Statement by

Dr. Tony Tether

Director
Defense Advanced Research Projects Agency

Submitted to the

Subcommittee on Terrorism, Unconventional Threats and Capabilities
House Armed Services Committee
United States House of Representatives

March 19, 2003

NOT FOR PUBLICATION UNTIL RELEASED BY THE SUBCOMMITTEE

Mr. Chairman, Subcommittee Members, and staff: I am Tony Tether, the Director of the Defense Advanced Research Projects Agency (DARPA.) I am pleased to appear before you today to discuss DARPA's research to counter the weapons of mass destruction (WMD) that our nation faces today.

At DARPA, our primary area of emphasis in countering WMD has been biological warfare defense (BWD) research, work that we began in earnest in the mid-1990s when it become clear that the threat of biological attack was growing sharply. DARPA moved out ahead of the threat by establishing a comprehensive, aggressive, and innovative BWD program. DARPA's work complements mainstream Federal and commercial BWD efforts. However, DARPA does not constrain its work to the Validated Threat List published by the Defense Intelligence Agency because our enemies will not necessarily stick to the validated list. It is important to also work on "non-validated" threats that could pose a great danger to all Americans. This lets us pursue general solutions to the biological warfare (BW) problem, including the worrisome threat from genetically engineered pathogens.

A framework for discussing BWD is to consider the different stages surrounding a biological attack. These stages tell us what we need to do and when we need to do it – that is, what technology we need and what research we need to invest in.

- *Prior to a BW attack*, we need to boost people's immunity and the effectiveness of vaccines and, if possible, do all we can to keep an attack from happening in the first place.
- *During an attack*, we need sensors to determine its nature – including what agent was used and who was exposed – to set the stage for our response.
- In the *minutes and hours after an attack*, we need immediate ways to protect people.
- In the *hours to days after an attack*, we must coordinate the first responders and manage the medical system. During those same hours and days, we must begin to diagnose and treat the victims.
- And in the *days and perhaps years after an attack*, we must decontaminate the attacked area.

Let me take these stages one by one, and give you a sample of what DARPA has been doing in each.

Prior to an Attack

Let's begin with the time *before* an attack. Obviously, our number-one priority is to try to prevent an attack from occurring at all. We want to discover the plan for an attack and then take action to disrupt it before it can be carried out. This requires good, actionable intelligence, and DARPA's Information Awareness Office (IAO) is focused on developing the tools to ferret out terrorists' plans. IAO's programs have been the subject of recent controversy, and, since their scope is counter-terrorism in general, rather than specifically focused on countering WMD, I won't discuss them in detail today. But IAO's activities are all about "connecting-the-dots" to uncover planned terror attacks and prevent them.

To protect people from an attack before it occurs, we have been working with considerable success on a compound called CpG. CpG boosts the body's natural immunity to disease, essentially by priming the immune system to mount an aggressive defense, which could be of great use to first responders. And, it can be used as an adjuvant to dramatically improve the effectiveness and speed of vaccines. For example, animal tests have shown that by combining anthrax vaccine with CpG, we need less vaccine and fewer doses while achieving faster protection with fewer side effects. CpG is part of our comprehensive effort to take anthrax "off the table" as a threat. I will talk more about anthrax later, but we think CpG will prove useful against many other pathogens. We expect to begin human trials of CpG with the current anthrax vaccine this summer.

During an Attack

First, I'd like to talk about sensors. The ideal sensor would specifically identify individual pathogens across the entire range of pathogens, including previously unknown ones, and it would be very fast. Moreover, it would be small, inexpensive, lightweight, and low-power. Unfortunately, as you might guess, these qualities tend to be in conflict with each other, and tradeoffs are necessary. Hence, we need a whole family of sensors – different ones optimized for different purposes. For example, to protect people from being exposed during an attack, *speed* is paramount to protect first and only later figure out what the pathogen was. On the other hand, if

an attack has already happened and people have been exposed, *specificity* is paramount, because we need to determine exactly what people have been exposed to so we can immediately begin administering the right treatment. Another issue is the false-alarm problem, which varies with the specific environment in which the sensors are used and whose severity depends on the steps taken in response to an alarm; in both aspects, military and domestic applications differ widely. Across this complex trade space, DARPA has been working since the mid-1990's to develop a family of sensors that systematically meet these challenges.

A number of our sensors have been picked up by the Military Services and are being fielded or are close to being fielded. DARPA developed a biosensor microarray for rapid identification of biological warfare agents. Like computer chips, which perform millions of mathematical operations per second, DARPA's microarray biochips can perform thousands of biological reactions in a minute with great sensitivity. Moreover, these biochips can be reused up to 50 times, effectively reducing their cost to about $1.00 per use. These biochips have been transitioned to U.S. Army Soldier and Biological Chemical Command for further testing against live biological agents.

