

**FOR OFFICIAL USE ONLY
UNTIL RELEASED BY THE HOUSE ARMED SERVICES COMMITTEE**

**STATEMENT OF
MR. JEAN D. REED
DISTINGUISHED RESEARCH FELLOW
CENTER FOR TECHNOLOGY AND NATIONAL SECURITY POLICY
NATIONAL DEFENSE UNIVERSITY**

BEFORE THE

**EMERGING THREATS AND CAPABILITIES SUBCOMMITTEE
COMMITTEE ON THE ARMED SERVICES
UNITED STATES HOUSE OF REPRESENTATIVES**

ON

**DEPARTMENT OF DEFENSE INVESTMENT IN TECHNOLOGY AND
CAPABILITY TO MEET EMERGING SECURITY THREATS**

24 July 2011

**FOR OFFICIAL USE ONLY
UNTIL RELEASED BY THE HOUSE ARMED SERVICES COMMITTEE**

Introduction

Mr. Chairman and members of the sub-committee, it is an honor to be here today to speak to you about some of the potential emerging and future security threats and challenges facing the United States and the Department of Defense.

I am Jean Reed. I'm a distinguished research fellow at the National Defense University's Center for Technology and National Security Policy, one of the core strategic research centers of the University's Institute for National Strategic Studies where I focus on chemical and biological defense and related policy and program issues. I am also a senior fellow at the Potomac Institute for Policy Studies.

National Defense University (NDU) is the Department of Defense's pre-eminent academic institution for education, research, and outreach in national and international security. As the nation's senior institution for Professional Military Education, NDU prepares military and civilian leaders from the United States and other countries to think strategically and lead effectively across the range of national and international security challenges faced by this nation today and in the future. It performs research and develops issues in support of the national security strategy and national military strategy development needs of the Secretary of Defense, the Chairman of the Joint Chiefs of Staff, and the combatant commanders; and conducts outreach across the U.S. interagency community and internationally. The eight NDU research centers specialize in understanding the emerging strategic situation and the development of creative policy options for how the United States' might respond to the challenging, complex, multi-polar international environment that we face today and anticipate the challenges the Nation might face in the future. Having the advantage of being in-house and close to the

policy process while retaining its academic freedom and integrity, the NDU research team is poised to contribute fully to meeting the needs of the Department and the Nation. It is in that spirit that I appear before you today.

My remarks today will focus on future threats that I see and general trends with regards to areas of emphasis. They reflect my own views and are not necessarily those of the National Defense University, the Department of Defense, or any other organizations with which I am affiliated.

Thinking About Emerging and Future Threats and Challenges

A common theme in statements of the U.S. national defense strategy over the last several years recognizes that “increasingly, the Department of Defense will have to plan for a future security environment shaped by interaction of powerful strategic trends.” Over the next 20 years, the confluence of trends with rapid social, cultural, technological and geopolitical change will present greater uncertainty. “This uncertainty is exacerbated by both the unprecedented speed and scale of change, as well as by the unpredictable and complex interactions among the trends themselves.”

Defense policy must account for uncertainty by acting to reduce risk and by developing the capacity to hedge against it. Institutional agility, flexibility and resilience are key to dealing with uncertainty and the potential for strategic surprise.

Throughout history, planners have had a tendency to consider future threats within the context of what they knew about the current threat. The natural approach has been to focus on trend projections – predictable paths along which events are expected to evolve. Thinking about science and technology has been similarly linear and

compartmentalized, with projections within any scientific discipline being based on past progress. As a result, strategists and planners have been repeatedly surprised by the application of new technology to warfare, whether actual or economic, by the advantages conferred by the unique combinations of different technologies, and by the non-linear, often exponential, advances in science and technology.

