Heritage Lectures
Published by The Heritage Foundation

No. 885
Delivered January 17, 2005

June 6, 2005

# The Future of Anti-Terrorism Technologies

*James Jay Carafano, Ph.D.*

For most of the 20th century, counterterrorism and technology coexisted in a one-sided relationship. In large part, law enforcement and the military adapted the technologies that were commercially available to their needs.

That relationship may simply be inadequate for addressing the challenges of the 21st century. Meeting the test of terrorism will likely require a more proactive approach to technological innovation—betting on the future: formulating clear requirements, prioritizing needs, establishing cooperative means to foster the development of technologies, and building the human and financial capital programs necessary to transition and sustain them as effective anti-terrorism tools.

In my remarks today, I want to list my "big bets" for the future—six technologies that I believe offer the greatest promise for providing significant advantages in combating terrorism—and address as well the challenge to turning the potential of technology into concrete capabilities.

## Why Worry?

Traditional means of developing law enforcement technologies are simply inadequate to deal with today's strategic realities, and the war on global terrorism should top our list of concerns.

While every country may not agree on a definition of terrorism, that does not mean that it does not exist and does not represent a terrible threat to world peace. Nor do terrorists seem concerned about definitional nuances. They have decided they are most cer-

## Talking Points

- The global war on terrorism, much like the Cold War, will be a long, protracted conflict because, despite the preponderance of power held by the nations united in their commitment to combat terrorism, we will not be able to come directly to grips with the enemy.
- Developing technologies that leap ahead of the terrorists requires vision and strategy, and a good strategy requires hard choices. It begins by establishing criteria for selecting the most crucial technological investments.
- The obstacles to creating counterterrorism technologies that are practical and affordable and overmatch the threat of 21st century terrorism are daunting. Creating a vision of these future technologies, implementing initiatives that broaden the market and make it more predictable and dependable, and developing policies that will help to overcome the barriers to innovation are essential steps to harnessing technology to the future needs of law enforcement.

This paper, in its entirety, can be found at:
*www.heritage.org/research/homelanddefense/hl885.cfm*

Produced by the Kathryn and Shelby Cullom Davis
Institute for International Studies

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

Nothing written here is to be construed as necessarily reflecting the views of The Heritage Foundation or as an attempt to aid or hinder the passage of any bill before Congress.

tainly at war with us, and they think they are in a war they can win.

We are at war. In fact, the global war on terrorism will be like most wars. It will have casualties and sacrifices, victories, defeats, advances, and setbacks. Progress will not be determined by the outcome of individual battles or campaigns. It will, to a remarkable degree, look much like the Cold War. Like the Cold War, it will be a long, protracted conflict because, despite the preponderance of power held by the nations united in their commitment to combat terrorism, we will not be able to come directly to grips with the enemy—then because it risked nuclear war and annihilation, now because the enemy is too disparate and diffuse to be defeated in climactic battle. We are in another long war.

It is, however, a war of a different kind. There are no frontiers in 21st century national security. Distinguishing clear lines of responsibility between foreign and domestic security is a thing of the past.

Additionally, the age when only great powers can bring great powers to their knees is over. The specter of catastrophic terrorism that could threaten tens of thousands of lives and hundreds of billions of dollars in destruction will be an enduring concern. And if catastrophic terrorism is a threat to great countries, the prospects for smaller nations is even more daunting to imagine.

## Making Big Bets

Technology is, of course, not the only answer to addressing the specter of transnational terrorism, but the technological answers we have today are inadequate to deal with the scope and potential severity of the threat. Rather than adapting technologies to stay apace of evolving dangers and changing tactics, we need to get ahead of the terrorists and develop "overmatching" security systems that protect the public, safeguard their liberties, and leave travel and commerce unencumbered.