We are all familiar with how canaries were used in coal mines to test the air. DARPA has been pursuing a similar approach, except in our case the "canary" consists of cells on a chip. Cells, of course, do not like being exposed to pathogens, and they are very fast and very sensitive indicators of a problem. Tests have shown that these chips can detect as few as 10 to 50 viruses or bacteria in only 10 to 20 seconds.

A more recent sensor program is TIGER (Triangulation Identification for Genetic Evaluation of Risk). TIGER is trying to develop a universal sensor that can detect any type of pathogen – even unknown and engineered ones – through an innovative method of measuring and weighing nucleic acid sequences. TIGER involves integrating data from multiple regions along an organism's genome to derive a unique identifier for that organism. This should enable us to detect and classify known and unknown threats in complex mixtures – especially those that, today, are known to result in false-alarm rates so high that other sensors are effectively useless.

Turning from sensors to making sense of information, our Bio-ALIRT (Bio-Event Advanced Leading Indicator Recognition Technology) program, one of our IAO Programs, is developing software to detect covert biological attacks early through statistical, population-level analysis on

items like school and work absences, over-the-counter medicine purchases, nurse hot line and poison control center calls, and even animal illness.

Because the surveillance target of Bio-ALIRT is diseases and not people, individual identifying information is not needed or wanted. What is important is statistics about the population, not the activities of any individual. We are also using medical information in nontraditional ways, examining items such as initial complaints or tests that are ordered, rather than waiting for formal diagnoses. Advancing the time we detect an attack by even a few days could help cut short an epidemic and prevent as many as half the casualties.

Bio-ALIRT technology is currently being used to monitor the health of our nondeployed military forces world-wide and will soon be incorporated into the Joint Medical Workstation for use by Central Command's command surgeon and his staff. Bio-ALIRT technology is being tested and evaluated around Washington, DC and Hampton Roads, Virginia, which have large concentrations of military assets.

Software developed at the University of Pittsburgh and Carnegie-Mellon University has been made available to public health departments for their use. In fact, Bio-ALIRT technology identified outbreaks of scarlet fever around Washington and the Norwalk virus at the Marine Base in San Diego, before they were noticed by local public health authorities.

Minutes to Hours after an Attack

In the minutes to hours after a biological attack, we need to protect the people in the area of the attack. Our most prominent program addressing this time period is the Immune Building program, the goal of which is to keep people safe inside a building that has been attacked by bioterrorists. The Immune Building program predates the anthrax attack on the Congress, which demonstrated why such an effort is needed. Protecting a building from an outside attack, while not trivial, is fairly well understood. The more insidious attacks originate inside a building, as the anthrax letters of 2001 demonstrated. Unfortunately, the Heating, Ventilation and Cooling (HVAC) systems in most office buildings actually spread an agent around the building and infect even more people. DARPA is developing components, systems, and architectures so "smart" HVAC systems, including sensors and neutralization devices, could be used to protect the

occupants of the building from attack and isolate the attacked area, instead of exacerbating its severity. These systems are being designed to protect against chemical attacks as well.

Hours and Days after an Attack

In the hours and days after a biological attack, we enter the consequence management phase, which involves managing the first responders and the medical resources to care for the victims. About two years ago, DARPA concluded its ENCOMPASS program, which was designed to effectively and efficiently deploy scarce medical resources in chaotic circumstances. A commercialized version of ENCOMPASS, LEADERS, provided medical surveillance for signs and symptoms of a biological attack for the state of New York within 24 hours of the attack on the World Trade Center. The Centers for Disease Control and Prevention (CDC) also used LEADERS to monitor for specified syndromes from hospitals in the New York City area and report them back in real-time to the CDC in Atlanta via the Internet. And, technology from ENCOMPASS is being used in emergency rooms in Northern Virginia to help 911 operators properly route patients.

In addition, while not originally designed for consequence management *per se*, other technologies that DARPA is working on today may eventually prove useful in such situations, particularly if adapted for use by first responders. For example, we are developing communications systems that could create self-forming networks for people on foot in urban environments (Small Unit Operations Situation Awareness System program). We may be able to restore communications throughout a region via a highly flexible, airborne communications switchboard (Airborne Communications Node). And our work in robotics and ducted-fan unmanned aerial vehicles (Organic Air Vehicle) could provide ways to enter and investigate attacked areas without putting more people at risk.

