Statement by

Dr. Tony Tether

Director
Defense Advanced Research Projects Agency

Submitted to the

Committee on Science

United States House of Representatives

May 14, 2003

NOT FOR PUBLICATION UNTIL RELEASED BY THE SUBCOMMITTEE

Mr. Chairman, Committee Members, and staff: I am Tony Tether, Director of the Defense Advanced Research Projects Agency (DARPA). I am pleased to appear before you today to talk about DARPA's work to develop secure Defense networks and how that work relates to the subject of cybersecurity, or what we call information assurance.

Some of you may not be familiar with DARPA, so let me begin by saying a few words about who we are and what we do.

Since the time of Sputnik, DARPA has had a special mission within the Department of Defense (DoD): maintain the technological superiority of the U.S. military and prevent technological surprise from harming our national security. DARPA does this by sponsoring revolutionary, high-payoff research that bridges the gap between fundamental discoveries and their military uses.

Let me tell you a little bit about how DARPA works.

Imagine a science and technology (S&T) investment time-line that runs from "Near" to "Far," indicative of how long it takes for an S&T investment to be incorporated into an acquisition program. On the "Near side" of this timeline we have a lot of investment that represents most of the work of the Service S&T organizations. This S&T tends to gravitate towards the Near side because the Services emphasize providing technical capabilities critical to the mission requirements of today's warfighter. This excellent work continuously hones U.S. military capabilities. However, it is typically focused on known systems and problems.

In contrast, out at the other end of the investment timeline – we'll call this the "Far side" – there is a much smaller investment that represents funding fundamental discoveries, where new science, new ideas, and radical new concepts typically first surface. People working on the Far side have ideas for entirely new types of devices, or new ways to put together capabilities from different Services in a revolutionary manner. But, the people on the Far side have a difficult, and sometimes impossible time obtaining funding from the larger, near side investors because of the near side's focus on current, known, and pressing problems.

DARPA was created to span the gap between these two groups. DARPA's mission is to find the promising ideas (and people) out on the Far side and accelerate those ideas to the Near side as

quickly as possible. DARPA emphasizes what future commanders might want and pursues opportunities for bringing entirely new core capabilities into the Department.

Hence, DARPA mines fundamental discoveries – the Far side – and accelerates their development and lowers their risks until they prove their promise and can be adopted by the Services. DARPA's work is high-payoff *precisely* because it fills the gap between fundamental discoveries and their military use.

What is surprising to many people, but entirely in-line with DARPA's mission, is that only about five percent of DARPA's research is *basic* research. Basic research, much of that "Far side" investment, is primarily supported by organizations like the Office of Naval Research (ONR), the National Science Foundation (NSF), the National Institutes of Health (NIH), and the Department of Energy (DOE).

Basic research creates new knowledge and technical *capacity*, whereas DARPA creates new *capabilities* for national security by accelerating that knowledge and capacity into use. So we count on institutions like ONR, NSF, NIH, and DOE to provide us with a feedstock of revolutionary technical concepts that we, at DARPA, can then develop and turn into revolutionary Defense capabilities.

Through the years, DARPA has refocused its work in response to evolving national security threats and technological opportunities, and DARPA's *Strategic Plan* describes how we are pursuing our mission today. One of our eight strategic thrusts is Robust, Self-Forming Networks, which contains our work in information assurance.

Let me briefly describe it to you:

DARPA's Strategic Thrust in Robust, Self-Forming Networks

The Department of Defense is in the middle of a transformation to what is often termed "network centric warfare." In simplest terms, network centric warfare is when military organizations and systems are seamlessly networked to change the terms of any conflict to favor U.S. and coalition forces. It will allow the United States and our allies to go beyond a simple correlation of local forces by providing them better information and letting them plan and coordinate attacks far more quickly and effectively than our adversaries can.

However, at the heart of this concept are survivable, assured, spectrum-agile communications at both the strategic and tactical levels. The goal of this work is a high capacity network that degrades softly under attack, while always providing a critical level of service.