Developing technologies that leap ahead of the terrorists requires vision and strategy, and a good strategy requires hard choices. It begins by establishing criteria for selecting the most crucial technological investments. In my mind, there should be three:

- **Seeking** out technologies that can contribute to building a true national system that addresses all the challenges of terrorism from intelligence and early warning to domestic counterterrorism and response. It is unlikely that any country will have the resources it needs to address every security shortfall or law enforcement need. Thus, the first priority of a sound strategy should be to invest in technologies that best leverage all the existing capabilities that are available by integrating them into a cohesive system.
- **Adopting** technologies that get the "biggest bang for the buck." Spending a little research, development, and procurement resources on many things may not buy much of anything. Husbanding and targeting investments on the technologies that can provide the most security for the resources invested, ones that are the most flexible, ones that contribute to addressing a wide range of threats from kidnapping to catastrophic, is a better approach for stealing a march on the terrorists.
- **Reaching** for "breakthrough" technologies. Terrorist groups have limited resources and limited means; thus, they are quick to refine their methods, improving on time-tested techniques, or improvise, seeking out new ways to strike or new targets to attack. In response, law enforcement officials update their investigatory techniques or implement new security measures. Breaking the cycle of innovation and countermeasures between terrorism and counterterrorism calls for unprecedented innovation with which terrorists can simply not compete.

I want to suggest six candidates that meet these standards. They are (1) system integration technologies; (2) biometrics; (3) non-lethal weapons; (4) data mining and link analysis technologies; (5) nanotechnology; and (6) directed-energy weapons.

In some cases, these technologies are fairly mature but are just finding their counterterrorism niche. Others show great potential but will still require many years of research and development before they are ready to become operational. Yet all share a common characteristic: They offer significant potential solutions to addressing the most pressing counterterrorism concerns.

## "National" Technologies

My first two candidates clearly fit the first criterion for a counterterrorism technology strategy. They represent a family of capabilities that are essential for building national capabilities.

**System Integration Technologies.** One of the highest priorities for technological innovation ought to be simply getting the most out of the resources that are already available. That means adopting a new approach to counterterrorism operations as well as the enabling technologies to support it. This approach is often called "network-centric" operations.

Network-centric operations generate increased operational effectiveness by networking sensors, decision makers, law enforcement officials, and emergency responders to achieve shared awareness, increased speed of command, higher tempo of operations, greater efficiency, increased security and safety, reduced vulnerability to potential hostile action, and a degree of self-synchronization. In essence, this means linking knowledgeable entities from the local to the national levels in an integrated network that addresses counterterrorism missions ranging from intelligence and early warning to response and post-strike investigations and forensic analysis.

Systems integration technologies might produce significant efficiencies in terms of sharing skills, knowledge, and scarce high-value assets, building capacity and redundancy in a national counterterrorism system as well as gaining the synergy of providing a common operating picture to all law enforcement and emergency responders and being able to readily share information.[1]

Many of the technologies required to facilitate network-centric counterterrorism operations are already widely commercially available, including information technologies that facilitate passing high volumes of secure digital data, create *ad hoc* networks, integrate disparate databases, and link various communication systems over cable, fiber-optic, wireless, and satellite networks.

**Biometrics.** Identity is the linchpin of virtually all security and investigatory systems. Since September 11, 2001, there has been increased interest in using biometrics for identity verification, especially in the areas of visa and immigration documentation and government-issued identification card programs.[2]

Biometrics are recorded measures of a unique physical or behavioral characteristic of individuals. They are thought to be more reliable and more difficult to forget, lose, have stolen, falsified, or guessed since they are part of a person rather than an ID card, a personal identification number, or a password.

Biometrics can be used for verification or for identification. When a biometric is used to verify whether a person is who he or she claims to be, that verification is frequently referred to as "one-to-one" matching. Identification, by contrast, is known as "one-to-many" matching. In identification, a person's presented biometric is compared with all of the biometric templates within a database.

There are five major types of mature biometric technologies. They include iris recognition, hand geometry, fingerprint recognition, face recognition, and voice recognition.

