provides an overall technical vision and oversees the organizational coordination and collaboration activities required of any DoD organization, thus freeing the program managers to focus on their programs. This approach has enabled DARPA to pursue the ideas and programs that have benefited DoD for more than 50 years.

DARPA's strategy for accomplishing its mission is embodied in a set of strategic thrusts that guide its investments. The current strategic research thrusts that DARPA emphasizes today are:

- Robust, Secure, Self-Forming Networks
- Detection, Precision ID, Tracking, and Destruction of Elusive Targets
- Urban Area Operations
- Advanced Manned and Unmanned Systems
- Detection, Characterization, and Assessment of Underground Structures
- Space
- Increasing the Tooth-to-Tail Ratio
- Bio-Revolution
- Core Technologies, which span investments in quantum science and technology, bio-info-micro, materials, power and energy, microsystems, information technology, mathematics, manufacturing science and technology, and lasers

Today, I will discuss DARPA's vision for DoD's Robust, Secure, Self-Forming Networks and the investments in information assurance to secure those networks.

Robust, Secure, Self-Forming Networks

DoD is in the middle of a transformation to network-centric operations, which has as its goal turning information superiority into a distinct advantage so U.S. forces can operate far more effectively than any adversary. Network-centric operations fuse the typically separate functions

of intelligence and operations to dramatically speed up the observe-orient-decide-act (OODA) loop.

At the core of this concept are robust, secure, self-forming networks. These networks must be at least as reliable, available, secure, and survivable as the weapons and forces they connect. They must distribute huge amounts of data quickly and precisely across a battlefield, a theater, or the globe, delivering the right information at the right place at the right time. The networks must form, manage, defend and, when disrupted, heal very quickly.

Military network technology requirements are divided according to their application into either tactical or strategic networks. *Tactical networks* are largely wireless and directly support units and their equipment on the front lines. They must be agile, adaptive and versatile, and connect units and their equipment that are operating together, sometimes with different communication equipment, at local area ranges in all environments, including urban areas. *Strategic networks* are largely optical wired and/or satellite-based, are often operated by commercial suppliers, and provide broadband links between overseas command centers and the United States. Strategic networks globally link air, ground, and naval forces for operational maneuver and strategic strike and enable the distribution of knowledge, understanding, and supply throughout the force.

Network-centric operations require connectivity between the strategic and tactical echelons so they can rapidly and effectively share information. Technology advancements now provide the opportunity to connect these two families of networks. DARPA is bridging strategic and tactical operations with high-speed, high-capacity communications networks. The DoD strategic, high-speed fiber optic network—the Global Information Grid (GIG)—is an integrated network with a data rate of hundreds to thousands of megabits per second. To reach deployed elements, data on the GIG must be converted into a wireless format for reliable transmission to the various units within theater. This creates problems in the timely delivery of information.

To connect the tactical warrior to the GIG, DARPA is developing high-speed network technology that can robustly disseminate voice, video, text, and situation awareness information to the various military echelons and coalition forces. To accomplish this, the high data rate capability of optical communications is being combined with the high reliability and adverse-weather performance of radio frequency (RF) communications.

The goal of DARPA's Optical RF Communications Adjunct (ORCA) program is to create a high data rate backbone network via several airborne assets that nominally fly at 25,000 feet and up to 200 kilometers apart and provide GIG services to ground elements up 50 kilometers away from any one node. ORCA provides billions of information bits per second, error-free on an optical link and, at radio frequencies, hundreds of millions of information bits per second when clouds block the optical link.

For applications at sea, DARPA is working to bridge strategic and tactical maritime operations with a revolutionary new capability for submarine communications based on a blue laser efficient enough to make submarine laser communications at depth and speed a near-term reality. If successful, it will dramatically change how submarines communicate and greatly improve their operations and effectiveness, enabling submarines to become truly persistent nodes for network-centric operations at sea.

At the tactical ground level, radio interoperability has plagued DoD for decades. To connect tactical ground, airborne, and satellite communications platforms and terminals together, the Network-Centric Radio System (NCRS) program has developed a mobile, self-healing, ad hoc network gateway that provides total radio/network interoperability among these platforms moving in any terrain. NCRS builds interoperability into the network itself—rather than into each radio—allowing any radio to communicate with any other radio. Now, previously incompatible legacy tactical radios can link seamlessly among themselves and to more modern systems, including military and commercial satellite systems. DARPA is taking this technology and working on commercial components and practices to make NCRS more affordable at low rate initial production quantities. A follow-on program, Mobile Ad hoc Information Network GATEway (MAINGATE), is focused on providing this capability at a low unit cost ($60,000 each) in small volumes (1,000 units).