To support this vision, DARPA is conducting research in areas that include: (1) self-forming *ad hoc* networks; (2) high capacity, multiband, multimode communications systems; (3) ultra-wideband communications; (4) spectrum sharing; (5) low probability of detection/intercept/exploitation communications; and, (6) information assurance or cybersecurity.

I could spend pages describing our efforts in the first five areas. However, our focus today is cybersecurity, so let me turn to what we are doing to ensure that those military networks are secure and reliable.

DARPA's Information Assurance Research

What we at DARPA call "information assurance" (often referred to as "cybersecurity") is crucial to having the robust, self-forming networks required to successfully conduct network centric warfare. One must look no further than the ongoing Iraq War to see that the United States has been moving toward network-centric warfare.

While people can debate the extent to which we have achieved network centric warfare, today's U.S. military forces are unmistakably *network-dependent*. Therefore, the very first thing that a sensible adversary would do to asymmetrically negate the U.S. force is take down our military networks. For quite some time, we have faced the very difficult problem of figuring out how to protect our military networks.

DARPA has had information assurance work going on in some form and by some name for decades. But, in the early 1990s we started to concentrate in earnest on the problem of information assurance, with the usual DARPA focus on solving extremely hard problems. Initially, our emphasis was to secure hardwired computer networks. DARPA's approach to solving the problem of information assurance evolved, over time, to a layered approach.

The first layer that we worked on in the early 1990's was preventing, or "locking out" cyber attacks. This resulted in the "firewalls" that are commonly available in the commercial world today.

In fact, today's commonly available commercial firewalls started with a DARPA project to protect the World Wide Web at the White House. The DARPA contractor that did this work published the firewall source code in the open literature, and from that work grew over a hundred firewall companies and an entire market for firewall products.

The second layer in DARPA's approach to information assurance has been detecting attacks and limiting their damage. In addition to intrusion detection, DARPA has more recently demonstrated both hundred-fold reduction in the false alarm rates that plague current intrusion detection systems, and the ability to detect new and novel forms of attack through anomaly based detection. Over the last two years, DARPA has demonstrated such detection capabilities in the field in major exercises such as the Navy Fleet Battle Experiment series.

A third pursuit, and one that DARPA has been increasingly emphasizing, is developing the ability to operate *through* cyber attacks. The simple logic here is that we simply cannot block all attacks, nor can we completely limit the damage from attacks. So we have to be able to continue operating while an attack is underway, in spite of the damage that the attack may inflict.

Let me give you a flavor of where we are today in some of the information assurance programs that we are working on at DARPA right now:

- The **Cyber Panel** program is working on ways to detect new attacks in real-time, including previously unknown attacks, predict what damage the attacks will inflict, and implement effective defenses.

- The **Fault Tolerant Networks** program is working on ways to ensure that a network remains available, even during an attack, while restricting the network resources available to the attacker. In fact, this program has resulted in a commercial product, Peakflow™, that is being used to protect against Distributed Denial of Service attacks.

- The **Dynamic Coalitions** program is working on methods to quickly set up secure networks – a critical problem for today's U.S. fighting forces. Some of this technology is being used in the joint DARPA-Army Future Combat Systems program, a program that has network centric warfare as a starting assumption.

- The **Organically Assured and Survivable Information Systems** (OASIS) program is working to provide a "last line of defense" by developing ways to enable critical DoD

computers (as distinct from the network level) to operate through a cyber attack, degrade gracefully if necessary, and allow real-time, controlled trade-offs between system performance and system security through such techniques as redundancy and diversity of operating systems.

A prototype military system to produce Air Tasking Orders for the U.S. Air Force is also being developed. The system, and the underlying information assurance technology, will be tested in 2004 by subjecting it to a sustained cyber attack from a "red team."

Much of what we have done, particularly for wired systems, has proved useful in both commercial and military systems. But, our focus is the specific problems DoD needs solved for network centric warfare.