- *Iris recognition* technology relies on the distinctly colored ring that surrounds the pupil of the eye.
- *Hand geometry* relies on measurements of the width, height, and length of the fingers; distances between joints; and the shape of knuckles.
- *Fingerprint recognition* technology is probably the most widely used and well-known biomet-

[1] *Army Science and Technology for Homeland Security*, Vol. II (Washington, D.C.: National Research Council, 2004), Chapter 4.

[2] Paul Rosenzweig, Alane Kochems, and Ari Schwartz, "Biometric Technologies: Security, Legal, and Policy Implications," Heritage Foundation *Legal Memorandum* No. 12, June 21, 2004, at *www.heritage.org/Research/HomelandDefense/lm12.cfm* (November 16, 2004).

ric. Fingerprint recognition relies on features found in the impressions made by distinct ridges on the fingertips.

- *Face recognition* technology identifies individuals by analyzing certain facial features such as the upper outlines of the eye sockets or sides of the mouth.
- *Voice recognition* technology identifies people based on the differences in the voice resulting from physiological differences and learned speaking habits.

Researchers are also looking for other useful biometrics. Some of these emerging technologies include vein scans, facial thermography, DNA matching, odor sensing, blood pulse measurements, skin pattern recognition, nailbed identification, gait recognition, and ear shape recognition. Biometrics like vein scanning are just becoming commercially available, while others, such as ear shape recognition, are recently started research projects.

## "Biggest Bang for the Buck" Technologies

The next two categories of candidate technologies that I want to mention fall under the second criterion for an aggressive counterterrorism technology strategy: getting the "biggest bang for the buck."

**Non-lethal Weapons.** One of the most significant challenges in the war on terrorism is that its battlefields are often the everyday world, where civilians and terrorists often stand side-by-side, where as much attention must be given to safeguarding lives and property as to disrupting, apprehending, or incapacitating terrorists. Non-lethal weapons may offer the military and law enforcement a new range of options for taking the battle to the terrorist without endangering others.

Non-lethal weapons are discriminate, explicitly designed and employed to incapacitate personnel or materiel while minimizing fatalities and undesired damage to property and environment. These weapons are actually a set of capabilities which have approximately three functions:

1. *Counterpersonnel,* which involves controlling crowds, incapacitating people, preventing access to specific areas, and removing people from facilities, buildings, or areas of operation;
2. *Countermaterial,* which may involve preventing vehicles, vessels, or aircraft from entering an area or disabling or neutralizing these means of transportation; and
3. *Countercapabilities,* which focuses on disabling or neutralizing facilities and systems, including those for weapons of mass destruction.

Today, non-lethal weapons technologies cover a broad spectrum, including areas related to the development of acoustics systems; chemicals (e.g., antitraction materials, dyes, markers, and malodorants); communications systems; electromagnetic and electrical systems; entanglement and other mechanical systems; information technologies; optical devices; non-penetrating projectiles and munitions; and many others.[3] It is also possible to combine non-lethal weapons with lethal ones or with electronic, psychological, and/or information warfare, making these other anti-terrorism tools more effective and discriminate.

Research by the U.S. military suggests four areas of non-lethal weapons development that show particular promise. They are:

1. Calmatives and malodorants for controlling crowds and clearing facilities, developed and applied in accordance with U.S. treaty obligations in the Chemical Weapons Convention;
2. Directed-energy systems beyond the vehicle-mounted active denial system (VMADS): high-power microwave (HPM) for stopping vehicles or vessels and solid-state lasers for advanced non-lethal weapons applications;
3. Novel and rapidly deployable marine barrier systems; and
4. Adaptation of unmanned or remotely piloted platforms and other sensors for non-lethal weapons applications, including intelligence collection and assessments.[4]

[3] Naval Studies Board, *An Assessment of Non-Lethal Weapons Science and Technology* (Washington, D.C.: National Academies Press, 2003), executive summary, at *www.nap.edu/execsumm/0309082889.html* (November 16, 2004).