Another wireless challenge is frequency spectrum; it is scarce and valuable. DARPA's NeXt Generation (XG) Communications technology is making up to 10 times more spectrum available by taking advantage of spectrum assigned to others, but unused at a particular place and time. XG technology senses the spectrum being used and dynamically makes use of the spectrum that is not busy. Recently, XG conducted a series of successful experiments and demonstrations at several military locations, and various organizations within DoD are planning to transition XG technology broadly into current and existing wireless communication systems.

DARPA is developing communication networks specifically for the kind of urban environments our troops are encountering today. As is the case for civilian wireless networks, urban clutter can create multiple signals from diverse reflections ("multipath") of the initial signal, and the result is weak or fading communications. This problem is being turned into an opportunity through the DARPA Mobile Networked Multiple-Input/Multiple-Output (MNM) program, which is actually exploiting multipath phenomena to *improve* communications between moving vehicles in cities without using a fixed communications infrastructure. MNM has demonstrated reliable non-line-of-sight communications during on-the-move field trials in urban environments. The program successfully exploited multipath to increase information throughput and reliability while maintaining high data rates. It also demonstrated reliable communications in the face of interference by enabling multiple signals to simultaneously occupy the same frequency band, resulting in increased capacity of that channel.

Building on XG, MNM, and other technologies, the Wireless Network after Next (WNaN) program is developing an affordable communication system for reaching to the "tactical edge." The WNaN low-cost, highly capable radio will allow the military to communicate with every warfighter and every fielded device at all operational levels. WNaN technology will exploit high-volume, commercial components and manufacturing techniques so DoD can affordably evolve the capability. The radio cost will be low enough so that they can be refreshed after a few years of use with updated, more capable radios—as are today's commercial cell phones. DARPA is working with the Army to make a "low cost handheld networking radio" for about $500 apiece a reality. In fact, we recently signed a memorandum of agreement that could lead to the Army buying large numbers of units for military use.

Information Assurance for DoD Networks

The vision for DoD's networks covers great scope and depth, starting with the building blocks of component hardware and software, ranging from smaller networks for individual systems and tactical use to huge global networks; from wired to wireless; from mobile to fixed; and many combinations in between. These networks give the U.S. military significant advantages, which make them a very attractive, high value target for any adversary. The United States must assume its adversaries will seek ways to destroy, disrupt, distort, or infiltrate DoD's networks.

Those networks must be reliable in any environment for extended periods and protected against cyber threats. As technologies are developed and deployed to successfully block overt cyber attacks, adversaries will likely attempt to insert malicious code to disrupt the networks. DoD, with some of the most sophisticated and complex networks and facing the most sophisticated attacks, must rigorously protect its networks or suffer terrible consequences. The ever-growing sophistication of these threats has surpassed the ability of current commercial markets to provide DoD with rapid and robust solutions.

While many threats and problems are common to most types of networks—private, civilian government, and military—and many private and non-DoD researchers are addressing them, DARPA's efforts are focused on technologies to solve the Defense Department's information assurance operational challenges. Funding for our information assurance research is primarily contained in two places in our budget: an applied research budget project called "Information Assurance and Reliability" and a program element called "Cyber Security Initiative," which covers the National Cyber Range. The total in these for FY09 is about $127M, and we are requesting about $164M in FY10. The details on these requests may be found in our budget, which is available online at www.darpa.mil/budget.html.

Critical to DoD's transformation to network-centric operations are the wireless networks known as Mobile Ad Hoc NETworks (MANETs), which are designed to fluidly and automatically connect moving vehicles and dismounts as needed without a static network infrastructure. A rough analogy is a cell phone network made up *only* of cell phones—without cell towers or a telephone company. For example, a television ad for a telecommunications company shows a large crowd of people standing behind its network. MANETs must operate without this support, yet remain fully functional networks while being vigorously attacked.