The military-specific problems that we are working on go beyond those faced by the commercial world today. Military networks, more than commercial networks, involve large-scale, highly distributed, mobile networks-of-networks that are increasingly wireless, deal with time-critical problems, and face potential attackers who are extremely dedicated and sophisticated. Failure in military networks has extreme consequences.

Moreover, network centric warfare involves networks that must assemble and reassemble on-the-fly on an *ad hoc* basis without having a fixed or set infrastructure in-place. In effect, we must achieve what has been called, "critical infrastructure protection" without infrastructure.

In the most advanced cases, these are peer –to-peer or "infrastructure less" networks. There is no fixed, in-place network equipment – the whole network architecture is fluid and reassembles dynamically. It could be that, in the long term, commercial networks will acquire some of these features, but, for now the Department of Defense is in the lead in facing these problems.

DARPA is taking a broad-based view of information assurance. When we think about information assurance, we include technology such as communications security and encryption as part of our solution. The threat to military networks is not simply hackers, but organized and well resourced nation states that want to eavesdrop on military network traffic, or interfere with it at precisely the wrong time.

In fact, information assurance in a world of growing network centric warfare must become a regular feature of most military programs – in the same sense that everyone building an airplane must consider materials, not *only* material scientists.

A significant and growing element of DARPA's work in information assurance is classified, and cannot be discussed in this forum. The future thrust is for more of these efforts to become classified. Why? Because of our increasing dependence on networks, their vulnerabilities and techniques for protecting them become more and more sensitive. Accordingly, our efforts have become classified.

In the longer term, I expect that DARPA's strategic thrust in Cognitive Computing could also lead to important contributions to information assurance. While I cannot discuss it at length today, our Cognitive Computing thrust aimed at developing computers and networks that are "self-aware" – that is, computers that actually *know* what they're doing and *know* what is happening to them.

Future network-centric warfare systems will be able to leverage "self-aware" capabilities to determine when they are under attack and autonomically respond, and reconfigure themselves in much the same way as the human body reacts to an infection. If such systems could be built, they should be able to do a much better job of protecting themselves because they will understand that they're being attacked.

I realize that there has been some concern about DARPA's level of funding in the area of information assurance. For example, some have expressed the opinion that our budget for this effort is dropping drastically.

Let me reassure you that we have a robust program in information assurance, and we plan to continue this robust program in the coming years. There are natural variations in our budget, and they are due to several factors such as when large programs like Fault Tolerant Networks and OASIS come to an end.

The budget structure does not always capture the great variety of information assurance work going on, particularly when it is an integral part of another program, as it is in Future Combat Systems. And, there are the aforementioned classified programs that obscure the budget picture.

Thus, while we are putting more emphasis on military-specific problems, we will continue to have a robust program that will, in the long term, have a broad, beneficial impact on the commercial world.

Finally, I understand that a particular interest of the committee is how we coordinate and disseminate the results of our research to other Federal agencies and to the commercial world.

Much of our interaction with industry stems from using companies as performers of our research, and the strong desire of smaller commercial firms to commercialize their technology. For instance, in 1999 DARPA foresaw the threat of Distributed Denial of Service that hit Yahoo and e-Bay a few years later, and invested accordingly to create the Fault Tolerant Networks program. Today, the nascent market for solutions against this threat consists primarily of technologies that have their roots in DARPA research, technology that can protect the military, like the example I mentioned earlier.

DARPA also makes efforts to broadly communicate our results in a more structured way by sponsoring the DARPA Information Survivability Conference and Exposition (DISCEX) conferences. The audience at DISCEX is very broad, and it includes the extended research community, the operational military, developers of military systems, and the commercial industry that generates the "off the shelf" systems that comprise most military information systems.

Our goal in these meetings is to stimulate scientists, developers, and joint operational customers with research products, experimental results, and capabilities emerging from DARPA research to better address the military's needs for information security. The most recent conference included over 250 attendees with 60 researchers giving technology demonstrations and produced two volumes of technical proceedings.

