2005 Naval – Industry Partnership Conference
Washington, D.C.
July 28, 2005

John Marburger
Director, Office of Science and Technology Policy
Executive Office of the President

"Enabling Naval Innovations to Win the Global War on Terrorism,"

I thank the Chief of Naval Research, Rear Admiral Jay Cohen, for inviting me to speak today. In his invitation the Admiral asked that I "provide a framework for the scientific solutions necessary to win the global war on terrorism" and discuss recent initiatives to achieve those solutions. This is a welcome task because it gives me an opportunity to reflect on the larger picture that links science, its applications, and the unprecedented quality of the war on terrorism.

That terrorism should be regarded as a cause of war is already a sign of something new. Throughout the history of human conflict terrorism has been a means to demoralize the enemy. It has been used in the past (but infrequently) by state supported armed forces as one component in a broader array of aggressive measures. More often terrorism has been the tool of otherwise relatively powerless individuals or guerilla organizations for whom it may be the only affordable potentially effective tactic. Until recent decades, however, it would have been difficult to make the case that terrorism was strategically important.

One development that has magnified the importance of terrorism is the spread of technologies that enhance the power of individual action. Strategically significant force had always been so expensive as to be the exclusive province of states. The cost of horses and cannon, ships and transport, equipment and supplies for large numbers of war-fighters has impoverished many nations who aspired to conquest. Even as warfare became more technical, diminishing the ratio of manpower to effective force, the added cost of new military technology tended to balance or even outweigh the savings in reduced numbers of combat personnel. This trend culminated in the Cold War, whose outcome was determined not on the battlefield but by the economic capacity of the contending powers to deploy the most powerful and sophisticated technology.

As the Cold War progressed, so too did a linked set of technologies that had broad civilian as well as military application. The most transformational of these, to use a current buzzword, we call *information technologies*, but that is more descriptive of their end use than of their basis in materials, electronics and optical sciences, and computer science. Initially the information applications had the greatest impact on military and commercial operations, but by the time the Soviet Union collapsed in the early 1990's, information technology had begun to influence the way of life for the general public throughout the world. The widespread dissemination of inexpensive but powerful means of communication and information processing is fueling a global revolution that is transforming economies, business models, and life-styles at an unprecedented rate.

It is this change in the information environment, more than anything else, that has elevated terrorism from a tactical to a strategic level. From the recruitment and training of terrorists to the implementation of coordinated acts of terrorism, information technology is a major force multiplier of relatively small low-tech operations. This is the paradox of terrorism: the actual materials and techniques deployed are inexpensive and widely available to the international public. Modern terrorism, like modern economies, is driven by knowledge and information. It exploits readily available technology to achieve its objectives. As the technical infrastructure of society becomes more sophisticated, coordinated incidents of terrorism grow more powerful. This is the challenge of modern terrorism, and it is a serious one.

This thirty-thousand foot view suggests several dimensions along which new weapons for the war against terrorism must be developed. I am going to focus on three dimensions. First of all is the *nature of the aggressor*. While states may aid and abet terrorism either deliberately or inadvertently, the agents of terrorism are not in general state-sponsored personnel. They tend to be widely dispersed volunteers attracted to the cause by a variety of social and psychological forces, focused by an ideological framework to justify violence against innocent people. Are there more potential terrorists today than in the past? I do not know, but I do know that conditions today are much better for translating that potential into action. Discovering how and why individuals become mentally committed to terrorism ranks high among science priorities for combating terrorism. Inhibiting the diabolical machinery at its source is the highest leverage action we can take to reduce the terrorist threat. Another high priority is deepening our understanding of how recruiting, training, and implementation activities are financed, and what motivates donors to fund these activities. Many observers have concluded that the social sciences have much to offer here, so let me say a word about these fields.

I agree that social science research is likely to be important in combating terrorism, but much work is needed to translate research products into practical applications. Researchers need to be fluent in the culture of the people whose behavior they are studying, and this limits the scope of effort to societies familiar to the community of social scientists. In the long run, we need more scientists with language and culture skills in the terrorists' countries of origin. We also need "applied social scientists" who can work in teams with law enforcement officials, and operational personnel to develop strategy and tactics for specific regional campaigns to combat terrorism. Earlier this year the Department of Homeland Security established a Center of Excellence for Behavioral and Social Research on Terrorism and Counter-Terrorism at the University of Maryland, partnering with five other universities. The Center will look not only at the causes of terrorism and strategies to counter terrorism, but will also examine the psychological impact of terrorism on society, and strengthening the population’s resilience in the face of the terrorism. This is a commendable response to a priority need, and deserves support.