The DARPA Intrinsically Assurable Mobile Ad Hoc Network (IAMANET) program is aimed directly at building DoD MANETs that are secure from the ground up. IAMANET is developing network architectures and protocols to authenticate and authorize all traffic on a MANET, quarantine problems so they don't spread, and prevent data from corruption and unauthorized exfiltration. In contrast, the current Internet does not deny unauthorized traffic by default and violates the "principle of least privilege," where a user is given no more privilege than required to perform a given task. Existing protocols are not resistant to malicious acts that can produce faulty outputs and inconsistent behavior. IAMANET technology will provide a smart router

technology for ad hoc network environments that will not forward malicious traffic, preventing infections from spreading through the network and securing information within the network.

IAMANET builds on earlier DARPA research from the Dynamic Quarantine of Worms (DQW) program. DQW technology creates an integrated system that automatically detects and responds to worm-based attacks against military networks, provides advanced warning to other DoD networks, studies and determines the worm's propagation, and automatically immunizes the network against these worms. The system quickly quarantines so-called "zero-day worms" to limit the number of machines affected and restores the infected machines to an uncontaminated state in minutes, rather than hours and days. The Marines are now conducting tests of DQW-protected systems.

MANETs are of such significance to DoD that DARPA is sponsoring basic research to develop Information Theory for Mobile Ad Hoc Networks (ITMANET) to provide a more powerful theory for mobile wireless networks. The ITMANET program is motivated in part by a major scientific accomplishment of the last century: Claude Shannon's information theory, which provides a mathematical foundation for understanding information capacity in wired, point-to-point networks. This theory is an essential foundation for today's information revolution, but is incomplete when dealing with wireless MANETs. ITMANET is extending Shannon's classic description of information capacity to the more complex mobile ad hoc network case. Stanford University and the University of Texas are leading two research teams in this effort, which involves 24 faculty members from several universities. Important program results are being reported in peer-reviewed professional journals, and, based on this research, a popular science magazine is planning a tutorial article on MANETs to popularize the concepts among a wider audience. While this work may not seem to be strictly information assurance, DARPA researchers believe it will help us understand the limits of what can and cannot be done in MANETs and inform the design of MANETs that are more secure.

DARPA's information assurance programs for wired networks will likely yield results that could be useful to a wide range of users beyond DoD.

The Trustworthy Systems program is developing innovative methods to detect unusual traffic in networks. These methods promise to be orders of magnitude more effective than traditional approaches by leveraging recent advances in statistical physics, information theory, and

thermodynamics. The goal is to detect 99 percent of attacks launched with no more than a single false alarm per day—all at gateway speeds, in the gigabits-per-second range.

The Self-Regenerative Systems (SRS) program is developing techniques to allow networks to work through attacks and automatically adjust themselves to provide critical functions in the presence of attacks. Over time, SRS will "learn" their own vulnerabilities and how to correct them, even protecting against incorrect or improper actions by authorized users. Started in 2004, the SRS program involves several universities and research firms and is advancing four key cyber defense technologies: automated software diversity, scalable redundancy, insider threat mitigation, and self-healing. The current phase of the program will move SRS technologies from the laboratory to an actual DoD system to show that the system can automatically heal itself from expert attack, while maintaining a viable level of service.

The DARPA Application Communities (AC) program is building an automatic cyber defense infrastructure for large deployments of similar applications in many places, for example, the same web browser running simultaneously on many separate computers. As a network comes under attack, continued comparison across the network permits the online construction of a universal software patch for all affected machines. The core technology for the AC program was developed at MIT and will be demonstrated in the current phase of the program in conjunction with MIT's commercial partner.

All networks rely on hardware, and to work properly that hardware must be secure. With much of the microelectronics used in DoD and other systems manufactured off-shore, the question naturally arises, "How do we know we are getting what we asked for in the microelectronics and *only* what we asked for?" The integrity of the hardware components is commonly not addressed when considering cybersecurity and networks, but it is a key issue in DoD information assurance. To the extent DoD systems use microelectronics purchased from several vendors, including foreign sources, they are at risk.

DARPA's Trusted, Uncompromised Semiconductor Technology (TRUST) program, a major information assurance program, is directly tackling this issue. Pursuing a series of complementary technologies and techniques to ensure that DoD's microelectronics will do only what they are supposed to do and nothing more, TRUST program research addresses the full production cycle of microelectronics, including design and fabrication. The program is studying

ways to determine whether malicious features have been inserted during the design or fabrication of application-specific integrated circuits or during the programming of field programmable gate arrays. DARPA is at the forefront of research in this area, confronting these issues in a comprehensive manner for the first time with expected results that will enhance and ensure the trustworthiness of microelectronics—regardless of where they have been manufactured.

