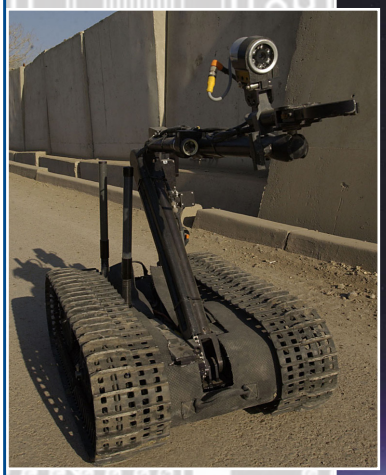
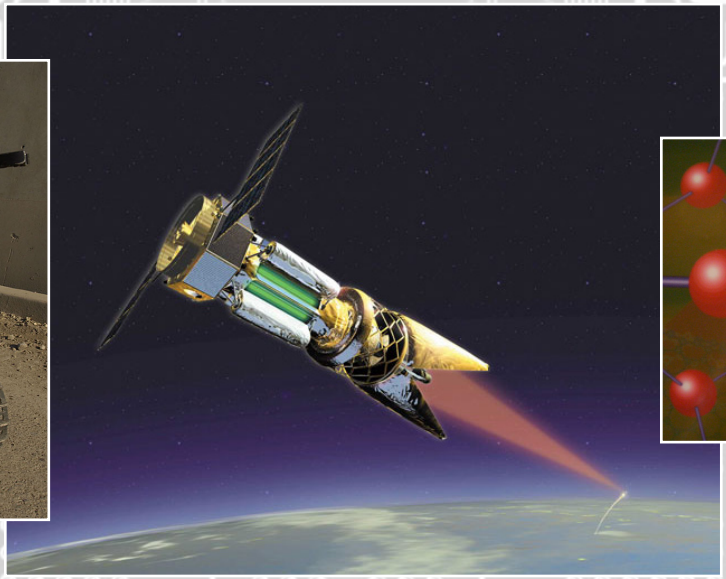
Heritage Special Report

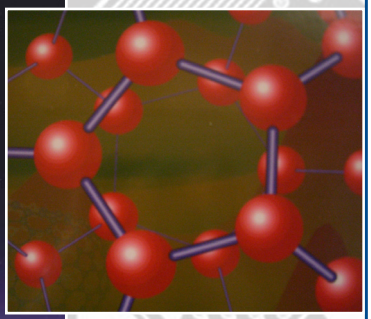
SR-21
February 29, 2008

Published by The Heritage Foundation

Competitive Technologies for National Security:







Review and Recommendations

By James Jay Carafano, Ph.D., Andrew Gudgel, and Alane Kochems

The Heritage Foundation
LEADERSHIP FOR AMERICA

214 Massachusetts Avenue, NE | Washington, DC 20002 | (202) 546-4400 | heritage.org

Competitive Technologies for National Security

Review and Recommendations

By James Jay Carafano, Ph.D., Andrew Gudgel, and Alane Kochems

Contributors

James Jay Carafano, Ph.D., is Assistant Director of the Kathryn and Shelby Cullom Davis Institute for International Studies and Senior Research Fellow for National Security and Homeland Security in the Douglas and Sarah Allison Center for Foreign Policy Studies at The Heritage Foundation.

Andrew Gudgel, a former Army Warrant Officer, is currently a freelance science writer living in Maryland.

Alane Kochems is a former Policy Analyst for National Security in the Douglas and Sarah Allison Center for Foreign Policy Studies, a division of the Kathryn and Shelby Cullom Davis Institute for International Studies, at The Heritage Foundation.

214 Massachusetts Avenue, NE
Washington, DC 20002–4999
(202) 546-4400 • heritage.org

This paper, in its entirety, can be found at:
www.heritage.org/Research/NationalSecurity/sr21.cfm

Contents

Introduction

Technology does not win wars or make nations safe. The search for security is shaped by larger cultural, economic, and political factors and strategic choices. On the other hand, technology has always been the handmaiden of national security. Nations always look for innovations that can offer them competitive advantages over their adversaries. Innovation will always be a national security "wild card." New technologies may unleash or accelerate social and cultural changes that affect how nations protect themselves on battlefields and behind the scenes.

Over the course of the 20th century, America's genius was its capacity to ride above the wave of technological change. That may not be the case in the future. American prowess is at risk. Congress will have to play an active role in ensuring that the United States does not lose its competitive edge.

In 2006, The Heritage Foundation organized a series of workshops to examine emerging technologies that have significant implications for national security. These technologies include nanotechnology, biotechnology, advanced computing, directed energy, and robotics.

This report reflects the results of these workshops and additional research by Heritage scholars exploring the current and future uses of these innovations, as well as what policy, guidelines, and programs Congress and the Administration should undertake to ensure that the United States remains at the forefront of cutting-edge technological development. Among the key recommendations of this report are that Congress should:

- **Establish** a legislative framework that encourages the development of emerging technologies; the promotion of research, innovation, and investment; and the protection of U.S. citizens. Congress should address litigation and civil liberties protection and environmental and public health standards. It should, for example, consider expanding the scope of the SAFETY Act, which provides liability protection for the development and deployment of homeland security and counterterrorism equipment and services, to cover innovations that support other national security missions. Congress should also prompt the Administration to work with other countries to adopt similar legislation that will facilitate deploying technologies developed in the U.S. to support national security missions overseas.
- **Implement** visa issuance and management reforms to ensure that the best and the brightest continue to study and work within the competitive technology fields in the United States. Congress should, for example, significantly expand the H1B visa program, end the requirement for 100 percent interviews for visa applications, and reform and expand the Visa Waiver Program.
- **Ensure** that federal agencies efficiently and effectively fund research and development on the emerging technologies with significant national security implications, particularly those that are not being developed aggressively by the private sector, including nanotechnology and directed energy.
- **Encourage** more interdisciplinary approaches to research that combine disparate scientific disciplines in both the basic and applied sciences, some creating new methods of investigation, such as "network" science, which combines studying physical, biological, and social phenomena to understand how complex networks operate.

The Past Is a Poor Prologue

Congress can ill afford to neglect science and technology policy. It can no longer assume that the United States will maintain a decisive technological edge over its global competitors. The world has changed.

At the outset of the Cold War in 1947, America stood as the undisputed world leader in science and technology. The nation's scientists, bolstered by colleagues that had fled from war-torn Europe, provided an unparalleled pool of knowledge with access to vast government resources. As a result, the nation's leaders could rely on the best and brightest for innovation and creativity to maintain the United States' technological edge. At the same time, govern-

ment-sponsored research fueled by a decades-long competition with the Soviet Union funded many of the premier technological innovations of the age.

The 21st century is very different. The best and the brightest are not located exclusively in the United States, and the United States is not necessarily the preferred destination for foreign scientists. Countries throughout Europe and Asia have recognized the importance of cutting-edge technologies, both in terms of economic growth and in terms of military capabilities, and have devoted enormous resources to their development. Consequently, not only is the United States seeing its scientific lead shrink, but it is also experiencing difficulty in attracting and retaining the talent necessary to produce next-generation technologies.

Another major change is that the federal government is no longer the principal player in the research and development that shapes the character of the modern era. Private-sector innovations in biotechnology and information systems dwarf government research. These emerging industries are creating products that science-fiction writers never even imagined, with dual-use capabilities that could potentially transform the fields of homeland security and defense. In many cases, national security innovation will come from adapting commercial off-the-shelf technology.

Still another significant difference from Cold War competition with the Soviet Union is that many of America's enemies today seek to avoid America's technical prowess, fighting space-age weapons with ancient tactics like kidnapping, guerilla warfare, and suicide bombers. The technological advantages of the Cold War era have proven ill-suited to these challenges.

Emerging technologies will have a dramatic impact on the future of our security. In the short term, these technologies will provide capabilities that include protection and possible immunity against biological agents, better screening at airports and ports, more efficient information-gathering and information-sharing techniques, and better armor for our troops. In the long term, the sky is the limit. These fields will be at the center of scientific advances for years to come and perhaps will redefine not only our national security capabilities, but also how we conduct our daily lives.

Dialogue, Not Monologue

Competitive Technologies for National Security: Review and Recommendations represents the beginning, not the end, of The Heritage Foundation's research on the challenges of adapting emerging capabilities for national security. Facing the future will require finding the right answers to some tough questions:

- How will the United States attract the best and the brightest to work and study here?
- How will the United States maintain access to the global research and technological base?
- How will the United States share innovations and collaborate with its friends and allies?
- How will the United States counter emerging national security threats and prevent its enemies from exploiting new technologies?
- How will the United States educate, train, and retain a quality workforce that can meet its national security needs?
- How will the U.S. government be able to identify and exploit cutting-edge technologies that are being developed in the private sector?

These are timeless questions, but the 21st century they will require new answers—answers that will help to keep America safe, free, and prosperous.

—James Jay Carafano, Ph.D.
Assistant Director,
Kathryn and Shelby Cullom Davis Institute for International Studies,
and Senior Research Fellow for National Security and Homeland Security,
Douglas and Sarah Allison Center for Foreign Policy Studies
The Heritage Foundation
Washington, D.C.

Chapter 1

The Viability of Directed-Energy Weapons

Alane Kochems and Andrew Gudgel

When directed-energy weapons are mentioned, most people think of "death rays" or Hollywood's latest science fiction movie. However, directed-energy weapons (DEWs) are a reality, and several have already been tested under battlefield conditions.[1] They may begin to appear on the battlefield within the next decade, bringing a revolution in weapons and how war is waged.

While DEWs are not the solution to all combat situations, these technologies would provide the U.S. military with additional flexibility in tailoring its response to different types of threats. However, considerable work still needs to be done before they can be deployed. These technologies need the full support of the armed services, and the Department of Defense (DOD) needs to generate clear guidelines for their use.

The Pentagon believes that DEWs are legal under international law, but human rights groups are arguing that DEWs could be used inhumanely. Putting the proper protocols in place should mitigate these concerns. While DEWs are not a panacea, the armed services should fully support research and development of these useful technologies.

Weapons Revolutions

From the Stone Age until the Middle Ages, a weapon's power was limited by the strength of the man wielding it or, in the case of bows, by the strength of the material from which it was made. In the late Middle Ages, a revolution in weaponry occurred when chemical-powered (gunpowder) weapons began to replace swords and bows. This revolution changed the nature of warfare: not just tactics, but also the usefulness of armor, castles, and then-popular weapons.

Since the invention of gunpowder, a weapon's effectiveness has no longer depended on the wielder's strength, but on the chemical energy of the propellant or explosive. While centuries of technological advances have improved the power of these materials, the basic operating principle of chemical-powered weapons ultimately remains the same. Modern battlefield weapons are the descendents of muskets and cannon.

Another revolution in weaponry is currently underway, with directed-energy weapons on the cusp of replacing chemical-powered weapons on the battlefield. DEWs use the electromagnetic spectrum (light and radio energy) to attack pinpoint targets at the speed of light. They are well suited to defending against threats such as missiles and artillery shells, which DEWs can shoot down in mid-flight. In addition, controllers can vary the strength of the energy put on a target, unlike a bullet or exploding bomb, allowing for nonlethal uses.

The Beginning of Directed-Energy Weapons

Both the Allies and the Axis powers conducted basic research and studies into primitive directed-energy weapons before World War II. However, British scientists calculated that the electronic systems of the time

1. On August 24, 2004, the Tactical High Energy Laser (THEL) system destroyed a salvo of mortar rounds in midair during a test. "Mobile/Tactical High Energy Laser (M-THEL) Technology Demonstration Program," *Defense Update*, at *www.defense-update.com/directory/THEL.htm* (March 10, 2006).

could not generate the power necessary for a "death ray," and research was redirected into early radar detection systems.[2]

During the Cold War, the U.S. and the Soviet Union studied the possibility of creating particle-beam weapons, which fire streams of electrons, protons, neutrons, or even neutral hydrogen atoms. The kinetic energy imparted by a particle stream destroys the target by heating the target's atoms to the point that the material literally explodes. These weapons were considered for both land and space-based systems. However, because beam strength degrades rapidly as the particles react with the atoms in the atmosphere, it requires an enormous power plant to generate a weapons-grade beam. The countries abandoned particle-beam weapon research as impracticable.[3]

How Lasers Work

Albert Einstein described the theoretical underpinnings of lasers in 1917. However, the first working laser was not built until 1960, opening an entirely new avenue of directed-energy research. Lasers produce narrow, single-frequency (i.e., single-color), coherent beams of light that are much more powerful than ordinary light sources.

Laser light can be produced by a number of different methods, ranging from rods of chemically doped glass to energetic chemical reactions to semiconductors. One of the most promising laser devices is the free-electron laser. This laser uses rings of magnetically confined electrons whirling at the speed of light to produce laser beams that can be tuned up and down the electromagnetic spectrum from microwaves to ultraviolet light.[4]

Lasers produce either continuous beams or short, intense pulses of light in every spectrum from infrared to ultraviolet. X-ray lasers may be possible in the not too distant future. The power output necessary for a weapons-grade laser ranges from 10 kilowatts to 1 megawatt. When a laser beam strikes a target, the energy from the photons in the beam heats the target to the point of combustion or melting. Because the laser energy travels at the speed of light, lasers are particularly well suited for use against moving targets such as rockets, missiles, and artillery projectiles.