Information technology is the second important dimension of the new terrorism. The Internet, cell phones, and wireless technology have all played enabling roles for terrorism. The other side of this coin is they are also sources of information that can be

mined for patterns of terrorist activity, and exploited for counter-terrorist tactics. As the main technology enabling the new terrorism, information technology should receive the highest priority for both long term and short term attention. Given the rapid advance of inexpensive commercially available information technology, the strategy here must be to develop military capabilities far beyond the publicly available state of the art. I do not know any way of doing this within the existing technology mainstream driving Moore's law. Commercial interests are pushing this technology as fast as it can go, and there is little chance a special government sponsored initiative will get ahead of it following the same route. In my opinion, only developments *outside* this mainstream can lead to significant leapfrogging capabilities. And that means major investment in certain areas of basic science.

Let me give you an example of what I mean by a leapfrogging technology. Laser light made its first appearance in 1960. Within months the Army's Redstone Arsenal had a laser-guided weapons program. The Air Force joined the effort in 1964. The first laser-guided bomb was demonstrated successfully in 1966, and was deployed effectively in Vietnam. Where did the laser come from? Key ideas started with Charles Townes who had worked on wartime radar concepts at Bell Labs during World War II. He and co-workers invented the maser there in an effort to improve molecular spectroscopy. Townes left Bell Labs in 1948 to work at Columbia University because, in his words: "I left to go to Columbia partly because Columbia was more interested in the physics and the principles which I was interested in. And furthermore I liked university life much better anyhow -- I really always wanted to be in a university." His work was funded by the Office of Naval Research, the Army Research Office, and the Air Force Office of Scientific Research under the Joint Services Electronics Program established in 1948. That first laser in 1960 was built at Hughes Research Lab in California. So we have an extended interaction between defense agencies, universities, and industrial laboratories in two different sectors, communications and aerospace. The laser grew out of an interest in basic science, but it occurred in an environment where the actors were aware of national security applications, so when the breakthrough occurred it was immediately recognized and followed up. Much of the early laser work was done by graduate students in groups at Columbia and MIT who received their funding from various sources.

I mention this case study because categories of physical phenomena exist that are known today to be likely to lead to entirely new applications in information technology. These phenomena are not receiving the attention they deserve from the defense agencies that have the most to gain from them, and the most to lose from delays in developing their implications. Of particular interest are the quantum coherence phenomena that previously were inaccessible to us for practical applications, but which the same new technologies responsible for the information revolution are now bringing into view. These phenomena occur in a wide variety of physical systems, and it is not yet clear which ones will provide the foundation for the leap in information technology. Probably there will be several very different physical platforms, but the computer science can be worked out ahead of time for many platforms, and this is research that urgently needs to be done. Equally urgent, of course, is the systematic exploration of the various schemes for scaling up quantum coherence effects into viable foundations for new information technologies. The physical phenomena I am talking about are spintronics, quantum dots, Josephson junctions, photonics, Bose-Einstein condensates, single atom or molecule and

single photon systems, and a variety of phenomena in what has come to be called nanotechnology.

This work is being funded by several different agencies, including DOD, DOE, NSF, and NIST, but the logical source of support for the basic science is DOD. Legitimate questions have been raised about the adequacy of this support. Just a few months ago the Defense Science Board observed that "DOD now is no longer perceived as being seriously involved in – or even taking steps to ensure that others are conducting – research to enable the embedded processing proficiency on which its strategic advantage depends. This withdrawal has created a vacuum where no part of the U.S. government is able to exert leadership, especially with respect to the revolutionary component of the research portfolio." The comment specifically refers to high performance microchip concepts, a mainstream information technology component, but it applies to the fields I mentioned above.

The information technology industry has also been vocal in its call for greater attention to these areas. Such attention is warranted not only to ensure continued economic competitiveness in this sector, but for clear national security reasons as well. Critics link the problem to inadequate funding. I believe the root problem is inadequate attention in DOD's own planning and prioritization process, and I know defense agencies are looking at this issue. I will say more in a moment about White House priorities in these areas.

The third important dimension of the new terrorism is the *widely dispersed and complex nature of the battlefield*. Terrorism is directed against unsuspecting personnel, military or civilian, at random times and locations. Intelligence and understanding of motives and enemy capabilities are not enough to prevent attacks. The situation calls for widely dispersed and highly capable sensor systems, and rapidly deployable means for mitigation and response to large and diverse populations. Terrorist methods and materials have physical characteristics that may provide clues to their existence. We need to identify these and develop appropriate detectors. The state of science today offers numerous options for physical detection schemes, and we can expect vendors to respond effectively to clear procurement specifications, whether for applied research or for products. The greater problem is not producing the devices, but to integrate detector arrays and systems with intelligence and the insights of the social sciences. System design must go hand in hand with detector development, but for the most part the needed science is mature. To exploit it we need to support targeted applied research and development.