**Data Mining and Link Analysis Technologies.** We live in a world that is becoming increasingly awash in commercial and government information. The trail of the terrorist, however, is often indistinguishable from a mass of bills, license applications, visa forms, census records, and telephone lists. Traditional law enforcement investigation techniques often begin with the identification of a suspected individual, followed by the laborious process of seeking out information related to that individual. As more and more information becomes available, this task becomes more and more problematic.

Technology, however, now has the potential to turn this challenge into an advantage. Rather than trying to narrow the scope of information that has to be looked at, data mining and link analysis technologies work best by exploiting larger and larger amounts of information.

Data mining is a "technology for analyzing historical and current online data to support informed decision making."[5] It involves identifying patterns and anomalies from the observation of vast datasets. The primary goals of data mining are prediction and description. Prediction involves using some variables or fields in the database to predict unknown or future values of other variables of interest, and description focuses on finding human-interpretable patterns describing the data. Description concerns increasing knowledge about a variable or dataset by finding related information.[6]

This second characteristic of data mining—description—is often referred to as link analysis. Whereas data mining attempts to identify anomalies in vast amounts of information, link analysis technologies sift through databases to find commonalties.

Link analysis is a slightly different twist on data mining. In preventing a terrorist attack, it is critical that one understands the relationships among individuals, organizations, and other entities which could be security threats. Link analysis is the process of analyzing the data surrounding the suspect relationships to determine how they are connected—what links them together.

While the technology to conduct data mining is rapidly maturing, it is currently limited by its capacity to handle non-structured formats; i.e., those that are a mix of text, image, video, and sensor information. In addition, future algorithms will also need to incorporate the knowledge of human experts into their derivation of patterns.

## "Breakthrough" Technologies

My final two candidate technologies definitely fit into the last category of an aggressive technology acquisition program. They offer two potential breakthroughs which could significantly reshape the nature of competition between terrorism and counterterrorism.

**Nanotechnology.** As a counterterrorism tool, nanotechnologies are in their infancies. Nanotechnology involves developing or working with materials and complete systems at the atomic, molecular, or macromolecular levels where at least one dimension falls with the range of 1–100 nanometers.[7] Working at such a small scale offers unique capabilities, such as being able to control how nanodevices interact with other systems at the atomic or molecular level.

Current research areas include materials, sensors, biomedical nanostructures, electronics, optics, and fabrication. Materials which have been modified at

[4] *Ibid.*

[5] Committee on the Role of Information Technology in Responding to Terrorism, Computer Science and Telecommunication Board, *Information Technology for Counterterrorism: Immediate Actions and Future Possibilities*, eds. John L. Hennessy, David A. Patterson, and Herbert S. Lin (Washington, D.C.: National Academies Press, 2003), p. 68.

[6] Usama Fayyad, Gregory Piatetsky-Shapiro, and Padhraic Smyth, "From Data Mining to Knowledge Discovery in Databases," *Artificial Intelligence*, Fall 1996, p. 44, at *www.kdnuggets.com/gpspubs/aimag-kdd-overview-1996-Fayyad.pdf* (November 16, 2004).

[7] Daniel Ratner and Mark A. Ratner, *Nanotechnology and Homeland Security* (Upper Saddle River, N.J.: Prentice Hall Professional and Technical Reference, 2004), p. 13.

the nanoscale can have specific properties incorporated into them. For instance, materials can have coatings that make them water-repellant or stain-resistant. According to a study by Daniel Ratner and Mark A. Ratner:

> Nanoscale sensors are generally designed to form a weak chemical bond to the substance of whatever is to be sensed, and then to change their properties in response (that might be a color change or a change in conductivity, fluorescence, or weight).[8]

Biomedical nanostructures, by design, interact with people at the molecular level, allowing for targeted drug delivery, adhesive materials for skin grafts or bandages, etc. Nanoscale electronics can help to shrink computer circuits even further and to make them more efficient. Nanoscale optics allow once again for materials that fluoresce to be tuned at the nanoscale to change specific properties under certain conditions. Fabrication at the nanoscale offers the potential of creating devices from the atom up, as opposed to having to shrink materials down to the needed size.