National Cyber Range

DARPA's most prominent information assurance program is the National Cyber Range (NCR) project, which is part of the Comprehensive National Cybersecurity Initiative (CNCI). DARPA was selected to run this program because we have some experience in the area of cybersecurity testing.

The NCR will result in a testbed on which researchers and developers can simulate and measure technologies and their performance in a realistic environment, allowing cybersecurity technology testing under real-world conditions and across a variety of network types.

DARPA believes the NCR will accelerate the development of leap-ahead cybersecurity technology for the larger research community. The fundamental idea underlying the rationale to develop a large-scale cyber test range is the recognition that scientific progress is often paced by advances in the instrumentation available to observe and test new phenomena and to run rigorous experiments to verify the significance of these observations and theoretical insights they stimulate. Just as developments in microscopes and telescope technologies opened new worlds to scientific exploration and revolutionized our understanding of nature, the NCR, if successful, will provide the same opportunity for the cybersecurity research community.

The design goal for the NCR is to enable researchers to rapidly create network architectures under a variety of conditions, from high operational demand to aggressive cyber attack, and develop responses based on the collected data. Simulations conducted with the highly automated cyber range will allow a variety of user and network behaviors, providing researchers insight and deeper understanding of how cybersecurity and situational awareness tools function in complex environments.

When completed, the NCR will allow realistic, quantifiable tests and assessments of cybersecurity scenarios and defensive technologies, revolutionizing cybersecurity testing by offering vastly improved cyber testing capabilities in terms of:

- Scope. The NCR will allow unclassified and classified testing on the same facilities, including wired and wireless networks, MANETs, supervisory control and data acquisition systems, and other features to simulate an extremely large variety of networks. It will allow defensive technologies to be tested against realistic offensives and greatly improve and accelerate researchers' abilities to produce solutions and rapidly deploy them.

- Scale. The NCR will have orders of magnitude more nodes than currently available test ranges, providing a much more realistic and valid test environment.

- Flexibility Through Automation. Under software control, the NCR will be able to quickly set up a wide variety of test networks and permit multiple, independent experiments on the same infrastructure. A graphical user interface will allow test directors to use a drag-and-drop feature to quickly lay out a network architecture, its hosts, system latency, environmental characteristics, and other pertinent test qualities and requirements. Once this infrastructure is created, it will be ready for testing immediately; the impact will be to dramatically change the time required to create a test environment from months to minutes.

- Efficiency. The NCR's state-of-the-art instrumentation and forensics technology will enable far better use of test time.

I think that NCR could operate much like other major National research assets and laboratories. A number of potential operating models exist, including the DoD's High Performance Computing Modernization Program, which has been run by the DoD since the early 1990s and makes high performance computing facilities available to Defense researchers for both classified and unclassified projects.

I believe, for example, that NCR could have a panel that reviews and prioritizes proposals submitted by potential users for time on the range. One of their guiding principles would be to ensure that the portfolio of research fulfills the mission of the range. Such a panel would then

schedule who gets access to the range and when, and what they can do on the range. An administrator would facilitate users' access and use of the range and ensure their individual research goals on the range are met. I am sure that other possible operating models exist.

Two primary technical challenges must be tackled to achieve NCR's goals: (1) How are large-scale, highly heterogeneous networks simulated realistically, and what is the scale and scope needed for realistic experiments?; and (2) What instruments can be created to monitor performance during experiments to provide the greatest meaningful understanding of the results, even providing quantitative measures of performance? Real-world cybersecurity events are taking place all the time, but existing network administration techniques provide little insight into their cause without considerable effort. The point of the NCR is to incorporate highly sophisticated, fast, flexible, and efficient instrumentation and administration technologies, in a controlled environment, to enable full understanding of such phenomena rapidly and with little effort.

In November 2007, DARPA released an unclassified Request for Information where we solicited the community for ideas to improve cyber testing. In May 2008, DARPA released a Broad Agency Announcement and conducted a two-day unclassified industry day soliciting solutions from the community and answering questions posed by the community. A government-wide source selection process selected the best of breed from those proposed. The NCR program is in its first phase. During this phase, there are seven teams of defense contractors, universities, small businesses, vendors, and service providers working on competing designs to be completed and delivered this summer. The next phase will be to take several selected design teams forward to build small-scale prototypes. We expect that selection and build phase to be completed in fall of next year, and then move on to completion and operation of the range.