This is the dimension where the threat of Improvised Explosive Devices looms large. The Navy deserves credit for flagging IED's as a target for fundamental research, and supporting a strong R&D effort. Detecting IED's is not simply a matter of remote sensing of explosives or material signatures, but also one of identifying and recognizing signatures of human intent. Here again the social and behavioral sciences intersect with devices and system engineering.

I mentioned the Homeland Security Center of Excellence in Behavioral and Social Research on Terrorism and Counter-Terrorism. DHS has also created a Center for

Risk and Economic Analysis of Terrorism Events at the University of Southern California (USC), a Center for Foreign Animal Disease and Zoonotic Disease Defense at Texas A&M, a Center for Food Protection and Defense at the University of Minnesota, and is planning two others, one jointly with EPA on microbial risk assessment, and the other on high consequence event preparedness and response. Each of these Centers has multiple partners with other universities, laboratories, and corporations. They are typically funded for three years at levels currently ranging from $12 to $18 million. These are excellent examples of a research model reminiscent of DOD's Joint Services Electronics Program that laid the foundations for breakthrough technologies more than four decades ago. Other successful partnership models exist, particularly the DOD University Affiliated Research Centers program (UARC's). Many other agencies support science and technology R&D programs related to the needs of the war against terrorism, but the need for additional investments in long lead time, high risk research in the physical sciences remains great.

Let me close with some information about the White House role in coordinating interagency R&D efforts. Each year my office produces a guidance memo in cooperation with the Office of Management and Budget for agencies sponsoring research and development that outlines priorities for the forthcoming Presidential Budget Proposal to Congress. This guidance is based on input from the policy level committees OSTP operates under the umbrella of the interagency National Science and Technology Council. Under the Homeland Security interagency R&D priority, the current guidance document for Fiscal Year 2007 states that

"Agencies should place increased emphasis on R&D efforts that support: quick and cost-effective decontamination capabilities following a biological, chemical, nuclear or radiological incident; predictive modeling to assess the rate of geographic spread of emerging and/or intentionally released infectious diseases; enhanced biometric systems; secure land and maritime borders through more reliable technologies for screening cargo and visitors; increased effectiveness of existing security systems through automation; improved understanding of the social and cultural dynamics of regional population groups; safety of the Nation’s food supply and agricultural systems; and social and behavioral research to anticipate, counter and diffuse threats to our homeland security and enhance response and recovery capabilities. As we continue the rapid development of near-term technologies, we also need to enhance fundamental studies that may lead to transformational concepts for solving truly difficult challenges including the remote detection of nuclear material and/or devices and the remote detection and/or disabling of explosive devices ranging from suicide vests to vehicle-borne bombs."

The memo also has a physical science priority that states, in part that "Investments in the physical sciences likely to lead to or enable new discoveries about nature or strengthen national economic competitiveness continue to be important. Priority will be given to research, instrumentation and facilities that aim to close significant gaps in the fundamental physical understanding of phenomena that promise significant new technologies with broad societal impact." The physical science priority is also clearly linked to national security for the reasons I have given.

The OMB/OSTP memo continues to give priority to the ongoing National Information Technology R&D program currently at about $2 billion, and the National Nanotechnology Initiative funded at about $1 billion annually. Funding for these programs depends upon the commitment that participating agencies have to them, and program priorities are established through an interagency process that includes the Department of Defense agencies. Program coordination is provided by offices with staff drawn from the agencies. Much more detail is available on the websites for these initiatives.

These brief remarks cover a lot of territory, but I have tried to show that the science and technology needs of the war against terrorism cover the entire spectrum from fundamental research to narrowly specific applications. It is a broad spectrum, but within it priorities are relatively easy to identify. The Department of Homeland Security is preparing a strategic plan for homeland security science and technology with substantial interagency participation. This plan will provide a more articulated framework for the many diverse tasks needed to execute the war against terrorism with the greatest possible effectiveness.

From my perspective, the struggle against terrorism requires new knowledge and new technology in the three areas I mentioned that could be summarized as: human behavior, information technology, and devices and systems. We have substantial knowledge bases relevant to each area, and the likelihood of breakthroughs in strategically important technologies. Exploiting these opportunities to give our defense personnel the upper hand in combating terrorism requires close cooperation among all the agents and institutions in which expertise resides, including government, universities, and industry. I commend the Office of Naval Research for sponsoring this conference, and am grateful for this opportunity to participate.

Thank you.