According to a RAND report, there are numerous future applications for nanotechnology, though most face at least some technical hurdles. They include nanofabricated computational devices like nanoscale semiconductor chips, biomolecular devices, and molecular electronics.[9] If one includes integrated microsystems and micro-electrical-mechanical systems (MEMS) in the discussion, and one probably should, there are additional uses for nanotechnology, including smart systems-on-a-chip and micro- and nanoscale instrumentation and measurement technologies.[10]

While there are counterterrorism applications for all of the research areas, sensors are the most promising. Nanodevices offer the opportunity for fast, cheap, and accurate sensors and detectors, and markers that can be used for a wide range of forensic activities.

**Directed-Energy Weapons.** Active defenses such as directed-energy weapons could provide counterterrorism protection for critical infrastructure.[11] Directed-energy weapons include a host of technologies, including lasers and microwave radiation emitters. These weapons can inflict casualties and damage equipment by depositing energy on their intended target.

Compared with conventional weapons, which rely on the kinetic or chemical energy of a projectile, directed-energy weapons can hit a target with subatomic particles or electromagnetic waves that travel at speeds at or near the speed of light. They generate very high power beams and typically use a single optical system both to track a target and to focus the beam on the target in order to destroy it.[12]

Lasers—the most mature form of directed-energy weapon that can counter airborne threats—form intense beams of light that can be precisely aimed across many kilometers to disable a wide range of targets, from satellites to missiles and aircraft to ground vehicles.[13] Additionally, the laser beam can be redirected by mirrors to hit targets not visible from the source, all without compromising much of the beam's initial power.

Such systems could evolve to provide active defenses against a wide array of potential threats from artillery, rockets, mortars, missiles, and low-flying unmanned aerial vehicles to improvised

[8] *Ibid.*, p. 21.

[9] Philip S. Anton, Richard Silberglitt, and James Schneider, *The Global Technology Revolution: Bio/Nano/Materials Trends and Their Synergies with Information Technology by 2015*, Prepared for the National Intelligence Council (Santa Monica, Cal.: RAND, 2001), pp. 25–28.

[10] *Ibid.*, pp. 28–30.

[11] Jack Spencer and James Jay Carafano, "The Use of Directed-Energy Weapons to Protect Critical Infrastructure," Heritage Foundation *Backgrounder* No. 1783, August 2, 2004, at *www.heritage.org/Research/NationalSecurity/bg1783.cfm*.

[12] Loren B. Thompson, Ph.D., "The Emerging Promise (and Danger) of Directed-Energy Weapons," Lexington Institute Capitol Hill Forum on Directed Energy, July 11, 2002, at *www.lexingtoninstitute.org/defense/energyforum_thompson.htm* (July 23, 2004).

[13] *Ibid.*

explosive devices. For example, these weapons could be deployed at airports to defend planes from attacks by shoulder-fired missiles (and by makeshift rockets and missiles) during takeoff and landing—the times when aircraft are most vulnerable.

With most airports located in or near major urban centers, directed-energy weapons could help to address the near impossibility of providing adequate, credible security zones around airports. Furthermore, they could defend coastal airports from attacks launched from a commercial or private ship loitering offshore—a potentially ideal platform for launching precision strikes. Several countries, including the United States, already have these systems under development.[14]

## Challenges Ahead

It remains to be seen how governments and the private sector apply their energy and imagination to turning these technologies into potent anti-terrorism tools. There are several serious obstacles to be overcome.

**Research and Development Trends.** The September 11, 2001, attacks on New York and Washington seem only somewhat to have affected research and development trends in the United States, and, indeed, it appears that the same trend is holding true for other nations as well. American research and development efforts have been affected only "on the margins."[15] For example, the newly created Department of Homeland Security has a science and technology directorate with a research budget of about $800 million. While that seems like a great deal of money, it is a small fraction of the $90 billion the U.S. government spends on research.