One problem that affects laser beam strength is a phenomenon known as "blooming," which occurs when the laser beam heats the atmosphere through which it is passing, turning the air into plasma. This causes the beam to lose focus, dissipating its power. However, a variety of optical methods can be used to correct for blooming. Laser beams also lose energy through absorption or scattering if fired through dust, smoke, or rain.

The number of "shots" a laser weapon can produce is limited only by its power supply. Depending on the type of laser, this means that the weapon can have an almost "endless magazine" of laser bursts. In addition, a laser shot (including the cost of producing the energy) is much cheaper than a shot from a chemical-powered weapon system. For example, when deployed, the anti–ballistic missile Airborne Laser will cost approximately $1,000 per shot,[5] while each Patriot missile currently costs $2 million to $3 million.[6]

Current Laser Technology

Because they were invented several decades ago, lasers are the most mature of the DEW technologies. Laser dazzlers—devices that use laser light to temporarily blind sensors, optics, and personnel—are already available for law enforcement and military use. In 1995, the Chinese military marketed the ZM-87 laser interference device, a tripod-

2. David E. Fisher, *A Race on the Edge of Time: Radar—The Decisive Weapon of WWII* (New York: McGraw-Hill, 1988), pp. 15–31.
3. Richard M. Roberds, Ph.D., "Introducing the Particle-Beam Weapon," *Air University Review*, July–August 1984, at *www.airpower.maxwell.af.mil/airchronicles/aureview/1984/jul-aug/roberds.html* (March 15, 2006).
4. *Encyclopedia Britannica*, 15th ed., s.v. "laser."
5. Suzann Chapman, "The Airborne Laser," *Air Force Magazine*, Vol. 79, No. 1 (January 1996), at *www.afa.org/magazine/jan1996/0196airbo.asp* (March 15, 2006).
6. GlobalSecurity.org, "Patriot Advanced Capability–3 (PAC-3)," at *www.globalsecurity.org/space/systems/patriot-ac-3.htm* (March 15, 2006).

mounted battlefield laser dazzler designed to blind enemy soldiers and optics temporarily. In March 2003, North Korea may have used a ZM-87 to "paint" two U.S. Apache helicopters patrolling the Demilitarized Zone.[7]

The two U.S. laser weapons systems closest to actual deployment are the Tactical High-Energy Laser (THEL) and the Airborne Laser (ABL).

Development of the THEL began in 1996 as a joint program between the United States and Israel to develop a laser system capable of shooting down Katyusha rockets, artillery, and mortar shells. The THEL system uses radar to detect and track incoming targets. This information is then transferred to an optical tracking system, which refines the target tracking and positions the beam director. The deuterium fluoride chemical laser fires, hitting the rocket or shell and causing it to explode far short of its intended target.[8]

In August 2004, the THEL system shot down multiple mortar rounds during testing. However, the Army felt the fixed-base laser system was too large and cut funding for the program after the demonstration phase. Research was also conducted on a mobile version of the THEL called the MTEL.[9]

The ABL is a system that uses a megawatt chemical laser mounted on a modified Boeing 747 to shoot down theater ballistic missiles. The system consists of several modules: an infrared detection system to detect the missile's launch; the Tracking Illumination Laser (TILL); the Beacon Illuminator Laser (BILL); and the Chemical Oxygen Iodine Laser (COIL).[10]

Once tracked by the TILL, the BILL measures the atmospheric distortion between the COIL and the missile. These data are then passed on to the mirror system, which makes appropriate corrections so that, when the COIL fires, maximum energy is transmitted to the target. The skin of the missile heats up, melts, and deforms, and the target breaks up in midair.[11]

The megawatt-class laser was tested at full power in early 2006. The Beacon Illuminator Laser system, which measures and corrects for atmospheric distortion, has also been shipped to Boeing for testing.[12] A complete prototype ABL weapons system will be assembled in 2006.[13]

A related project is the Advanced Tactical Laser (ATL) system, which uses a less powerful version of the ABL's COIL laser, instead of missiles, to attack ground targets. The laser is being built and will be tested in mid-2006. Boeing has received a C-130H transport aircraft from the Air Force and is modifying it for installation of the laser system. The full system will be fitted to the aircraft by 2007 and test-fired against ground targets.[14]

One shortcoming of laser weapons is that their beams travel only in straight lines, which means they have no indirect-fire mode and cannot shoot beyond the system's visual horizon. The DOD Office of Force Transformation, in conjunction with the Air Force Research Laboratory, is developing the Tactical Relay Mirror System (TRMS), which would use a mirror system mounted on an aerostat or UAV (unmanned aerial vehicle) to redirect the beams from laser weapons such as the ATL and ABL. Design specifications are already being determined.[15]

---

7. Bill Gertz, "N. Korea Fired Laser at Troops," *The Washington Times*, May 13, 2003, at *newsmine.org/archive/war-on-terror/north-korea/nkorea-fired-laser-at-troops.txt* (March 15, 2006).
8. "Mobile/Tactical High Energy Laser (M-THEL) Technology Demonstration Program."
9. *Ibid.*
10. Press release, "Airborne Laser Progress Continues as Northrop Grumman Runs Full-Power COIL Tests, Delivers Beacon Illuminator Laser," Northrop Grumman Corporation, January 4, 2006, at *www.irconnect.com/noc/pages/news_printer.mhtml?d=91869* (March 15, 2006).
11. *Ibid.*
12. *Ibid.*
13. SPG Media, "ABL YAL 1A Airborne Laser, USA," at *www.airforce-technology.com/projects/abl* (March 15, 2006).
14. Press release, "Boeing Receives Aircraft for Laser Gunship Program," Boeing, January 23, 2006, at *www.boeing.com/news/releases/2006/q1/060123a_nr.html* (March 15, 2006).
15. Colonel Craig Hughes, Office of Force Transformation, U.S. Department of Defense, "Re-directed Energy: the Tactical Relay Mirror System," presentation at The Heritage Foundation, Washington, D.C., February 13, 2006.

How Microwave Weapons Work

Written off as impractical during World War II, technological advances have now made microwave weapons feasible. However, current research focuses on using them as a means of nonlethal area defense and as anti-electronic weapons rather than as "death rays."

High-power microwave (HPM) weapons work by producing either beams or short bursts of high-frequency radio energy. Similar in principle to the microwave oven, the weapons produce energies in the megawatt range.[16] When the microwave energy encounters unshielded wires or electronic components, it induces a current in them, which causes the equipment to malfunction. At higher energy levels, the microwaves can permanently "burn out" equipment, much as a close lightning strike could.

Semiconductors and modern electronics are particularly susceptible to HPM attacks. Electronic devices can be shielded by putting conductive metal cages around them; however, enough microwave energy may still get through the shielding to damage the device.

The short, intense bursts of energy produced by HPM devices damage equipment without injuring personnel. Mounted on properly shielded aircraft or ships, or dropped in single-use "e-bombs," HPM weapons could destroy enemy radars, anti-aircraft installations, and communications and computer networks and even defend against incoming anti-aircraft and anti-ship missiles. With the ever-increasing use of electronics in weapons systems, HPM devices could have a devastating but nonlethal effect on the battlefield.

Current Microwave Weapons

HPM weapon technology is based on the same technology as radar devices, which already have a long history of research and development. However, no military has yet openly deployed HPM weapons. Current HPM research focuses on pulsed power devices, which create intense, ultrashort bursts of electrical energy and would be used to power the microwave generator of an HPM weapon. The Air Force Research Lab's Propulsion Directorate has studied using generators that use high-temperature superconducting wire and high-voltage capacitors.[17]

Another power source, well suited to one-time use in an e-bomb, is the Explosively Pumped Flux Compression Generator (EPFCG). The EPFCG uses chemical explosives to compress an electrically charged coil. This destroys the device but produces electrical pulses in the terawatt range—the equivalent of 10 to 1,000 lightning strikes.[18]

Paired with a microwave generator, an EPFCG could produce an ultrashort, intense microwave burst. Depending on factors such as burst height, microwave frequency, and the shielding around the target electronics, such an e-bomb could have an effective range of several hundred meters.[19]

A subset of HPM devices can affect the human body. Millimeter waveband energy can penetrate human skin to a very shallow depth, heating the tissue below. This produces a burning pain without actually damaging the tissue. The pain forces the person to flee the area. This type of weapon shows great potential as a riot-control device or area-denial system.[20]

The Active Denial System (ADS) is a nonlethal anti-personnel DEW that uses millimeter-wavelength beams to create a painful sensation in an individual without causing actual injury. It is relatively close to deployment. The sys-

16. U.S. Air Force Research Laboratory, "High-Power Microwaves," fact sheet, September 2002, at *www.de.afrl.af.mil/Factsheets/HPM.swf* (March 15, 2006).
17. Dr. Stephen Adams, "Electrical Power and Thermal Management for Airborne Directed Energy Weapons," U.S. Air Force Research Laboratory, September 2001, at *www.afrlhorizons.com/Briefs/Sept01/PR0101.html* (March 15, 2006).
18. Carlo Kopp, "The Electromagnetic Bomb—A Weapon of Electrical Mass Destruction," at *www.globalsecurity.org/military/library/report/1996/apjemp.htm* (March 15, 2006).
19. GlobalSecurity.org, "High Power Microwave (HPM)/E-Bomb," at *www.globalsecurity.org/military/systems/munitions/hpm.htm* (March 15, 2006).
20. *Ibid.*

tem generates a focused beam of energy at the frequency of 95 gigahertz. These waves penetrate only a few millimeters into the skin and cause the sensation of heat. The sensation increases in intensity until the affected individual moves out of the beam or it is shut off. There is no injury to the target individual.[21]

A demonstration system was tested at Kirtland Air Force Base in 2000. A year later, testing showed that the ADS could produce effects at ranges beyond current small-arms range. A prototype ADS system mounted on a Humvee went into testing in August 2005.[22]

The Future of DEW

Future research will seek to increase the power and decrease the size of DEW systems. As they become smaller, DEW weapons will first be vehicle-mounted and then possibly man-portable. The death ray of science fiction may in fact become a reality in the not too distant future.

Lasers are becoming smaller and more powerful. For example, a recent test of a solid-state laser by Northrop Grumman produced a continuous 27-kilowatt beam that lasted just under six minutes.[23]

A possible future development is the electrolaser. Electrolasers make use of laser bloom, a normally undesired effect. In an electrolaser, twin laser beams create an ionized channel inside the atmosphere, which conducts electricity. A high-voltage electrical charge is then fed into one of the laser beams, striking the target. The electrical shock is enough to stun personnel, detonate improvised explosive devices, or destroy electronic equipment.

Improvements in energy-generating systems may also make particle-beam weapons feasible. Particle beams would have tremendous power as weapons. Like lasers, particle beams travel at the speed of light, but unlike lasers, the particles in a particle beam have mass, giving the beam tremendous kinetic energy.

At some point in the future, entire military units may be armed with only DEWs. A mechanized unit advancing through a town, protected by an anti-artillery and anti-missile laser shield, clearing the surrounding buildings of snipers and enemy troops with an active denial system, and using electrolasers to stun them before taking them prisoner, all while using HPM weapons to render the enemy's communications useless, would be a powerful military unit indeed.

Policy and Legal Implications for DEWs

Weapons designed to cause undue suffering are banned under the Geneva Convention, and human rights groups argue that directed-energy weapons raise a host of new legal and moral concerns that do not apply to previous generations of conventional weapons. For example, while the Chinese ZM-87 laser interference device is technically a laser dazzler, it can permanently damage the human eye at a distance of two to three kilometers.[24] Would the permanent blinding of a soldier struck by a ZM-87's laser beam be considered intentional or accidental? Does the mere use of a weapon that can cause permanent blindness constitute inflicting undue suffering? The humanitarian community is also concerned about the long-term biological effects of DEWs (microwaves in particular) and their possible use against civilian targets.[25]

---

21. U.S. Air Force Research Laboratory, "Active Denial System," fact sheet, September 2005, at *www.de.afrl.af.mil/Factsheets/ActiveDenial.swf* (March 15, 2006).
22. *Ibid.*
23. Press release, "Northrop Grumman Surpasses Power, Run-Time Requirements of Joint High Power Solid-State Laser Program for Military Use," Northrop Grumman Corporation, November 9, 2005, at *www.irconnect.com/noc/press/pages/news_releases.mhtml?d=89438* (March 15, 2006).
24. China North Industries Corporation, "ZM-87 Portable Laser Disturber Fact Sheet," quoted in Human Rights Watch, "Blinding Laser Weapons: The Need to Ban a Cruel and Inhumane Weapon," September 1995, at *www.hrw.org/reports/1995/General1.htm* (March 15, 2006).
25. "Electromagnetic Weapons: Come Fry with Me," *The Economist*, January 30, 2003, at *www.globalsecurity.org/org/news/2003/030130-ebomb01.htm* (March 15, 2006).

However, a stronger counterargument is that directed-energy weapons, especially lasers, are more humane than conventional weapons because they can strike pinpoint targets, thus causing less collateral damage. A laser weapon could target not only a single vehicle in a convoy, but also a specific spot on that vehicle (e.g., the engine) and disable it without injuring the passengers. Furthermore, the power of lasers and microwave weapons has decreased, allowing for nonlethal uses.

DEW technology is changing faster than international laws and treaties can adapt. General DOD policy is that directed-energy weapons can be used legitimately on the battlefield. As with all new weapons, the DOD General Counsel reviews each DEW for compliance with international and U.S. laws before the Pentagon is allowed to field it.[26] Most DEWs are not yet far enough along in development and thus have not received this final stamp of approval.