We must also care for the exposed victims. DARPA's most prominent medical treatment program is the Unconventional Pathogen Countermeasures (UPC) program. UPC is an aggressive and innovative program that has been trying to go far beyond "one-bug/one-drug" therapies for BW pathogens. Instead, UPC is focused on trying to develop new drugs and treatments that would be useful against all pathogens, known and unknown, naturally occurring and engineered. We are trying to make drugs to which pathogens *cannot* develop resistance. We are trying to create therapies to push out the "point of no return" – that point in the progress of

disease beyond which there is no effective treatment. Our work here is driven by the recognition that there are extremely dangerous natural threats, such as smallpox, and there are engineered threats – pathogens we have not seen before and against which our current vaccines and therapies may not be effective.

A highlight of our UPC program has been its work to eliminate anthrax as a threat, which was accelerated in the aftermath of the attack on the Congress. We have been developing six new, distinct, and complementary approaches to fighting anthrax. One is CpG, which, as I mentioned earlier, can boost immunity and the effectiveness of vaccines. Another is an extremely broad spectrum antigenomic drug that should be able to kill most pathogens. The antigenomic drug works by "jamming" DNA that has many AT pairs, the nucleic acid pair that overwhelmingly dominates the genetic code of most pathogens. Another drug is an antibiotic that works by blocking a critical enzyme that is used briefly and only during cell replication. It would be extremely difficult for a pathogen to develop resistance to either this or the antigenomic drug. A fourth compound is a protein that essentially functions as a decoy to prevent anthrax toxins from being assembled and released. This might be particularly helpful in late-stage anthrax to limit toxicity, while other drugs attack the infection. A fifth compound is similarly meant to strengthen the body's overall resistance to septic shock, extend the point of no return, and buy time to fight the infection. The sixth program uses an enzyme called lysin as an antibacterial "precision-guided munition" that specifically targets and kills the anthrax bacterium and nothing else. Seventy percent of mice treated with this enzyme survived after they were exposed to a lethal dose of anthrax, compared to *no* survivors among the untreated mice. This approach to fighting disease was featured on the cover of *Nature* magazine last August.

I am pleased to report to you today that, based on current status of the research and assuming we continue to get good results, we anticipate that a majority of these accelerated anthrax therapeutics programs will be conducting Phase I human safety trials by the last quarter of this calendar year. This is, frankly, better than we expected. Just as important, and in keeping with the philosophy of the UPC program, most of these therapeutics show promise for many pathogens besides anthrax. For example, the antigenomic drug, when administered to mice, has shown itself to be a better treatment for malaria than the current "gold standard" antimalarial drug. And most thrilling is the fact that the antigenomic drug has shown real potential to become the first actual therapeutic for both anthrax and smallpox.

Days and Perhaps Years after an Attack

Now let me turn to the last phase of the postattack timeline, decontamination. The anthrax release in the Hart Building demonstrated how difficult it is to clean up a biologically contaminated building. Even if systems such as those being developed in the Immune Building program prove successful, we must still decontaminate the affected areas of buildings.

Because of DARPA's investments in the Immune Building program, we were asked to provide science advisors to the team responsible for the anthrax decontamination of the Hart Building. We reviewed decontamination technologies and conducted quick-turnaround testing on three separate candidates to determine efficacy. The chlorine dioxide approach developed under Immune Building was selected for the challenging job of remediating the Hart Building and, more recently, the Brentwood Post Office. In addition, DARPA helped identify and obtain air sampling equipment to support the Environmental Protection Agency and CDC in verifying that the buildings were safe for reoccupation. DARPA also developed, installed, and tested mail-screening equipment to prevent additional contamination from entering the buildings through the mail system.

Finally, in the area of non-BWD decontamination, increasing attention is being paid to the threat of a radiological dispersal device, the so-called "dirty bomb." Nuclear decontamination of an area, especially an urban setting, is an enormously difficult and expensive problem and helps explains its appeal to terrorists bent on creating physical, psychological, and economic havoc. This fiscal year, DARPA has begun studying decontamination methods and technologies following an attack using this kind of terrorist device.

I hope this brief sampling has illustrated the breadth and depth of DARPA's efforts to counter weapons of mass destruction, particularly biological warfare. Our initial work in 1995 on biological warfare defense has grown and adapted, we have made very solid progress over the past eight years. But we also know the threat remains quite real and may be spreading. We continue to press ahead to develop technologies that will change our fundamental approach to all phases of the biological attack timeline.

This concludes my remarks. Thank you for this opportunity to discuss DARPA's biological warfare defense research. I would be happy to answer any questions.