In addition, while many ideas on information assurance are being exchanged informally through the professional relationships between researchers and the U.S. Government officials who sponsor their work, DARPA is the primary sponsor of the Infosec Research Council (IRC), an informal coordinating body begun in 1996 that is comprised of U.S. Government members concerned with funding and conducting research in information security/information assurance/cyber security. The IRC members include DARPA, the National Security Agency, the

National Science Foundation, the National Institute of Standards and Technology, the Department of Energy, and the Federal Aviation Administration.

I should also mention the collaborations and consultations between NSF and DARPA personnel. This interaction goes beyond the simple exchange of technical information that typically characterizes inter-agency information exchange programs.

DARPA and NSF personnel for example co-fund particular projects where a true synergistic opportunity exists. NSF's program, "Ultra-High-Capacity Optical Communications: Challenges in Broadband Optical Access, Materials Processing, and Manufacturing" has direct participation by DARPA personnel and a modest level of DARPA funding. NSF personnel likewise take part in DARPA source selection panels where similar technical interests can be found.

NSF's "Networking Research Testbeds Program" is of special interest to DARPA in that it offers the possibility of making available world-class network testbeds to DOD contractors and personnel. Network testbed collaboration meetings are now routinely held by DARPA and NSF program managers, and I expect that these testbeds will be very useful as we explore alternative architectures, systems and protocols for future optical networks; wireless networks based on spectrum sharing; distributed sensor networks; and networking in highly dynamic and/or harsh environments. We have also been having discussions with NSF personnel about our thrust in Cognitive Computing.

The Department of Defense is steadily increasing its dependence on information systems that are crucial to our future vision of network centric warfare. I hope my remarks today have given you a sense of what DARPA is doing to ensure that those networks perform reliably and that they remain secure.

I would be happy to answer your questions.

ANTHONY J. TETHER
DIRECTOR
DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

Dr. Anthony J. Tether was appointed as Director of the Defense Advanced Research Projects Agency (DARPA) on June 18, 2001. DARPA is the principal Agency within the Department of Defense for research, development, and demonstration of concepts, devices, and systems that provide highly advanced military capabilities. As Director, Dr. Tether is responsible for management of the Agency's projects for high-payoff, innovative research and development.

Until his appointment as Director, DARPA, Dr. Tether held the position of Chief Executive Officer and President of The Sequoia Group, which he founded in 1996. The Sequoia Group provided program management and strategy development services to government and industry. From 1994 to 1996, Dr. Tether served as Chief Executive Officer for Dynamics Technology Inc. From 1992 to 1994, he was Vice President of Science Applications International Corporation's (SAIC) Advanced Technology Sector, and then Vice President and General Manager for Range Systems at SAIC. Prior to this, he spent six years as Vice President for Technology and Advanced Development at Ford Aerospace Corp., which was acquired by Loral Corporation during that period. He has also held positions in the Department of Defense, serving as Director of DARPA's Strategic Technology Office in 1982 through 1986, and as Director of the National Intelligence Office in the Office of the Secretary of Defense from 1978 to 1982. Prior to entering government service, he served as Executive Vice President of Systems Control Inc. from 1969 to 1978, where he applied estimation and control theory to military and commercial problems with particular concentration on development and specification of algorithms to perform real-time resource allocation and control.

Dr. Tether has served on Army and Defense Science Boards and on the Office of National Drug Control Policy Research and Development Committee. He is a member of the Institute of Electrical and Electronics Engineers (IEEE) and is listed in several Who's Who publications. In 1986, he was honored with both the National Intelligence Medal and the Department of Defense Civilian Meritorious Service Medal.

Dr. Tether received his Bachelor's of Electrical Engineering from Rensselaer Polytechnic Institute in 1964, and his Master of Science (1965) and Ph.D. (1969) in Electrical Engineering from Stanford University.

June 2001