As the Pentagon addresses these issues, it should do so in the same way that it would for any other category of weapon that it has reviewed. While some uses may be illegal (e.g., targeting an unarmed civilian who in no way poses a threat), other uses are just as assuredly legal and legitimate.

Fixing the Research and Deployment Bottlenecks

While directed-energy research is advancing, inadequate funding is hindering more rapid development and deployment of these technologies. The military has rhetorically embraced the wonders of DEWs, but it has not always opened its wallet to fund the technologies.

True support for a program is often best measured by the resources that an organization is willing to devote to it. For instance, the Active Denial System was not ready for deployment when the United States invaded Iraq, in part because the money was not there. The Defense Department and Congress should start to fund promising and proven DEW technology so that promising weapon systems can move from the lab to the battlefield where they can help military personnel.

Conclusion

DEW technology and its enabling infrastructure have matured to the point that DEWs can begin moving from the lab to the battlefield. While directed-energy technology is not the panacea for all situations that its most ardent advocates claim, it can give the U.S. military flexibility in tailoring its responses (e.g., lethal or nonlethal) to different types of targets (humans or machines).

Much work needs to be done before DEWs are deployed. The armed services need to move from just saying that DEWs are a good idea to fully supporting their development. The Defense Department needs to establish clear guidelines for using the technology. The speed, ultraprecision, and nonlethal capabilities of directed-energy weapons are all good reasons why the United States should continue to research, develop, and, where appropriate, field these technologies.

First published as Heritage Foundation Backgrounder *No. 1931, April 28, 2006.*

26. David Ruppe, "Directed-Energy Weapons: Possible U.S. Use Against Iraq Could Threaten International Regimes," Global Security Newswire, at *www.globalsecurity.org/org/news/2002/020816-dew.htm* (March 15, 2006).

Chapter 2

Future Computing and Cutting-Edge National Security

James Jay Carafano, Ph.D., and Andrew Gudgel

Data mining and cognitive computers are two emerging aspects of future computing that show promise for a large number of national security applications, from detecting terrorists to making battlefield decisions. New computational capabilities are already foreshadowing the next turn of the information revolution: an unprecedented capacity to sift through ever-increasing amounts of data on the Web and on the battlefield to detect patterns and identify which bits of information are essential to human decision-makers.

Future computing capabilities could give the United States an enormous advantage in many areas. In addition, these capabilities can be employed in manner that both respects civil liberties and enhances the protection of individual privacy.

Congress clearly has a role in advancing the use of data mining and other future computing technologies and ensuring that they are employed in an appropriate manner. Congress should establish federal guidelines for the use of data-mining technologies that promote their use for national security purposes while safeguarding the liberties of American citizens. Congress should also monitor government efforts to support research into cognitive computing, encouraging research and development into what could become a significant competitive advantage for the United States in the race for hyper-computing power in the 21st century.

History in the Making

Machines that actually manipulate data are as old as the ancient Greeks, who developed the Antikythera mechanism, a mechanical analog computer that predicted the movements of the sun, moon, and planets.[1] In the 1820s and 1830s, Charles Babbage designed a "difference engine" and an "analytical engine," analog computers that could make complex calculations. However, they were never completed. The ENIAC, one of the first electronic, reprogrammable computers, was built by the University of Pennsylvania and used during World War II to calculate artillery firing tables.[2]

The development of the solid-state transistor and later the integrated circuit allowed the manufacture of cheaper, completely electronic digital computers. In the post–World War II era, digital computers not only served national security needs, but also were used to track bank accounts and other business transactions.

The mathematical foundations of cognitive computing (computers that operated more like human brains) were laid in the 1940s and 1950s and expanded in the 1980s.[3] Computers became increasingly more powerful while simultaneously becoming smaller in size. The development of the personal computer in the 1970s led to improved graphics, and computers went from "crunching numbers" to assistants that helped to represent information visually.

1. Peter James and Nick Thorpe, *Ancient Inventions* (New York: Ballantine Books, 1994), pp. 121–123.
2. Isaac Asimov, *Asimov's New Guide to Science* (New York: Basic Books, 1984), pp. 860 and 862.
3. Neural Network Solutions, "Introduction to Neural Networks: History and Development of Neural Networks," at *www.neuralnetworksolutions.com/nn/intro2.php* (November 27, 2006).

Since the 1980s, the cost of computational power has continued to decline, while the computational capacity of computers has grown exponentially. Today, computers are ubiquitous on battlefields and in boardrooms—key tools in virtually every field in national security and the commercial sector.

Until recently, computers only displayed or modified data in fixed ways that had been predetermined by humans. A computer could only do exactly what it was programmed to do, without deviation. Advances such as data mining and cognitive computing allow computers to manipulate data within general guidelines, finding associations and patterns that humans are unable to see.

Computers are becoming adaptable, capable of learning and making decisions. Applied to national security policy, this evolution of technology has large implications. In addition to being aware of this growing field, Congress should encourage its development.

Computers Rising: Data Mining and Cognitive Computing

Terms such as "data mining" and "cognitive computing" conjure up images of the HAL 9000 computer from the movie *2001: A Space Odyssey*. Data mining is nothing more than looking for patterns in data. Advertising agencies have used it for decades to determine which campaigns have the greatest draw and to identify specific target audiences. Like many other techniques originally done with pencil and paper, data mining has become faster and easier with the use of computers. Coupled with technologies that allow for better gathering of raw data—everything from laser scanners at supermarket checkouts to unmanned aerial vehicles on the battlefield—the volume of data available to decision-makers has increased dramatically.

Data mining has gone through several stages. At first, computers simply collected and stored data. Separate software was required to manipulate the data. Then the tools were built into the database software itself so that the information could be analyzed on the spot.

With the growth of large, networked databases, information had to be moved to a central "warehouse" where it could be analyzed. This centralized system is now giving way to a system in which the data stay in place and software "agents" communicate between databases, mining the data "on site." This allows for real-time analysis of ever-changing information.[4]

Other uses of data mining include bioinformatics, which sifts through large volumes of information from biological experiments. Earlier this year, researchers at Stanford and Harvard Universities used data-mining techniques to identify gene correlations across a number of different experiments by sifting through results that had been submitted to scientific journals.[5] GlaxoSmithKline, a pharmaceutical company, is developing a similar database and techniques to conduct drug discovery research.[6] Data-mining techniques are also used extensively in detecting computer intrusions and for terrorist screening.[7]

Cognitive computing promises a new generation of computers that mimic the functions of human brains. Unlike today's computers, cognitive computers operate autonomously, using learning and reasoning to derive new knowledge. The Department of Defense has explored the use of cognitive computing for autopilots and has already tested self-piloting craft that adapt to changing conditions. Cognitive computing promises to reduce the time needed to develop new smart weapons and unmanned combat aerial vehicles.[8]

---

4. Jesús Mena, speaking at program on "Future Computing: Shaping National Security Policy from the Inside Out," The Heritage Foundation, Washington, D.C., November 6, 2006, at *www.heritage.org/Press/Events/ev110606a.cfm*.
5. Press release, "Stanford/Packard Scientist's Data-Mining Technique Strikes Genetic Gold," American Association for the Advancement of Science *EurekAlert!*, January 10, 2006, at *www.eurekalert.org/pub_releases/2006-01/sumc-ssd011006.php* (November 27, 2006).
6. Press release, "Output of e-Science Project Helps GSK Speed Up Drug Discovery," American Association for the Advancement of Science *EurekAlert!*, September 21, 2005, at *www.eurekalert.org/pub_releases/2005-09/eaps-ooe091905.php* (November 27, 2006).
7. Varun Chandola, Eric Eilertson, Levent Ertoz, Gyorgy Simon, and Vipin Kumar, "MINDS: Architecture & Design," University of Minnesota, Minneapolis, July 14, 2006, at *http://handle.dtic.mil/100.2/ADA455153* (June 29, 2007), and Jeffrey W. Seifert, "Data Mining and Homeland Security: An Overview," Congressional Research Service *Report for Congress*, updated January 27, 2006, at *http://handle.dtic.mil/100.2/ADA450426* (June 29, 2007).

Cognitive computing is also being used to translate spoken language in real time, creating an "instant translator." The technology has already been used to demonstrate simultaneously translation between spoken English and Spanish and between English and Mandarin Chinese.[9]

Potential National Security Applications

While current computing technology continues to expand the ability of the intelligence community and Department of Homeland Security to "connect the dots," the most dramatic unclassified developments in future computing are happening within the Department of Defense.

As the number of sensor systems on the battlefield increases dramatically, so does the volume of raw information flowing to military commanders and decision-makers. Picking the handful of essential facts out of this ocean of information will become increasingly more difficult.

To this end, the U.S. Army Research Laboratory has established a research program to investigate the use of data mining to ensure that soldiers and commanders are not overburdened with data.[10] In June 2006, the U.S. Air Force Research Laboratory awarded a contract to conduct research on developing filter and data-mining technologies to provide information to aid intelligence analysts in making decisions.[11]

Advances in sensors, as well as in computer hardware and software, could lead to integrated sensor-processor suites that take in raw information on the battlefield, determine which data are valuable, process them, and forward decision-ready intelligence to the human that receives the sensor's output. Other integrated sensor-processor packages could allow weapons systems to identify and reprioritize targets on the fly.

Sensors and data mining are not only useful in making targeting decisions. Weather can profoundly affect military operations and communications, and wind patterns are important in tracking clouds of chemical or biological agents. The U.S. Army Research Laboratory has established a research project that hopes to use networks of sensors and computers to turn weather data into real-time weather intelligence and decision aids for commanders.[12]

Cognitive computers, which could learn and re-learn, would be capable of not only working around battle damage, but also improving the speed and accuracy of their calculations, essentially gaining experience.[13] The U.S. Office of Naval Research is examining the feasibility of creating large-scale neural networks (structures that mimic brain functions) that would do more than simple pattern matching and enter into the realm of cognitive skills that can make human-like decisions.[14]

Cognitive computers could also perform mundane tasks such as preventive maintenance. The U.S. Air Force Research Laboratory is conducting research on creating an advanced aircraft engine that would both adapt to changing flight conditions and self-identify maintenance problems and needed repairs.[15]

---

8. Jeff Pleinis, "Advanced Adaptive Autopilot," U.S. Air Force Research Laboratory, Munitions Directorate, at *www.afrlhorizons.com/Briefs/Jun03/MN0213.html* (November 20, 2006).
9. U.S. Air Force Research Laboratory, "Automatic Spoken Language Translation," at *www.rl.af.mil/div/IFB/techtrans/datasheets/ASLT.html* (November 20, 2006; unavailable June 29, 2007).
10. U.S. Army Research Laboratory, "ARO Computing and Information Sciences 11.0," at *www.arl.army.mil/main/Main/default.cfm?Action=29&Page=205* (November 27, 2006; unavailable June 29, 2007).
11. Francis Crumb, "AFRL Awards Small Business Contract to Utica Firm," June 23, 2006, at *www.if.afrl.af.mil/div/IFO/IFOI/IFOIPA/press_history/pr-06/pr-06-61.html* (November 27, 2006; unavailable June 29, 2007).
12. U.S. Army Research Laboratory, "C4I: Battlefield Weather for Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR)," modified August 11, 2005, at *www.arl.army.mil/main/Main/default.cfm?Action=18&Page=69* (November 20, 2006).
13. U.S. Defense Advanced Research Projects Agency, "Self-Regenerative Systems: Mission," at *www.darpa.mil/ipto/programs/srs/index.htm* (November 15, 2006).
14. U.S. Office of Naval Research, "Neural Engineering & Biorobotics: Neural Computation," at *www.onr.navy.mil/sci_tech/34/341/ne_comp.asp* (November 15, 2006).
15. Tim Lewis, "Future Aircraft Jet Engines Will Think for Themselves," U.S. Air Force Research Laboratory, Propulsion Directorate, at *www.afrlhorizons.com/Briefs/Dec01/PR0105.html* (November 20, 2006).

Besides weapons systems, cognitive computers could be used to simulate possible scenarios and indicate courses of action for battlefield decision-makers. The Air Force Research Laboratory is looking at ways to create systems that would run multiple, branching simulations within a computer and use "intelligent" adversaries that would adapt their responses to changing conditions and human-made choices.[16] A similar system is being developed to run command-and-control-type exercises.[17]

What Congress Should Do

Data mining and cognitive computing show promise in many important applications. Improved data mining and cognitive computing techniques will increase the number of potential uses and push the actual manipulation of raw data "down the chain" toward sensors and other input devices. Congress can best help to exploit these emerging technologies by setting rules and investing in future computing.

Setting the Rules. Congress clearly has a role in advancing the use of data mining and other information technologies for national security purposes and in ensuring that they are employed in an appropriate manner. Establishing federal guidelines for the use of these technologies is one way to address the issue.

Such guidelines would begin by defining what programs should come under the scope of data-mining programs. They should also include the following elements:

- Every deployment of federal data-mining technology should require authorization by Congress.
- Agencies should institute internal guidelines for using data analysis technologies, and all systems should be structured to meet existing legal limitations on access to third-party data.
- A Senate-confirmed official should authorize any use of data-mining technology to examine terrorist patterns. The system used should allow only for the initial query of government databases and disaggregate personally identifying information from the pattern analysis results.
- To protect individual privacy, any disclosure of a person's identity should require a judge's approval.
- A statute or regulation should require that the only consequence of being identified through pattern analysis is further investigation.
- A robust legal mechanism should be created to correct false positive identifications.
- To prevent abuse, accountability and oversight should be strengthened by internal policy controls, training, executive and legislative oversight, and civil and criminal penalties for abuse.
- The federal government's use of data-mining technology should be strictly limited to investigations related to national security.