Examples abound. Billy Mitchell demonstrated the vulnerability of battleships to bombs dropped from airplanes, yet the use of air power was largely ignored by the world's navies. The combination of aircraft, highly mobile armor and communications – known as *blitzkrieg* – took the Allied armies by surprise. More recently, use of precision guided munitions, armed drone aircraft and satellite global positioning has changed the complexion of today's battlefield. Advantages can be gained by ingenious use of low technology as well, such as delivering biological agents via the postal service, flying passenger planes into buildings or improvising roadside bombs.

Within the context of the Cold War, planners on both sides had a degree of confidence in the technological capabilities of their counterparts. Science, for its part, was highly “disciplinary” and progress was largely made in incremental fashion within a given discipline, allowing for reasonably accurate planning and the ability to integrate new advances into weapons platforms and defensive systems. Three things have changed all that. First, the bipartite, U.S. vs. U.S.S.R polarity vanished with the demise of the Soviet Union, and has been replaced by new transnational adversaries. Second, science underwent a dramatic paradigm shift in which trans-disciplinary research, with its ability to affect exponential advances within disciplines and, in fact, create entirely new disciplines, became the norm. Third, information has become ubiquitous, allowing individuals access to technology on an unprecedented scale. The world, in short, is a

much more unpredictable and chaotic place, and the emerging threats are equally problematic:

Current Department of Defense (DOD) programs are primarily threat driven, with knowledge of the potential threats being based both on intelligence and a technical assessment of the art of the possible in science. The spectrum of emerging threats has been enlarged by both the exponential advances in scientific knowledge, and its availability to a broader range of potential bad actors that no longer need to have advanced scientific training. Deciphering this threat spectrum will require a robust investment in science and technology, particularly in its evolving trans-disciplinary paradigm.

The concept of technological convergence is critical to understanding future threats, as there are some scientific disciplines which will be radically shaped by their convergence with other areas. The disciplines of nanotechnology, biotechnology, information technology and cognitive neuroscience, collectively known by the acronym “NBIC”, are four areas which will be pivotal in anticipating and countering future threats, and NBIC Convergence is an apt metaphor for the paradigm shift in science described earlier. The classic example of NBIC Convergence was the convergence of genomics and information technology, which led to the elucidation of the human genome and which will be the basis for personalized medicine, but the flip side is the ability to manipulate the genomes of pathogenic organisms to create entirely new biological threat agents not found in nature. The ability to predict and plan for such optimal technological convergences will largely determine the technological leaders of the 21st century.

Nanotechnology has been much in the news as well as in popular culture, but is largely misunderstood. Scientists have been conducting work in nanotechnology for at

least three centuries, that is, as long as there has been a discipline called chemistry. The difference now is the ability to manipulate materials on the atomic scale, and to therefore create miniature devices too small to be seen by the naked eye. Such devices could have promising medical applications, such as creating artificial organs or repairing small structures within the body; they could be incorporated into materials and coatings to decontaminate environmental pollutants; or, they could be designed to kill people, disable equipment or have a deleterious effect on the environment. Further, materials which are benign when manufactured at the macro scale can have unpredictable and/or toxic properties when manufactured at the nano-scale, implying an entirely new spectrum of potential threats.

Biotechnology has been largely focused on medicine, but is increasingly finding applications in materials science, alternative energy, agriculture and industrial manufacturing. The tools of biotechnology are ubiquitous and available to anyone in the world. While the Human Genome Project will be the underpinnings for the development of new therapeutic drugs, the “dark side” of biotechnology is its ability to manipulate life, to create new life forms, and to imbue them with pathogenic characteristics. Beyond classical biotechnology, the new field of synthetic biology will be the next revolution in the biological sciences. Synthetic biology is currently in a nascent stage in which genes from one organism are used to create new metabolic pathways in another organism. Used properly, synthetic biology offers the promise of greatly enhanced manufacturing processes for high value biological products such as vaccines. Alternatively, synthetic biology could be used to create entirely novel synthetic systems which have some of the characteristics of living systems, but which are tailored to possess characteristics which would make them a threat to people, agriculture or materials.