DARPA will not own or operate the NCR when completed. Historically, DARPA facilities and institutional interests have been held to an absolute minimum, allowing the Agency to be open to new ideas. To remain consistent with this management philosophy, DARPA will not own or operate the NCR once it is built.

The NCR is an integral part of the CNCI, and within NCR are two key working groups. The NCR Joint Working Group is a stakeholders' panel headed by DARPA that is developing the technical vision and business model for the NCR. This work informs the technical capabilities

needed and provides options on how the NCR will operate. Many issues are being studied, including who will manage the NCR, how it will be funded, who will have access, and conditions for use. Working group members represent DoD; the Intelligence Community; Departments of Homeland Security, Energy, and Treasury; National Science Foundation; Federal Bureau of Investigation; National Institute of Standards and Technology; the New York State Governor's Office; and the New Jersey State Police. They are invited to participate in all the steps from concept development to performer selection and periodic program reviews.

A separate working group focuses on the crucial issue of NCR security requirements. The range will have to be certified to run classified and unclassified testing, and the various agencies have different security requirements and nomenclatures. This working group seeks security protocols that will allow the NCR to be properly accredited by agencies from across the Government.

Coordination of Research

Much of the coordination of DARPA research with other Government agencies occurs as a bottom-up process within technical communities. DARPA program managers are hired from Government, industry, and academia in large measure because they are world-class technical experts with extensive knowledge of the research being done in their technical areas. In the last 8 years, roughly one-third of DARPA program managers have come from industry, one-third from other parts of DoD, one-quarter from academia, and one-tenth from elsewhere. More than 95 percent of DARPA's program managers have advanced degrees and are subject matter experts from a wide variety of backgrounds. DARPA's policy of rotating program managers after 4 to 6 years ensures a steady stream of new people bringing fresh ideas to the Agency.

Because DARPA conducts none of its research in-house, its program managers look externally for ideas and research performers. During the process of starting programs, they seek good ideas wherever those ideas can be found, frequently by hosting workshops attended by researchers and other Government experts. Engaging a wide spectrum of experts in a field through this extensive outreach effort is how DARPA coordinates ideas and research.

With that overall process in mind, let me give you some examples of how we have worked with the National Science Foundation (NSF) in information assurance.

DARPA co-funded three projects through the NSF Cybertrust Program (led by Stanford, University of Texas, and Princeton) dealing with fundamental software techniques for high assurance and security. NSF administered these grants to university researchers after their selection through the Foundation's standard, community-based, merit review process.

This summer, DARPA and NSF will co-sponsor two research workshops related to cybersecurity. Both workshops will bring together key thought leaders from universities, National Institute of Standards and Technology, Department of Homeland Security, National Science Foundation, and DARPA. The first workshop is in clean slate security architectures, which will identify paths to fundamentally redesigning computers for modern threats. The second workshop is meant to begin re-thinking the Internet. As you know, DARPA played a key role in developing the Internet, and our interest in the future Internet design workshop is to identify fundamental new network concepts that are far more resistant to attack than the current Internet.

60-Day *Cyberspace Policy Review*

The report that came out of the 60-day *Cyberspace Policy Review* is a high-level document covering a very wide variety of policy issues, including leadership, organization, legal, education and training, and operations and incident response. With respect to research issues, the area of DARPA's expertise, the review clearly recognizes the centrality of innovation to our national cybersecurity capabilities. In particular, it contains a discussion of the supply chain threats that we are addressing in our TRUST program—a problem that may not be widely appreciated outside the national security community. It also discusses the need for modeling and simulation, capabilities that could be provided by the NCR when it is completed. In general, between the game-changing technology we are promoting and the new tools and facilities of the NCR, DARPA will be able to make a significant contribution to the innovation goals of the *Cyberspace Policy Review*.

We are at the early stages of what will come out of the 60-day review, but having senior leadership at the White House looking hard at cybersecurity across the federal government will keep it high on the national agenda and stimulate progress throughout the field. As this process moves forward and we get a new Director at DARPA, we will be sure to continue to evaluate our own plans, programs and budgets for cybersecurity. We have been a leader in promoting

cybersecurity research, and we look forward to continuing our role promoting radical innovation for national security as the implications of 60-day review develop more fully.

The DoD's move toward network-centric operations means that information assurance will remain a crucial and long-standing concern. I hope my testimony today has given you a sense of DARPA's plans and ambitions.

I would be pleased to answer your questions.