Investing in Future Computing. Congress should encourage government research into exploiting cognitive computing for national security applications. These technologies could meet a wide range of homeland security and defense needs, from information systems that draw on retained information to identify links between terrorists to weapons with instantaneous target acquisition that also provide real-time information to battlefield decision-makers. The Department of Homeland Security and the Department of Defense should continue to fund and develop cognitive computing.

16. Duane A. Gilmour, James P. Hanna, Walter A. Koziarz, William E. McKeever, and Martin J. Walter, "High-Performance Computing for Command and Control Real-Time Decision Support," U.S. Air Force Research Laboratory, Information Directorate, at *www.afrlhorizons.com/Briefs/Feb05/IF0407.html* (November 20, 2006).
17. Michael J. Young, "Agent-Based Modeling and Behavioral Representation," U.S. Air Force Research Laboratory, Human Effectiveness Directorate, at *www.afrlhorizons.com/Briefs/0006/HE0009.html* (November 20, 2006).

The Way Forward

Data mining and cognitive computers are powerful tools that could greatly improve the identification, analysis, and decision-making capabilities in homeland security and defense. Congress not only should be aware of these computing technologies, but also should encourage their development by creating policy that establishes clear guidelines for responsible use within constitutional limits without impeding future development.

First published as Heritage Foundation Backgrounder *No. 2049, July 5, 2007.*

Chapter 3

National Security and Biotechnology: Small Science with a Big Potential

James Jay Carafano, Ph.D., and Andrew Gudgel

Biotechnology is one of the world's fastest growing commercial sectors. Since 1992, the number of biotechnology companies in the United States alone has tripled. These firms are research-intensive, every day bringing into the marketplace new methods and products that may reshape medical practices and human performance, allowing for unprecedented improvements in health care.

Many of biotechnology's benefits are dual-use, increasing the possibility that knowledge, skills, and equipment could be adapted for use as biological weapons. As the global biotechnology industry expands, the U.S. government should therefore increase its capacity to exploit biotech advances for national security.

The challenge of exploiting cutting-edge biotechnology will be different from the way the Pentagon harnessed science and technology for national security during the Cold War. Rather than driving the biotechnology revolution, the federal government will need to figure out how best to utilize and adapt the products developed by a multibillion-dollar transnational industry that already has the money and capacity for research and development.

To keep up, the federal government must adopt legislative, policy, and organizational innovations. These should include promoting international liability protection for developing and deploying new national security goods and services, promoting scientific travel and exchanges, and assigning a lead agency to coordinate biotechnology exploitation for national security.

From There to Here

Biotechnology refers to any technological application that uses living organisms to make or modify products for explicit use,[1] specifically through DNA recombination and tissue culture. Gregor Mendel first described the role of genes through his research on "dominant and recessive factors" in the 1860s. By the 1940s, scientists were aware of DNA, and James Watson, Francis Crick, and Rosalind Franklin modeled its structure in the 1950s.

In 1970, the discovery of enzymes, which break apart and connect snippets of DNA, allowed for the creation of genetically modified organisms. This bore fruit by the early 1980s, when scientists managed to genetically modify bacteria to produce human insulin,[2] which is now the principal source of insulin for diabetics.

Recently, major advances in information technologies have led to the development of bioinformatics.[3] Bioinformatics focused initially on creating and storing biological and genetic information, most notably in the Human Genome Project. Scientists are now combining this information into a comprehensive picture, enabling researchers to study how different diseases alter these activities. Combining advances in genomics and information technology has significantly enhanced the industry's capability to bring new products to the marketplace.

---

1. See, for example, Article 2 of the Convention on Biological Diversity at *www.cbd.int/doc/legal/cbd-un-en.pdf*.
2. Isaac Asimov, *Asimov's New Guide to Science* (New York: Basic Books, 1984), pp. 627 and 635.

Many of the advancements in biotechnology are dual-use. The technology that may revolutionize medical care by providing faster-acting and more effective drugs could also be used to field more lethal biological weapons. Thus, federal agencies have a clear imperative not only to exploit the advantages of new developments, but also to anticipate and prepare countermeasures for how potential adversaries might exploit these medical advances.

Current Research

Much of the current biotech research focuses on agent detection, vaccines, and treatment. Scientists are studying the immune systems of primitive organisms, such as jawless fish, to garner greater understanding of the human immune system and to develop new antibody therapies.[4] They are also studying how diseases infect and affect human cells. For example, recent research indicates that the family of bacteria that includes bubonic plague blocks immune system responses using a protein related to one naturally found in humans.[5] Scientists are also investigating ways to create vaccines that work against whole classes of disease-causing organisms and to boost the human immune system in general.[6]

Research is also underway to counter the rise of multidrug-resistant bacteria. Scientists are investigating the use of bacteriophages, which are viruses that prey on bacteria, as a means to fight infectious disease. Ironically, research on bacteriophages began in the early 20th century but declined after the discovery of antibiotics. In the summer of 2006, the U.S. Food and Drug Administration approved the use of a bacteriophage preparation on meat as an antimicrobial agent against Lysteria bacteria.[7]

Better vaccines and treatments could provide permanent immunity to all "classic" biological agents or at least reduce their lethality to a considerable degree. In October 2006, the Institute for Soldier Nanotechnologies at the Massachusetts Institute of Technology announced the development of microscopic pumps that would allow rapid testing of blood and other fluids by pumping them into a "lab on a chip," which would detect biological or chemical agents.[8]

Argonne National Laboratory is also developing its own biochip detection technology.[9] This "lab on a chip" research points to the feasibility of rapid biological agent detection, allowing individuals to know whether they have been exposed within minutes rather than days. It may even be possible to develop implantable biosensor chips that would continuously monitor for exposure to biological agents.[10]

---

3. Bioinformatics is the use of databases and analytical tools for genome analysis and innovations in molecular biology. One study holds that bioinformatics can reduce the cost of drug development by 18 percent and cut one year from developmental timelines. "The Race to Computerize Biology," *The Economist*, December 12, 2002. Among its many applications to biowarfare, bioinformatics can facilitate the identification of pathogens. For example, see D. A. Henderson, Director, Office of Public Health Preparedness, U.S. Department of Health and Human Services, statement before the Committee on Science, U.S. House of Representatives, December 5, 2001, at *www.hhs.gov/asl/testify/t011205.html* (July 16, 2007). Bioinformatics also holds great promise in developing therapeutic responses to a bioattack. For example, studies show that variations in individual responses to therapeutic drugs are affected by genetic polymorphisms (variations in enzymes caused by slightly different amino acid sequences). Pharmacogenetics employs bioinformatics to assist in decoding and mapping millions of polymorphisms across the human genome, which can provide insights into the links between disease-causing genes and drug-response genes, facilitating the development of new therapeutic strategies. Michael M. Shi, "Diagnostics Meets Therapeutics: The Impact of Pharmacogenetics," *Drug Discovery Today*, Vol. 7, Issue 23 (December 2002), pp. 1161–1162.
4. "Tiny Tampa Bay Fish Key to Evolution of Immune System," American Association for the Advancement of Science *EurekAlert!*, October 2, 2006, at *www.eurekalert.org/pub_releases/2006-10/uof-ttb100306.php* (November 21, 2006).
5. "Study Illuminates How the Plague Bacteria Causes Disease," American Association for the Advancement of Science *EurekAlert!*, September 7, 2006, at *www.eurekalert.org/pub_releases/2006-09/cp-sih090106.php* (November 21, 2006).
6. "Medical College of Wisconsin Researchers Develop Broad-Spectrum Defense Against Germ Warfare: Biodefense Leaps Ahead of One Vaccine for One Germ Approach," American Association for the Advancement of Science *EurekAlert!*, December 9, 2005, at *www.eurekalert.org/pub_releases/2005-12/mcow-mco120805.php* (November 21, 2006).
7. *Federal Register*, Vol. 71, No. 160 (August 18, 2006), at *www.cfsan.fda.gov/~lrd/fr060818.html* (November 30, 2006).
8. Anne Trafton, "MIT Designs Portable 'Lab on a Chip,'" American Association for the Advancement of Science *EurekAlert!*, October 17, 2006, at *www.eurekalert.org/pub_releases/2006-10/miot-mdp101706.php* (October 18, 2006).
9. Donna Jones Pelkie, "Biochip Technology Would Become Standard Diagnostic Tool for Human, Veterinary Medicine," Argonne National Laboratory, November 17, 2006, at *www.anl.gov/Media_Center/News/2006/ES061117.html* (November 21, 2006).
10. Trafton, "MIT Designs Portable 'Lab on a Chip.'"

The Future of Biotechnology

Future advances in biotechnology will continue to improve the protection of both the general public and military personnel from deadly biological agents. The creation of broad-spectrum vaccines may give the public health community the ability to vaccinate the country's entire population against both endemic diseases and biological weapons. A bioweapon inoculation may someday be as common as other childhood vaccinations.

Besides disease detection and vaccines, biotechnology has numerous other potential applications. The military is exploring the use of biomimicry, which uses natural biological systems or material as an inspiration for solving engineering problems. For example:

- In 2002, scientists discovered how geckos stick themselves to smooth surfaces using van der Waal's forces—the weak natural attraction between atoms—and were then able to re-create the surface of a gecko's foot artificially.[11]
- The Defense Advanced Research Projects Agency is researching devices that mimic geckos' use of van der Waals force to enable soldiers to climb buildings without ropes or ladders.[12]
- Scientists are also researching spider silk and abalone shell to create stronger, lighter armor for personnel and vehicles.[13]
- Other projects include developing organic solar cells[14] and a new generation of sensors and optics derived from biological and silicon-based systems.[15]

The next great step in biotechnology is proteomics: the direct manipulation and construction of proteins. While DNA instructs cellular mechanisms in how to operate, proteins do the actual work inside and outside of cells. Proteins are found in everything from papayas to snake venom. Because protein structure and composition is much more complex than DNA, protein analysis is much more difficult and time-consuming. However, understanding how proteins are constructed and how they behave promises to be as great an advance in biological science as understanding DNA was in the 20th century.

If advances in biotechnology continue, constructing a completely artificial organism from the "ground up"—creating synthetic DNA and proteins from raw materials and then combining them to form living cells—may be possible in the not too distant future.

National Security and Biotechnology

The challenge for the federal government is to figure out how to leverage cutting-edge biotechnology for national security purposes. Before 2001, the Department of Defense (DOD) was the primary arm of the federal government in funding biological defense and research related to national security. The DOD research program focused primarily on the battlefield uses of biotechnology.

The events of 9/11 and the post-9/11 anthrax letters shifted the focus to the American people's vulnerability to biological threats. In many respects, the DOD research was not directly applicable to other biodefense national security needs. For example, DOD immunization programs assume that the individuals to be immunized will be gener-

---

11. Keller Autumn, "Evidence for van der Waals Adhesion in Gecko Setae," *Proceedings of the National Academy of Sciences*, Vol. 99, No. 19 (September 17, 2002), at *www.pnas.org/cgi/reprint/99/19/12252.pdf* (July 16, 2007).
12. Defense Advanced Research Projects Agency, "Z-Man," at *www.darpa.mil/dso/thrust/matdev/zman.htm* (November 29, 2006; unavailable July 16, 2007).
13. "Biosteel®," Nexia Biotechnologies Inc., *www.nexiabiotech.com/en01_tech/01-bst.php* (November 30, 2006). Robin Lloyd, "Abalone Armor: Toughest Stuff Theoretically Possible," LiveScience, *www.livescience.com/technology/050118_abalone_armor.html* (November 28, 2006).
14. Michael Durstock and Timothy Anderl, "Organic Solar Cells," U.S. Air Force Research Laboratory, *www.afrlhorizons.com/Briefs/Jun04/ML0319.html* (November 20, 2006).
15. Defense Advanced Research Projects Agency, "Biological Sensory Structure Emulation," at *www.darpa.mil/dso/thrust/biosci/bsse.htm* (November 15, 2006; unavailable July 16, 2007), and "Engineered Bio-Molecular Nano-Devices/Systems," at *www.darpa.mil/dso/thrust/biosci/moldice.htm* (November 15, 2006; unavailable July 16, 2007).

ally healthy and young. On the other hand, immunizations for a general population in the event of biological weapons attack would have to consider the effects of vaccines on old and young people and on individuals with medical conditions who might have weakened or compromised immune systems and react very differently to a vaccine developed by the military.[16]

To apply research to broader national security concerns, the National Institutes of Health (NIH) under the Department of Health and Human Services (HHS) received the bulk of increased funding for developing biodefense measures.[17] In recent years, in addition to HHS and DOD, many other federal agencies have initiated biotechnology research related to national security, including the recently established Department of Homeland Security (DHS). While much of the research in DOD, HHS, and other federal entities involves detecting, protecting against, and mitigating biological attacks and pandemics, it also involves other products related to national security, including human performance enhancement (such as reducing the effects of stress and fatigue) and battlefield medical treatment. There is a plethora of ongoing programs.