With the evolution of the internet, information technology has brought technology to the masses in a very efficient manner. The dependence of the economy on information which has high fidelity and is uncorrupted cannot be exaggerated, and the constant cyber attacks by hackers, whether individual or state sponsored, has both economic and military significance.

Finally, within the concept of NBIC, cognitive neuroscience is probably the least mature but most rapidly advancing discipline. The ability to fully image the brain will dramatically increase our understanding of cognitive function, and will facilitate the development of therapeutic approaches to mental disease. There is also the potential to degrade cognitive function, interfere with decision making, and inhibit performance of the civilian and military populations.

The exponential advances in scientific knowledge, its broader range of availability, and technological convergence for the paradigm shift in science could yield capability outcomes for the good, or that could be a future threat, as noted in my comment about NBIC Convergence. The ability to predict and plan for such an outcome is the question.

Some of my colleagues at NDU suggest navigating through this increasingly complex environment using “foresight” — a structured effort to think about potential security challenges from several –to-many years in the future. Foresight is not about making predictions, but is meant to help decision-makers under conditions of uncertainty by conceiving and testing options and exploring consequences. Foresight helps us think about what we don’t know by examining alternative futures. NDU and the Department of State have been running a project exploring the idea of “Actionable Foresight”— the

disciplined analysis of alternative futures that would provide decision makers with the understanding needed to better influence the future environment. Some of the key findings of this project highlight the need to use foresight to identify alternative possibilities in an increasingly complex, interconnected global security environment. Both consumers and producers of foresight need to recognize the speculative nature of foresight as opposed to evidence based recommendations. The interface between foresight and policy should occur regularly and be linked to ongoing decision making processes. Informal, persistent and diverse networks of foresight should include the whole of government and society. Foresight should be linked to current events in order to gain the attention of the policy maker. A venue or central hub is needed for facilitating and coordinating foresight. Finally, foresight should be used to identify opportunities (preventive and responsive) to inform policy makers of actions that would help achieve specific goals.

Another NDU effort, “Anticipatory Governance,” would make foresight a component of the policy process; using networked systems to support whole-of-government responsiveness, applying feedback systems to monitor performance and speed up learning from the results. The guiding premise of each of these NDU initiatives is that the United States is confronted by a new class of complex, fast moving, cross-cutting challenges that simultaneously engage our social, economic, and political systems and that challenge our traditional boundaries of national security. Foresight, as a structured effort to think about evolving trends and future possibilities, can inform decision making related to threat prevention, preparedness, and response management.

Conclusion – Anticipating and Responding to the Threat

I believe that the DOD has recognized the changes in the threat landscape and understands the paradigm shifts which have changed both the way science is conducted, and also its potential to generate new threats. There is also a clear awareness that the DOD needs to continually invest in its laboratory infrastructure in order to stay abreast of exponentially increasing scientific advances and, perhaps more importantly, to invest in training the next generations of scientists and engineers. There is also a science-driven emphasis on strategic research investment planning with a focus on key, emerging scientific areas with disruptive potential.

While it is virtually impossible to predict *a priori* what the future threats will be, maintaining clear scientific superiority with a strategic investment based on technology convergence offers the best chance to drive and exploit scientific advances, and to anticipate and respond to new threats based on these technological advances. In addition, foresight, as a disciplined analysis of alternative futures may help us make sense of emerging trends and threats, and better anticipate the future.

Finally, if I may be allowed to add a philosophical caveat, the uncertainty and disruption caused by the context of accelerating changes puts a greater emphasis than ever on our core values. As time goes on, there will be less and less time to think through the larger implications of our vision for the future; so it is increasingly important that we articulate with clarity and precision, exactly what principles we believe should govern our policies as they develop and adapt. The more quick, flexible, and agile our movements, the more important it is that we keep track of where we are and where we want to go.

Mr. Chairman, this completes my prepared remarks and I will be happy to answer your questions.