The Pentagon has considerable experience and capacity for medical research and development of products related to national security, but this is virtually a new mission for the NIH, which historically has focused on basic scientific research.[18] The U.S. Army Medical Research Institute for Infectious Diseases has unique research facilities and expertise in biowarfare defense. On the other hand, the DOD's record with respect to developing and producing vaccines has engendered significant controversy.

The post-9/11 expansion of the government application of biotechnology to national security has not been matched by organizational innovations to manage and integrate programs more effectively. DOD, DHS, and NIH research programs are not routinely coordinated, and NIH policies prohibit funding other federal institutions. Thus, NIH programs cannot utilize DOD scientists who may have valuable knowledge and experience relevant to NIH national security research. In some cases, government-sponsored research duplicates other programs, and opportunities for complementary research programs are missed.[19]

Enlisting the Private Sector

Harnessing the vast capabilities of the private sector has proven similarly challenging. Compared to potential commercial buyers, the government is a modest-sized customer for biotech firms. There are also other issues. After 9/11, insurance skyrocketed for technologies developed for homeland security. While the demand for new security technologies has swelled, companies must weigh the pressure to rush new products to the marketplace against their liability risks.

In 2002, Congress enacted the Support Anti-Terrorism by Fostering Effective Technologies (SAFETY) Act[20] to encourage companies to continue researching and developing biotechnologies vital to homeland security. The act protects companies from litigation if their products fail during a terrorist attack or are harmfully employed by terrorists. The DHS has shown some success in implementing the legislation and granting SAFETY Act protections to goods and services that are employed to prevent or respond to terrorist threats. However, companies do not enjoy similar protections from other countries when the technologies are deployed outside the United States or adopted by U.S. friends and allies.

The government also has a mixed record in encouraging the private sector to develop new national security capabilities. In 2004, the President announced the implementation of Project Bioshield to accelerate research on and development, purchase, and availability of effective medical countermeasures against biological, chemical, radiological, and nuclear agents. The program provided $6 billion over the next 10 years to private companies for research

16. Coleen K. Martinez, "Biodefense Research Supporting the DoD: A New Strategic Vision," Strategic Studies Institute, p. 24, at *www.strategicstudiesinstitute.army.mil/pdffiles/PUB767.pdf* (July 16, 2007).
17. *Ibid.*
18. *Ibid.*, pp. 25–26.
19. *Ibid.*, pp. 28–29.
20. Public Law 107–296, Subtitle G, §§ 861–865.

and development of next-generation countermeasures against anthrax, smallpox, and other infectious agents and antidotes against chemical and radiological threats. To date, the effort has yielded meager results.[21]

The response to 9/11 has introduced another difficulty in advancing biotechnology research in the United States. After the terrorist attacks on New York and Washington, the United States imposed a number of additional requirements on visa issuance and monitoring to thwart travel by terrorists. These measures included more rigorous registration and monitoring of foreign graduate students, mandatory interviews of all overseas visa applicants, and requiring visa holders to return to their countries of origin to renew their visas.

These measures have had unintended consequences, including deterring top graduate students from coming to the United States, making scientific exchanges more difficult, and even prompting companies and academic and scientific associations to move meetings, conferences, and research facilities outside of the United States. As a result, the United States has become less competitive in many key scientific areas, including biotechnology.[22]

Moving Forward

The United States has no room for complacency. Without better policies, programs, and management, it risks losing its competitive advantage in exploiting biotechnology for national security. Congress and the Administration should act to set the right conditions for the government to adopt commercial biotechnology developments. Specifically, they should:

- **Restructure national security biotechnology programs**. While increased funding has transformed it into the leading federal agency in biosecurity research, the NIH is inexperienced and unproven in its ability to develop products. Likewise, the DHS has yet to demonstrate that it can produce cutting-edge biotechnology advances. Conversely, the DOD has significant experience and skills in developing biodefense countermeasures.

  To the maximum extent possible, research programs should be consolidated under a single agency. Where consolidation is not practical, a more effective management structure is needed to leverage the advice and expertise in different agencies in support of NIH programs.[23]

- **Encourage other countries to adopt SAFETY Act protections.** While the SAFETY Act has been successfully implemented in the United States, it does not protect companies from litigation abroad. Consequently, companies that operate outside of the United States have shied away from contributing to biosecurity because of the potential risks.

  The Administration should develop a strategy to encourage other countries to adapt similar protections. The U.S. strategy should take a regional approach, beginning with the European Union and Japan.

- **Reform visa issuance and management.** U.S. national security and competitiveness rely heavily on people's ability to travel to the United States, but the current visa system is unnecessarily depriving the United States of many of the world's best and brightest scientists, students, and entrepreneurs. Long wait times for personal interviews are among the most frequently cited factors that make travel to the United States difficult.

  Congress should remove the requirement for personal interviews of virtually all non-immigration visa applicants and restore the Secretary of State's ability to waive personal interview requirements. The U.S. should begin using electronic visa applications to reduce applicants' travel expenses and should reduce processing times to 30 days or less. All of these reforms can be implemented in a manner that makes international travel both more convenient and more secure.[24]

21. U.S. Department of Health and Human Services, Biomedical Advanced Research and Development Authority, "Project BioShield," updated April 3, 2007, at *www.hhs.gov/aspr/ophemc/bioshield/index.html* (April 23, 2007; unavailable July 16, 2007).
22. James Jay Carafano, "Sustaining Military Capabilities for the 21st Century: Rethinking the Utility of the Principles of War," Heritage Foundation *Lecture* No. 896, September 6, 2005, at *www.heritage.org/Research/NationalSecurity/hl896.cfm*.
23. Martinez, "Biodefense Research Supporting the DoD," p. 26.

Making the Nation Safer

Dual-use biotechnologies developed in the private sector offer powerful tools to protect Americans from biological threats and to increase the military's operational capabilities. Congress and the Administration should not only be aware of this growing field, but also act to ensure that the private sector—which is making the largest investment in basic research and product development—remains competitive. Specifically, the U.S. government should streamline the federal government's capability to fund and adapt new technologies, work to expand litigation protection beyond the country's borders, and further reform U.S. visa issuance and monitoring programs.

First published as Heritage Foundation Backgrounder *No. 2055, July 23, 2007.*

24. James Jay Carafano, Brian C. Goebel, and Josh Kussman, "Coming to America: Initiatives for Better, Faster, and More Secure Visas," Heritage Foundation *Backgrounder* No. 1976, September 29, 2006, at *www.heritage.org/Research/NationalSecurity/bg1976.cfm*.

Chapter 4

Nanotechnology and National Security: Small Changes, Big Impact

James Jay Carafano, Ph.D., and Andrew Gudgel

Nanotechnology is an emerging transformational technology that promises wide and dual-use applications in many fields, particularly national security. The United States is the world's acknowledged leader in nanoscience, but stiff international competition is narrowing America's lead. Many other countries, specifically European nations and China, have large, established nanotechnology initiatives. Most commercial applications of nanotechnology are still nascent.

In the near term, the most promising developments for national security will likely come from government research rather than from the application of commercial off-the-shelf nanotechnologies. To meet national security needs in the near term, the U.S. government needs to adopt new legislative and policy innovations, including promoting long-term research, distributing federal grants more widely, and promoting scientific travel and exchanges to maintain a supply of skilled experts. Over the long term, the government should remove capital and regulatory barriers to lower the cost of research and emerging technologies and should address safety and environmental issues.

What Is Nanotechnology?

"Nanotechnology" is derived from "nano," the Greek word for dwarf. It involves manipulating and manufacturing particles at the microscopic and even atomic levels, between 1 nanometer and 100 nanometers. By comparison, a human hair is roughly 100,000 nanometers wide.

Combining the ability to manipulate molecular structures with advances in genomics and other biological sciences has created a wealth of new research opportunities. By putting these unique properties to work, scientists are developing highly beneficial dual-use products in medicine, electronics, and many other industries that will also provide enormous defense and homeland security capabilities.

These scientific developments are creating new industries. The market opportunities are so substantial that many government and business leaders describe nanotechnology as "the next industrial revolution."

Nanotechnology was incorporated into manufactured goods worth more than $30 billion in 2005, and this figure is projected to reach $2.6 trillion by 2015.[1] However, since nanotechnology is relatively new, government research is critical for developing applications of this new technology, particularly in the field of national security.

A Small Beginning

The birth of nanotechnology can be traced to 1981, when Gerd Binning and Heinrich Rohrer, scientists at IBM Research, Zurich, created the scanning tunneling microscope (STM). The STM was the first instrument capable of

1. Sean Murdock, prepared statement in hearing, *Nanotechnology: Where Does the U.S. Stand?* Subcommittee on Research, Committee on Science, U.S. House of Representatives, 109th Cong., 1st Sess., June 29, 2005, p. 41, at *http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_house_hearings&docid=f:21950.wais.pdf* (September 13, 2007).

performing operations at the atomic scale, such as adding or removing individual electrons to or from atoms and molecules. It gave researchers the unprecedented ability to change materials "from the bottom up." The two scientists won the Nobel Prize in physics for their invention in 1986.[2]

Within a few years, scientists had demonstrated the capability to manufacture nanoparticles. The discovery of fullerines (isomers or molecules of pure carbon that can be manipulated into unique structures, such as "buckyballs") in 1985 and carbon nanotubes (manufactured one-atom-thick sheets of carbon rolled into cylinders) in 1991 sparked further interest in nanotechnology.

These molecules have novel properties that make them potentially useful in a wide variety of applications, including electronics, optics, and other fields of material science. They also exhibit extraordinary strength and unique electrical properties. Carbon nanotubes are 100 times stronger than steel at one-sixth the weight, while buckyballs are hollow, making them well suited for use as carriers of drugs or other materials.[3]

Nanotechnology Today

Current commercial nanotechnological products are limited to first-generation passive applications, such as nanoparticles, coatings, catalysts, and nanocomposites (materials formed from organic and inorganic components at the nanoscale). Products include cosmetics, automobile parts, clothing, and sports equipment. Research is quickly leading nanotechnology to converge with other fields, including biotechnology, information technology, and cognitive science.

Using techniques commonly found in semiconductor manufacture, researchers have created adjustable "quantum dots" by making "wells" and "corrals" on silicon chips where individual electrons can be trapped and held. The shell of electrons around every atom determines its properties, such as color and electrical conductivity. By filling these quantum corrals with differing numbers of electrons, researchers can create artificial "atoms" that have the same properties as any element on—or beyond—the periodic table, although these "atoms" are temporary and lack nuclei.

Simply adding or subtracting electrons from these wells changes the type of "atom." Grids of quantum corrals built across the surface of a silicon semiconductor chip would allow the creation of artificial molecules, which would theoretically allow the entire chip to have—at least on its surface—the physical properties of almost any material imaginable.

Some aspects of current nanotechnology also blur the line with biotechnology. For example, nanoparticles (clusters of tens to hundreds of individual atoms) have been used in medical research to fight diseases, including cancer. Researchers are also exploring ways to manipulate the genetic code that have tremendous implications in the diagnosis and treatment of diseases. A nanoparticle that encapsulates medication with biomolecules could be designed to bind only to the cells that need the medicine. Such research could also affect other disease research and possibly change the medical response to national catastrophic disaster.[4]

Nanophotonics is another growing field of nanotechnology research. Photonics, which uses light, is the ability to control photons for the purpose of carrying, processing, storing, or displaying information. Well-known applications of photonics include fiberoptic cable, television screens, computer displays, and laser and imaging systems.

In nanophotonics, scientists control the morphology of materials and, as a result, can now change how a material refracts light. Thus, nanophotonics is not simply the scaling-down of existing systems, but utilizing physics, functionalities, and design strategies that are different from regular photonics to produce tiny waveguides, microscopes on a single chip, better optical communications equipment, and chemical and biological sensors.[5]

---

2. John W. Cross, "Scanning Probe Microscopy (SPM)," June 13, 2003, at *www.mobot.org/jwcross/spm* (May 10, 2007).
3. Nanotechnology Now, "Nanotubes and Buckyballs," March 14, 2006, at *www.nanotech-now.com/nanotube-buckyball-sites.htm* (February 26, 2007).
4. Press release, "Gold Nanorods May Make Safer Cancer Treatment," Georgia Institute of Technology, March 14, 2006, at *www.gatech.edu/news-room/release.php?id=889* (February 26, 2007).

National Security Implications

In 2000, the federal government established the National Nanotechnology Initiative (NNI) to promote nanotechnology research at the federal level. The NNI is managed by the Nanoscale Science Engineering and Technology Subcommittee of the National Science and Technology Council, an interagency organization of 26 federal agencies that coordinates planning, budgeting, and program implementation among defense and national security stakeholders. This structure is vital to disseminating information and fostering cross-disciplinary networks and partnerships. Both the Department of Defense (DOD) and Department of Homeland Security (DHS) are NNI members.

In addition to funding research, federal support through the NNI provides crucial funds for the creation of nanotech support infrastructure, such as nanoscale research labs, and for educational resources to develop a skilled workforce capable of advancing nanotechnology. These programs encourage business, including small business, to pursue nanotechnology opportunities.[6]

Military Applications. All branches of the U.S. military are currently conducting nanotechnology research, including the Defense Advanced Research Projects Agency (DARPA), Office of Naval Research (ONR), Army Research Office (ARO), and Air Force Office of Scientific Research (AFOSR). The Air Force is heavily involved in research of composite materials.[7] Among other projects, the Navy Research Laboratory's Institute for Nanoscience has studied quantum dots for application in nanophotonics and identifying biological materials.[8] In May 2003, the Army and the Massachusetts Institute of Technology opened the Institute for Soldier Nanotechnologies, a joint research collaboration to develop technologies to protect soldiers better.[9]

Nanotechnology has numerous military applications. The most obvious are in materials science. Carbon nanotubes and diamond films and fibers have higher strength-to-weight ratios than steel, which allows for lighter and stronger armor and parts for vehicles, equipment, and aircraft. Such upgraded military Humvees would better protect soldiers from improvised explosive devices (IEDs) and small-arms fire.

In another application, adding nickel nanostrands (ropes of material no wider than a few molecules), which can conduct electricity, could make aircraft more resistant to lightning strikes. The nickel strands also have magnetic properties that may prove useful in filters and energy storage devices.[10]

The U.S. Army is actively pursuing nanotechnology for use in soldiers' uniforms, equipment, and armor. As part of the planned Objective Force Warrior Soldier Ensemble, the Army hopes to create a uniform that provides flexible armor protection for soldiers' limbs through the use of shear thickening liquids that solidify when force is applied to them. This would greatly reduce the weight that a soldier must carry. (Current body armor weighs around 25 pounds.)

Other features of the planned uniform include medical sensors, medical treatment capabilities, communications, and individual environmental control for the soldier and integrated thermal, chemical, and biological sensing systems woven into the garment's fabric.[11]

Nanotechnology would allow for more precise control of fuel combustion and detonation of explosives. Explosives and propellants could be constructed atom by atom to optimal particle sizes and ratios of ingredients so that the materials approach their theoretical limits of energy release. This would lead to smaller, more powerful rockets, propellants, warheads, bombs, and other explosive devices.

---

5. Ravi Athale, "Implications of Nanophotonics Technology for National Security," video recording, presentation at The Heritage Foundation, March 29, 2006, *at http://multimedia.heritage.org/content/wm/Lehrman-032906.wvx* (February 26, 2007).
6. National Nanotechnology Initiative, "About NNI," at *www.nano.gov/html/about/home_about.html* (August 6, 2007).
7. U.S. Naval Research Laboratory, "DOD Laboratories," at *www.nanosra.nrl.navy.mil/laboratories.php* (February 26, 2007).
8. U.S. Naval Research Laboratory, Institute of Nanoscience, "Publications," at *www.nrl.navy.mil/nanoscience/publications.html* (September 12, 2007).
9. Curt Biberdorf, "Institute for Soldier Nanotechnologies Opens," Army News Service, May 28, 2003, at *www.globalsecurity.org/military/library/news/2003/05/mil-030528-usa02.htm* (February 26, 2007).
10. U.S. Air Force Research Laboratory, Materials and Manufacturing Directorate, "Nickel Nanostrands Expand Nanotechnology Engineering Capabilities," at *www.ml.afrl.af.mil/stories/MLB/asc_03_1622.html* (February 26, 2007).
11. GlobalSecurity.org, "Objective Force Warrior," at *www.globalsecurity.org/military/systems/ground/ofw.htm* (February 26, 2007).

For slower release of energy, nanotechnology would allow for more powerful batteries, fuel cells, photovoltaic panels, and perhaps even more exotic methods of generating electrical power. Researchers at the Georgia Institute of Technology recently developed piezoelectric fibers, which someday may be used in fabrics that generate their own electricity, completely eliminating the need for batteries.[12]

In electronics, nanotechnology would allow the creation of ever-smaller computers and sensors, leading to integrated packages that could sense, discriminate, decide, report information, and provide control input to other devices. For example, tires that sense the surface over which they are traveling could automatically adjust tire pressure to maintain optimal traction.

Smart sensors could be used in single-chip chemical and biological agent laboratories that would be smaller, faster, and more accurate than current testing methods. They could also be attached to miniature disposable sensor platforms, allowing monitoring of a large battlespace at minimal cost, effort, and danger to soldiers.

In the more distant future, combining nanocomputers, sensors, and nanomechanical architectures into one system would make possible autonomously targeted and guided projectiles, such as bullets and rockets. Nanotechnology could also improve communications and information processing, whether on the battlefield or with the Oval Office, through microscopic computers, switches, lasers, mirrors, detectors, and other optical and electrical devices.

The laws of physics and optics change fundamentally at the near-atomic level. Instead of being masked by the manipulation of particles on the surface, materials can be changed at the optical electronic level. Materials that display one optical or electronic property at the macro level may display a different property at the nanometer level. Remarkable mechanisms become possible, such as negatively refractive optics that bend light at angles and in directions otherwise impossible.[13] Such devices could lead to the development of lenses that focus almost instantaneously and light-bending camouflage that changes as the solider or vehicle moves.

One theoretical and exotic use of nanophotonic materials would be fiberoptic waveguides that actually strengthen the light beams passing through them. These could be used for long-distance, strategic-level communications systems or high-power narrow-beam lasers. With nanophotonics, optical computing, data storage, and signal processing become possible.

If the Defense Department is to remain a leader in exploiting nanotechnology, the Pentagon must ensure that it adequately understands how nanotechnology could be exploited for U.S. security and competitive advantage.

Homeland Security Applications. Only 0.25 percent of the government's 2004 funding for nanotechnology goes to the Department of Homeland Security. This is inadequate given that nanotechnology could play a major role in advancing the DHS capabilities. Nanomaterials could be used to create highly sensitive sensors capable of detecting hazardous materials in the air. For example, carbon-based nanotubes are relatively inexpensive and consume minimal power.

Other areas of nanotechnology pertinent to homeland security are emergency responder devices. Lightweight communications systems that require almost no power and have a large contact radius would give rescuers more flexibility. Nanotech robots could be used to disarm bombs and save trapped victims, reducing the risks to rescue workers.

Enlisting the Private Sector

In the United States, the commercial nanoscience industry is composed of traditional industrial sectors, newly formed startups, *Fortune* 500 companies, and academic research institutions. These groups will play a significant role in future developments of nanotechnology. The most recent analysis estimates that nanoscience will produce $2.6 trillion in economic output by 2015.[14]

12. American Association for the Advancement of Science, "Nanogenerators May Spark Miniature Machines," *EurekAlert!* April 13, 2006, at *www.eurekalert.org/pub_releases/2006-04/nsf-nms041306.php* (February 26, 2007).
13. "OIDA's Huff Discusses Nanophotonics in Keynote Address at NGC2007," *Business Wire*, March 16, 2007, at *www.allbusiness.com/services/business-services/4305830-1.html* (September 13, 2007).
14. Murdock, prepared statement, p. 41.

The U.S. is currently the global leader in nanotechnology. The National Nanotechnology Initiative coordinates over $1 billion in annual federal research and grants. Total U.S. public and private spending on nanotechnology research and development totals about $3 billion annually, or one-third of the estimated $9 billion that is spent worldwide.[15]

Global competition in nanotechnology is fierce, and many countries are challenging the U.S.'s supremacy, specifically in the European Union and Asia. The EU is strengthening its research and development capabilities by promoting partnerships among companies and universities through its Nanosciences/Nanotechnology Action Plan for Europe. The Chinese government has implemented initiatives that employ over twice as many engineers as are working in nanotechnology in the U.S.[16] Thus, U.S. government-sponsored research is still vital if America is to remain a global leader in the national security applications of nanotechnology.

Toward the Future

Congress and the Administration have done much to encourage the development of nanoscience. The challenge is to maintain this momentum, facilitating commercial innovation and the application of new advances for national security purposes. A few key initiatives would bolster America's global leadership in the science of small things.

Smarter Funding. In the near term, government research and development funds will continue to play a critical role in jump-starting national security innovations in nanotechnology. Congress should continue to provide strong support for nanoscience research programs in the Department of Defense and other federal agencies that support national security purposes.

Big Industry is currently averse to risk and is not providing the innovations needed for national security. In fact, investments in the private sector have been concentrated in just a few mature nanotech companies. In the first quarter of 2005, almost all of the venture capital invested in the nanotech industry went to four companies: NanoTex ($33 millon), Nanomix ($17 million), Nantero ($17 million), and NanoOpto ($12 million).[17]

The NNI needs to focus grants on the companies willing to pursue national security research. In doing so, however, it must walk a fine line between fostering cutting-edge technology advances and establishing a form of corporate welfare. Funding of the private sector should be limited to projects with such prohibitive risk and entry costs that companies would otherwise be unable to pursue them on their own.

Interagency Coordination. The DOD recently cited maintaining a consistent vision and stable funding as critical to future nanotechnology research and development.[18] Although federal agencies continue to coordinate through the NNI, each agency retains full control of its own budget decisions and sets its own research priorities.

The National Academy of Sciences has concluded that the "NNI is successfully establishing R&D programs with wider impact than could have been expected from separate agency funding without coordination." Increased coordination within the NNI would produce a centralized list of priorities and leverage resources even more effectively.[19]

Reform of Visa Issuance and Management. Congress needs to promote policies that continue to bring the best and the brightest in nanotechnology to study and work in the United States. Current visa policies are making it increasingly difficult to recruit students and scientists and to hold scientific conferences in the United States.

---

15. U.S. Department of State, Bureau of International Information Programs, "United States Leads Globe in Nanotechnology Research, Report Says," May 23, 2005, p. 1, at *http://usinfo.state.gov/xarchives/display.html?p=washfile-english&y=2005&m=May&x=20050523152217lcnirellep0.8238794* (September 14, 2007).
16. Jim O'Conner, "Motorola Trailblazing the Nanotechnology Frontier," testimony before the Subcommittee on Research, Committee on Science, U.S. House of Representatives, June 29, 2005, at *http://gop.science.house.gov/hearings/research05/june29/oconnor.pdf* (September 14, 2007).
17. Murdock, prepared statement, p. 48.
18. U.S. Department of Defense, "Defense Nanotechnology Research and Development Program," April 27, 2007, at *www.fas.org/irp/agency/dod/nano2007.pdf* (August 3, 2007).
19. National Research Council, Committee to Review the National Nanotechnology Initiative, *A Matter of Size: Triennial Review of the National Nanotechnology Initiative* (Washington, D.C.: National Academies Press, 2006), p. 6, at *http://books.nap.edu/openbook.php?record_id=11752&page=6* (September 12, 2007).

The nation's security and competitiveness relies heavily on people's ability to travel to the United States, but the current visa system is unnecessarily challenging, depriving the United States of many of the world's best and brightest scientists, students, and entrepreneurs. Long wait times for personal interviews are among the most frequently cited factors that make travel to the United States difficult.

Congress should end the requirement for a personal interview with virtually every non-immigration visa applicant and restore the Secretary of State's ability to waive personal interview requirements. The U.S. should also establish electronic visa applications to largely eliminate the cost of traveling to consulates and should reduce processing times to 30 days or less. All of these reforms could be implemented in a manner that makes international travel both more convenient and more secure.[20]

Safety and Environmental Issues. Congress should consider promoting the application of nanotechnologies for national security purposes in a manner similar to the provisions of the SAFETY Act, which facilitates the adoption of new capabilities for homeland security purposes.[21] Unlike in other industries such as biotechnology, there is no legal framework to guide responsibility and liability in nanotechnology.

While nanotechnology has advanced rapidly in many fields, health and safety issues have lagged behind. Among the many concerns with nanotechnology are the possible toxicity of nanoparticles and their potential to self-replicate.[22] These hazards are not only public safety concerns, but also risks that are driving away many potential investors and companies.

Congress should establish clear legal guidelines for responsibility and liability in nanotechnology research and development with respect to national security requirements.

Conclusion

Nanotechnology promises to revolutionize many fields and industries and to increase military operational capabilities. Congress and the Administration should not only be aware of this growing field, but also ensure that the private sector—which is rightly making the largest investment in basic research and product development—remains competitive. Congress could take steps now to make this happen.

First published as Heritage Foundation Backgrounder *No. 2071, September 21, 2007.*

20. James Jay Carafano, Brian C. Goebel, and Josh Kussman, "Coming to America: Initiatives for Better, Faster, and More Secure Visas," Heritage Foundation *Backgrounder* No. 1976, September 29, 2006, at *www.heritage.org/Research/NationalSecurity/bg1976.cfm*.
21. In 2002, Congress enacted the Support Anti-Terrorism by Fostering Effective Technologies (SAFETY) Act to encourage companies to continue researching and developing biotechnologies vital to homeland security by protecting companies from litigation if their products fail during a terrorist attack or are harmfully employed by terrorists. The DHS has shown some success in implementing the legislation and granting SAFETY Act protections to goods and services that are employed to prevent or respond to terrorist threats. However, companies do not enjoy similar protections from other countries when the technologies are deployed outside the United States or adopted by U.S. friends and allies.
22. U.S. Department of Labor, Occupational Safety and Health Administration, National Advisory Committee on Occupational Safety and Health, "Minutes of December 8, 2004 Meeting," at *www.osha.gov/dop/nacosh/nagenda041204.html* (February 26, 2007).

Chapter 5

The Pentagon's Robots: Arming the Future

James Jay Carafano, Ph.D., and Andrew Gudgel

Robots have stepped out of the science fiction pages and onto the battlefield. Thousands are deployed in Iraq and Afghanistan, supporting military operations on land, at sea, and in the air. Some robots cost as little as several thousand dollars each. Controlled remotely by soldiers, sailors, and airmen, they perform tasks such as disarming roadside bombs, scouting dangerous territory, and patrolling the sky.

As technology advances, robots will become increasingly autonomous of human supervision, providing new cutting-edge national security applications that could give the U.S. military significant competitive advantages. Robots on the battlefield will not bring an age of "bloodless" push-button warfare nor provide "silver-bullet" solutions to every combat challenge, but they can offer U.S. forces tactical advantages for outfighting both conventional (regular armed forces) and unconventional (e.g., terrorists and insurgents) enemies.

The U.S. government should continue prudent investments in robotic technologies, particularly for autonomous operations—an area of research not adequately supported by commercial research and development. Congress can help by establishing a framework that will facilitate national security research and development programs and by addressing concerns about the risk to humans with legislative guidelines for liability and safety issues in research, development, and procurement.

When the Future Arrives

The challenge of imagining the future of war is often a question of timing. Promising technologies are often derided or dismissed simply because their proponents' imaginations outpace the capacity of science and technology to deliver.

World War I offers a case in point. The nascent technologies described by 19th century science fiction writers and military futurists were not ready for prime time and incapable of breaking the gridlock of attrition warfare. While H. G. Wells and Jules Verne are often praised for their foresight in envisioning the proliferation of weapons like tanks, airplanes, and submarines, the machines that they described were little more than fanciful, completely out of the reach of foreseeable technologies. Military writers were more conservative in their appreciation of how machines would change warfare, but even they missed the mark.[1]

In World War I, the future arrived too fast, before new technologies had matured to the point that they could reshape the face of conflict. If World War I had been avoided and the great powers had not tested these new technologies until the 1940s when they were more mature, both science fiction writers and military futurists might have been much closer to making more accurate guesses.

Timing may not be everything, but it can dramatically affect the process of turning imaginative vision into reality. This may turn out to be the case for robotics. The vision of robots in combat, popularized in science fiction since the cliffhanger movie serials of the 1930s, never came to fruition in the succeeding decades. The Pentagon had little

1. Antulio J. Echeverria II, *Imagining Future War: The West's Technological Revolution and Visions of Wars to Come: 1880–1914* (Westport, Conn.: Praeger Security International, 2007), pp. 95–96.

to show after decades of research, leading the promise of robotics in battle to be largely derided and dismissed as a failure of overly exuberant imagination.

Dismissing military robotics as a failed future vision may be premature. The armed services' increasing expertise in robotic technologies, the effectiveness of robots in recent military operations, and promising new research developments suggest that artificial warriors may yet prove to be the next big thing.

The Pentagon's New Weapons

After decades of military research and development, robotic technologies have finally matured to where they present significant national security applications. Their effectiveness is most noticeable in environments that are ill-suited to manned warfare.

Robots have proven most efficient and cost-effective in combat tasks involving the three Ds—dull, dirty, and dangerous. Dull assignments are those that require routine functions such as monitoring a bridge crossing site. Dirty jobs are performed in harsh environmental conditions, such as searching contaminated areas. Dangerous missions involve tasks in which humans could suffer physical harm, such as disarming an improvised explosive device (IED). Currently, the U.S. military employs three different robotic platforms for three-D operations:

Unmanned Aerial Vehicles. Unmanned aerial vehicles (UAVs) have emerged as the most frequently employed robotic platform on the battlefield. Ironically, the failure of numerous programs during the Cold War initially earned them the reputation of "'vampires' of military acquisition," "sucking" up research and development dollars without delivering any practical utility. That began to change when UAVs first proved their effectiveness during the first Gulf War (1991) "when the low-tech, short-range Pioneer [short-range reconnaissance drone resembling a large model airplane]," as J. R. Wilson points out, "helped to identify artillery and naval gun targets, detected high-speed Iraqi patrol boats, and even became the first 'robot' to which enemy combatants surrendered."[2]

Throughout the 1990s, all of the military services developed new applications for UAVs. Many of the new capabilities were battle-tested in combat operations in Bosnia, Kosovo, Afghanistan, and Iraq. Today, over 700 types of UAVs support U.S. military forces.[3] The armed services employ about 3,000 individual UAVs in Iraq alone.[4]

The Predator—a medium-altitude, long-endurance, remotely piloted aircraft—stands out as the most notable UAV in military service. Initially used for reconnaissance, the Predator has also been armed with Hellfire air-to-ground missiles and has been used to conduct combat missions in Iraq and Afghanistan. Other UAVs range from the hand-launched Raven, used by ground troops, to Global Hawk, a high-altitude, long-range, long-endurance platform with a wingspan as wide as a commercial airliner that can conduct surveillance missions anywhere in the world.

UAVs are being used more heavily because of their increasing capacity to loiter over the battlefield for a long time and provide a persistent presence. For example, the Predator B can stay airborne for a day or more. The current generation of UAVs can track specific targets for extended periods and can attack the target or relay information to ground troops. Insurgents in Iraq have become so wary of UAVs that they are reluctant to loiter in any open place for more than a few minutes. Both Americans and their enemies now see UAVs as a ubiquitous presence on the battlefield.

Unmanned Underwater Vehicles. The Navy is developing unmanned underwater vehicles (UUVs) to hunt and destroy sea-based mines. Remus, a three-foot-long robot that can detect mines underwater, is being retrofitted with an explosive charge so that it can attach itself to and detonate underwater bombs and mines. Remus also carries a sensor payload that allows it to identify entities in the surrounding waters.

The Navy has tested Remus in real missions, using the robot to clear mines in the port of Um Qasr, Iraq, in 2003. Remus robots searched nearly a square-mile area and removed a number of mines in 16 hours. Divers would have needed 21 days to complete the same mission.[5]

---

2. J. R. Wilson, "A New Generation of Unmanned Aircraft," *Aerospace America*, January 2007, at *www.aiaa.org/aerospace/images/articleimages/pdf/AA_Jan07_WIL.pdf* (August 9, 2007).
3. *Ibid.*
4. Tim Mahon, "In Harm's Way: New Missions, Technology Shape UAV Combat Tactics," *C4ISR*, October 2006.

Unmanned Ground Vehicles. Unmanned ground vehicles have played a critical role in combating IEDs, the deadliest weapon used against U.S. troops in Iraq. Roadside bombs have accounted for more than 70 percent of U.S. casualties.[6] The Pentagon's Joint Robotics Program, established in 1990 to oversee robotics technologies, established a plan to acquire "small, man-portable robotics systems" equipped with explosives ordnance disposal (EOD) tools that would be "fielded as quickly as possible to assist EOD forces in the mission to defeat IEDs."[7]

Initially deployed to Afghanistan to search caves for weapons caches, the first small unmanned ground vehicles (SUGVs) arrived in Iraq in April 2004. One of the early SUGV models was the PackBot, a 30-pound robot that is small enough to fit in a backpack. It is also extraordinarily rugged. A PackBot can be thrown from the second story of a building and still work. PackBot has recently been equipped with a manipulator arm with a two-meter reach and a camera that allows the operator to remotely identify and disarm bombs.

Today, SUGVs are integral to ground operations. According to press reports, the military has deployed "nearly 5,000 robots in Iraq and Afghanistan, up from 150 in 2004.... Soldiers use them to search caves and buildings for insurgents, detect mines, and ferret out roadside bombs."[8] By the end of 2005, robots reportedly had rendered safe or exploded more than 1,000 IEDs.[9]

In addition to their utility, SGUVS are relatively inexpensive compared to other robots. Predators cost between $4.5 million and $8.3 million each, UUVs about $5.5 million, and PackBots between $80,000 and $150,000.[10] This low cost has enabled rapid procurement, deployment, and adoption of ground-based robots.

Empowering New Systems

Currently deployed robots are teleoperated, meaning that a human must direct their every move. However, robotic technology is moving toward more autonomous action. Autonomy will enable robots to sense, react, and even make decisions without human intervention. On the battlefield, these capabilities will transform robots from adjunct assets to independent combat platforms that can ferry supplies, search out and interpret intelligence for soldiers, make critical decisions with the most up-to-date information, guard roads and supplies, hunt enemy forces, and even engage in combat.

To achieve autonomy, research is focusing on three core aspects: sensors, cognition, and networking.

Sensing the Environment. Sensors allow robots to observe the world around them. Many robot designs use sonar, laser range finders, television cameras, and microphones. For example, the Massachusetts Institute of Technology and the Naval Research Laboratory are conducting extensive research into map-creation by robots to enable them to guide themselves.[11] A NASA laboratory is investigating the use of infrared sensors on a flexible outer body, allowing the robot to sense objects in its path.[12] Researchers at the University of Nebraska are developing a system to give a robot a sense of touch that equals that of the human finger.[13] These efforts are only a few of the entire spectrum of projects being undertaken by government and university research centers.

---

5. Associated Press, "Military Increasingly Looking to Robots to Clear Waterways of Dangerous Mines," *International Herald Tribune*, July 27, 2007, at *www.iht.com/articles/ap/2007/07/27/america/NA-GEN-US-Mine-Destroying-Robots.php* (August 14, 2007).
6. Associated Press, "Explosive-Sniffing Robots Headed to Iraq to Help U.S. Military Counter Deadly Roadside Bombs," *Niagara Gazette*, March 29, 2007, at *www.niagara-gazette.com/newtoday/gnnnewtoday_story_088144250.html* (August 9, 2007).
7. *Ibid.*, pp. 20–21.
8. Associated Press, "Explosive-Sniffing Robots Headed to Iraq."
9. *Ibid.*
10. Strategy Page, "Buying Predator Bs," February 8, 2006, at *www.strategypage.com/htmw/htproc/articles/20060208.aspx* (August 15, 2007); "2 REMUS 600 Systems for UK Royal Navy," *Defense Industry Daily*, September 23, 2007, at *www.defenseindustrydaily.com/2-remus-600-systems-for-uk-royal-navy-03860* (October 4, 2007); and Kris Osborn, "U.S. Wants 3,000 New Robots for War," *Defense News*, August 13, 2007, at *http://defensenews.com/story.php?F=2956107&C=thisweek* (August 14, 2007).
11. John J. Leonard, speech at program on "Robots: The Future is Here," audio file, The Heritage Foundation, June 5, 2006, at *www.heritage.org/Press/Events/ev060506a.cfm* (December 13, 2007), and U.S. Naval Research Laboratory, "Natural Interface and Control for a Segway RMP Robot," at *www.nrl.navy.mil/aic/iss/aas/SegwayRMP.php* (June 19, 2006).
12. Lori Keesey, "High-Tech Robot Skin," National Aeronautics and Space Administration, May 11, 2005, at *www.nasa.gov/vision/earth/everydaylife/vladskin.html* (June 6, 2006).

To encourage the development of self-guiding systems, the Defense Advanced Research Projects Agency (DARPA) has established the Grand Challenge, a competition for robotic vehicles. The goal of the race is to identify technologies that will enable robots to navigate complex terrain autonomously over a long distance. In the first Grand Challenge in 2004, not a single team completed the 150-mile course. The most prevalent difficulty was the robots' inability to navigate around detected obstacles while maintaining their GPS-derived locations. In the 2005 race, participants were able to surmount this critical problem. Six vehicles completed a 132-mile course. In November 2007, DARPA sponsored a 60-mile contest in an urban environment.[14]

Cognitive Action. To streamline robot–human interactions, researchers must develop machines capable of reasoning like human beings.[15] Autonomous robots must be capable of learning and making decisions. In dealing with humans, the robot will need not only to reason, but also to have cognitive skills, such as being able to follow an ambiguous order that requires intuitively understanding what the command means.

Evolutionary robotics is a newly emerging field of robotic design in which a machine system works out a solution and then repeats the process until the robot determines the most efficient process. The solution then guides the control system in operating the robot's physical attributes, such as walking.[16] Such innovations may presage the deployment of autonomous robots.

To maintain a level of control over autonomous robots, the military services are investigating "variable autonomy," combining aspects of autonomy and human control.[17] The Naval Research Lab is researching human control of robots through voice commands and hand movements.[18]

Network-Friendly. It is essential for robots to communicate and work together with the surrounding humans. In 2001, the Pentagon released the Joint Architecture for Unmanned Systems protocols to standardize communications software for unmanned systems. With these standards, systems can be configured to match a variety of human–machine environments in which robots, soldiers, civilians, and enemy combatants may share the same battlespace.

Developers of the Army's Future Combat Systems (FCS) are using the Joint Architecture for Unmanned Systems to develop interoperable programming for FCS robotic platforms. Robots will be operated under an umbrella of systems that will manage FCS, including the Warfighter Information Network-Tactical (WIN-T). Under WIN-T's Joint Tactical Radio and Ground Mobile Radio systems, soldiers and robots will be able to communicate via software networks that provide multichannel voice, data, imagery, and video communications.[19]

The Next Generation

Autonomous robots are closer to real combat capabilities. The Army will soon field the Mobile Detection Assessment Response System (MDARS), a semi-autonomous security-guard robot. This nine-foot, 3,500-pound robot can travel up to 20 miles per hour using inertial and satellite navigation and can scan the surrounding environment with radar and infrared beams. Using its on-board sensors, MDARS will able to conduct independent patrol or sentry duty, avoiding obstacles and detecting intruders up to 300 meters away.[20]

13. Rebecca Morelle, "Robot Device Mimics Human Touch," BBC News, June 8, 2006, at *http://news.bbc.co.uk/2/hi/science/nature/5056434.stm* (June 12, 2006).
14. Press release, "DARPA Announces Third Grand Challenge: Urban Challenge Moves to the City," U.S. Department of Defense, Defense Advanced Research Projects Agency, May 1, 2006, at *www.darpa.mil/grandchallenge/docs/urb_challenge_announce.pdf* (June 23, 2006).
15. John Bluck, "NASA Developing Robots with Human Traits," National Aeronautics and Space Administration, May 24, 2005, at *www.nasa.gov/vision/universe/roboticexplorers/robots_human_coop.html* (June 19, 2006).
16. Andrew Nelson, "Evolutionary Robotics," at *www.evolutionaryrobotics.org* (June 23, 2006).
17. U.S. Army Research Laboratory, "Robotics Alliance," modified July 28, 2006, at *www.arl.army.mil/main/Main/default.cfm?Action=93&Page=156* (June 16, 2006), and U.S. Naval Research Laboratory, "Adaptive Systems," at *www.nrl.navy.mil/aic/as/index.php* (September 25, 2007).
18. U.S. Naval Research Laboratory, "Human/Robot Interaction," at *www.nrl.navy.mil/aic/iss/aas/IntelligentHumanRobotInteractions.php* (October 17, 2007).
19. Doug Beizer, "Talk About an Evolution," *Washington Technology*, August 6, 2007, at *www.washingtontechnology.com/print/22_14/31155-1.html* (August 29, 2007).
20. Kris Osborn, "Army Set to Field Autonomous Security-Guard Robot at Bases," *Marine Corps Times*, July 16, 2007.

The Army is also developing the semi-autonomous Multifunctional Utility Logistics and Equipment (MULE) vehicle, a six-wheeled, 20-foot robot that can autonomously traverse rugged terrain, carrying 1,900 pounds of equipment.[21] MULEs will perform convoy operations and support ground assaults. Currently, one-fourth of the planned systems for FCS will be robotic, including both remotely piloted air and ground vehicles.[22]

The Navy recently tested two UUVs as part of the Long Term Mine Reconnaissance System. Submerged submarines launched and recovered the vehicles through their torpedo tubes.[23] MANTA, a proposed underwater system, would detach itself from a submarine's hull and be able to deploy torpedoes or small UUVs. These remote robots and weapons could extend a submarine's range into shallow waters that the boats cannot traverse.[24]

In the air, prototypes for fully autonomous UAVs are being developed. In August 2005, Boeing Corporation successfully tested two X-45A unmanned combat aerial vehicles (UCAVs). In these tests, the two X-45As took off, planned a route, evaded threats, and reached a designated target.[25] One recent study concluded that UCAVs offer significant potential for extended operations at long range.[26]

Continuing Development

Congress and the Administration should continue to promote the development of robotics. While the private sector is actively researching the application of robotics to a wide range of uses from building cars to sweeping floors, commercial research is not sufficiently focused on national security needs to develop the cutting-edge robotic applications that the military needs. Thus, in the decade ahead, commercial off-the-shelf products are unlikely to provide the Pentagon with dramatic new capabilities. Congress should therefore encourage and support national security robotic research.

Specifically, a few key initiatives would bolster the development and utilization of robots.

- **Interagency coordination.** Currently, each military service prefers separately managed programs geared to its individual needs. However, the Government Accountability Office (GAO) concluded that the military could save money and resources by combining the services' 13 UAV programs. The GAO cited the Fire Scout UAV program as an example of the potential of interagency cooperation. The Army and Navy are pursuing common components under the Navy contract, saving an estimated $200 million in research and development costs.[27]

  The Department of Defense should accelerate this type of cooperation, promoting common configurations, harmonizing performance requirements, and drawing on common testing, evaluation, and support. Cooperation should extend to the Department of Homeland Security, supporting the UAV requirements of the Coast Guard and Customs and Border Protection.

- **Continued funding.** Congress should continue to fund robotic research, development, and procurement across the board. Their success on the battlefield merits the resources necessary to meet the Pentagon's goal of replacing one-third of its armed vehicles and weaponry with robots by 2015.[28]

---

21. Kris Osborn, "Multitask MULE: Semi-Autonomous Robot Moves, Fights, Transports with Troops," *Defense News*, April 30, 2007.
22. U.S. Army, "Future Combat Systems," Web site, September 19, 2005, at *www.army.mil/fcs/index.html* (October 17, 2007).
23. Mark O. Piggott, "USS Scranton Completes Successful UUV Test," *Navy Newsstand*, March 9, 2006, at *www.news.navy.mil/search/display.asp?story_id=22618* (June 26, 2006).
24. Edward C. Whitman, "Unmanned Underwater Vehicles: Beneath the Wave of the Future," *Undersea Warfare*, Vol. 4, Issue 3 (Summer 2002), at *www.navy.mil/navydata/cno/n87/usw/issue_15/wave.html* (June 26, 2006).
25. News release, "Two Boeing X-45As Complete Graduation Combat Demonstration," Boeing, August 10, 2005, at *www.boeing.com/news/releases/2005/q3/nr_050810m.html* (December 17, 2007).
26. Thomas P. Erhard and Robert O. Work, "The Unmanned Combat Air System Carrier Demonstration Program: A New Dawn for Naval Aviation," Center for Strategic and Budgetary Assessments *Backgrounder*, May 10, 2007, at *www.csbaonline.org/4Publications/PubLibrary/B.20070510.The_Unmanned_Comba/B.20070510.The_Unmanned_Comba.pdf* (December 5, 2007).
27. "Collaboration Key to ISR Programs," *C4ISR*, June 1, 2007.
28. "Robot Wars," *The Economist*, April 17, 2007, at *www.economist.com/science/tq/displaystory.cfm?story_id=9028041* (August 18, 2007).

- **Establishing a legislative framework.** As autonomous robots come closer to becoming reality, safety will be a major issue. Robots, especially on the battlefield, should have "safety-critical computing" to maintain human control and to ensure they do not behave in unintended or dangerous ways.

  Public policy needs to recognize these dangers but to address them in a manner that does not unduly hold back research that could bring dramatic new capabilities to the marketplace and further national security. Congress can speed the development of autonomous robotics by creating a legal framework in which research can occur without unnecessary restraint. The framework should include input from the Defense Department, the Department of Homeland Security, and NASA.

A Window of Advantage

America's capability to seize and maintain a strategic advantage in robotic national security applications could be lost without sustained and focused commitment from the Administration and Congress. Congress should provide adequate funding, encourage increased coordination, and craft policies that encourage prudent investment in robotic technology. Congress can facilitate national security research and development programs by establishing a framework that addresses concerns about the risk to humans from autonomous robots.

First published as Heritage Foundation Backgrounder *No. 2093, December 19, 2007.*

Appendix 1

Realizing the Rice-Chertoff Vision: A National-Interest-Based Visa Policy for the United States

Our nation's ability to build and sustain strong diplomatic, academic, business, and cultural ties with other countries—ties critical to our leadership, security, and competitiveness—relies heavily on people's ability to travel to the United States. Without a system in place to ensure this essential flow, the United States risks losing its status as the destination of choice for the best and brightest in academia, business, and science. Yet, despite improvements in the visa process, travel to the United States remains unnecessarily challenging. The time has come for more fundamental reforms—reforms that address legitimate security concerns *and* keep our nation a welcoming nation. The United States needs a visa policy that keeps us safe, prosperous, and free. Our organizations have come together to urge Congress and the Executive Branch to take the following actions:

Congress must:

Restore to the Secretary of State the authority to grant U.S. consulates discretion to waive the personal interview requirement based on risk assessment.

In 2004, Congress unwisely wrote into law temporary State Department guidance requiring consular posts to conduct personal interviews of virtually all nonimmigrant visa applicants. In most cases these interviews add little security, and actually make us less safe as officers rush to complete interviews and are not focusing their time and efforts on truly suspicious travelers. The expense, inconvenience, and long wait times for personal interviews are among the most frequently cited factors that make travel to the United States unpopular, particularly in large, high-demand countries. Available technology and sophisticated risk-assessment techniques make interviews unnecessary in many cases. Congress should restore to the Secretary of State the authority to grant U.S. consulates discretion to waive the personal interview requirement, subject to State-DHS guidance, and according to plans submitted by each consulate for State Department approval.

Strengthen and expand the Visa Waiver Program.

The Visa Waiver Program allows most visitors from 27 countries who carry a valid passport to enter the United States without a visa for up to 90 days. Participating countries must meet strict eligibility standards based on U.S. diplomatic, immigration-enforcement, and national security interests. In recent years, about one-half of all nonimmigrant admissions to the United States have been VWP travelers. VWP has become a vital mechanism for facilitating legitimate travel, establishing strong diplomatic ties, sustaining economic growth, and enhancing our nation's security. This successful program should be strengthened and expanded in a manner that enhances security and increases opportunities for travel between the United States and its friends and allies.

Exercise vigorous oversight of Executive Branch implementation of the Rice-Chertoff vision, especially the recommendations listed in the following section.

Alliance for International Educational and Cultural Exchange. The Heritage Foundation. NAFSA Association of International Educators. NFTC NATIONAL FOREIGN TRADE COUNCIL, INC.

Realizing the Rice-Chertoff Vision: A National-Interest-Based Visa Policy for the United States

The Executive Branch must:

Articulate a clear, operational visa policy that fully realizes the Rice-Chertoff vision.

Despite the 2003 State-DHS memorandum of understanding on visa processing, and the 2006 joint-vision statement by Secretaries Rice and Chertoff, relationships between the two departments remain plagued by serious disconnects, which severely affect travel. More important, the very positive vision articulated by the secretaries—truly balancing security and openness—has not been achieved at the operational level, where that balance must be forged. In this operational policy vacuum, law enforcement authorities have an effective veto, and the essential balance is lost. The agencies must:

- Develop and implement a comprehensive human capital workforce plan for the appropriate selection, training, and supervision of all those whose contact with the public impacts America's image abroad, including consular, immigration, and customs officers.
- Implement plans to elevate DHS's assistant secretary for policy to an undersecretary, and fully staff the Office of Policy, to provide strong leadership to the former Immigration and Naturalization Service.
- Issue strong operational guidance to all consular posts to eliminate inconsistencies in visa processing, and hold posts accountable through regular reviews.
- Recognize that the conduct of visa policy and the treatment of international visitors at ports of entry *is* public diplomacy, and ensure that these procedures support our public diplomacy goals.

Improve efficiency, transparency, and reliability in the visa process.

We give the State Department credit for adding 570 new consular officers since 9/11, increasing the use of electronic visa processing, improving consular training, enhancing the information available to visa applicants, creatively adjusting its procedures to cope with an enormous workload, and cutting down the time required for security clearances for scientists. Yet more can and should be done, specifically:

- Establish a "Trusted Traveler" program to expedite approval for all frequent travelers willing to submit to extensive background checks in advance, and who have a prior history of visa approval.
- Implement a fully electronic ("paperless") application process to allow consulates to undertake necessary additional screening prior to the interview.
- Further improve the security clearance process for scientists to reduce the overall visa processing time to no more than 30 days. Establish a special review process to resolve applications that take longer than 45 days to process.
- Enhance consular resources to respond better to shifts in visa demand.
- Restore domestic visa-revalidation procedures that were available to non-immigrants with employment-based visas before 2004.
- Develop an efficient system for providing social security numbers at the port of entry for those visitors eligible to work, as is already done for immigrants.

January 31, 2007

Appendix 2

Participants in The Heritage Foundation's Public Events on Science and Technology

Nanotechnology: Changing the Face of National Security

March 29, 2006

Featuring:

- Ravi Athale, Ph.D.
  Principal Communications Engineer, Center for Innovative Computing and Informatics, MITRE Corporation
- James Murday, Ph.D.
  Executive Secretary, Nanoscale Science Engineering and Technology Subcommittee of the National Science and Technology Council
- John Parmentola, Ph.D.
  Director for Research and Laboratory Management,Office of the Assistant Secretary of the Army (Acquisition, Logistics, and Technology)

Robots: The Future is Here

June 5, 2006

Featuring:

- Helen Greiner
  Co-Founder and Chairman, iRobot
- John J. Leonard
  Professor of Mechanical and Ocean Engineering, Massachusetts Institute of Technology
- Vladimir J. Lumelsky, Ph.D.
  Technologist, Goddard Space Flight Center, National Aeronautics and Space Administration
- Stephen Welby
  Director, Tactical Technology Office, Defense Advanced Research Projects Agency

Biotechnology: Empowering the Long War

October 27, 2006

Featuring:

- Peggy Binzer
  Counsel, McKenna Long & Aldridge LLP
- David Siegrist, Ph.D.
  Senior Research Fellow, Potomac Institute
- Morley Stone, Ph.D.
  Branch Chief, Hardened Materials & Manufacturing Directorate, Air Force Research Laboratory/Wright-Patterson Air Force Base, Ohio

Future Computing: Shaping National Security Policy

November 06, 2006

Featuring:

- Jesús Mena
  Chief Strategy Officer, InferX Corporation
- Marcus H. Sachs, P.E.
  Deputy Director, Computer Science Laboratory, SRI International
- David Strand
  Vice President, Information Technology, ECD Ovonics

Competitive Technologies for National Security Policy: Obstacles and Options for Staying Ahead

December 15, 2006

Featuring:

- Marlene Johnson
  Executive Director and CEO, NAFSA: Association of International Educators
- Clarence W. (Wes) Kitchens
  Technical Fellow, Science Applications International Corporation
- Kei Koizumi
  Director, R&D Budget and Policy Program, American Association for the Advancement of Science