In turn, government research represents an increasingly less significant portion of the total research and development effort. In the 1960s, about two-thirds of U.S. research was federally funded. Today, two-thirds of research—about $180 billion—is funded by the private sector. For example, American software and semiconductor companies spend about $10 billion, which is about the same amount as the entire research budget for the U.S. space program.[16]

The balance of investments for research and development does not bode well for counterterrorism technologies. Most of the cutting-edge research in related areas, particularly with regard to information technology and biotechnology, is in the private sector where development programs are largely driven by potential markets and the profits to be made in the security sector seem to pale in comparison with other commercial opportunities.

In part, this challenge can be addressed by making the counterterrorism community a more attractive customer for the private sector. Legal incentives such as indemnification for products may help—as would broadly accepted international standards for the application of technologies, particularly in the areas of biometrics. Moving to open and non-proprietary information architectures that make it far easier to adapt commercial technologies to law enforcement needs would also be of great benefit.

A significant next step would be initiating a serious dialogue to determine what a future international counterterrorism security technology development regime might look like. It would require, among other things, a technology clear-

[14] Josef Schwartz *et al.*, "Tactical High Energy Laser," presented at the SPIE Proceedings on Laser and Beam Control Technologies, January 21, 2002, pp. 1–6. TRW developed a fixed-site THEL under an $89 million contract. In tests, the system has successfully shot down 25 rockets. It is, however, not currently capable of being deployed for operational use. The U.S. Army is developing a mobile version and has requested additional funding for the program. In February 2004, the Army's tactical laser project was formally converted into an acquisition program. The first prototype of the mobile laser is due to appear in 2008. See Loren B. Thompson, Ph.D., and Daniel Gouré, Ph.D., "Directed Energy Weapons: Technologies, Applications, and Implications," Lexington Institute *White Paper*, February 2003, pp. 11–12 and 24–25, at *www.lexingtoninstitute.org./docs/321.pdf*.

[15] G. Pascal Zachary, "Technology Is Destiny," *The Milkin Institute Review*, Vol. 6, No. 3 (Third Quarter 2004), p. 6.

[16] *Ibid.*

inghouse so that partners know what technologies are available for transfer; a method of setting standards so that technologies are understandable; interoperable and transferable means for industry-to-industry dialogue; predictable export control requirements; and acquisition mechanisms such as joint development programs, licensing agreements, and something comparable to the foreign military sales program.

Any of these or other initiatives that serve to create a more uniform and dependable market for counterterrorism technologies would serve to make it a more attractive target for the private sector and, in turn, stimulate the responsiveness of private research and development in support of key law enforcement needs.

**Barriers to Innovation.** Even if private research and development can be better teamed with government efforts and focused on the terrorism challenges of the 21st century, the traditional barriers to innovation in law enforcement technologies will remain. These challenges include four areas.[17]

1. **Cost.** The expense of new technologies includes both the cost of procuring a technology and the opportunity cost of adopting that technology as compared to other uses to which resources might be put.
2. **Technology Risk.** This includes the ever-present risk that "big bets" will fail. The technology may not perform as expected or adequately address the tasks for which it was adopted.
3. **Human Factors.** New counterterrorism technologies can face a plethora of obstacles that have nothing to do with fiscal costs or technical specifications. For example, data mining and biometrics have raised an array of concerns about the protection of civil liberties and safeguarding of proprietary commercial information. Non-lethal weapons face legal barriers.

   Additionally, institutional cultures may have difficulty adapting to new technologies, and new systems may present significant training and leader development challenges. Systems integration, for example, can enable law enforcement agencies to share information with others, but a number of concerns might make them reluctant to do so.
4. **Unanticipated Costs.** Any new technology will bring unintended consequences. The introduction of nanotechnologies, for example, has raised concerns about the potential consequences of unintentionally introducing new compounds into the environment. New technologies can also bring unexpected liabilities and adverse public reactions.

Perhaps the best means to satisfy these concerns is to address potential policy issues that may serve as barriers to the adoption of new technologies before new capabilities are introduced. Policy development that anticipates technological development represents a largely unprecedented challenge to law enforcement. More often than not, law enforcement's approach has been to take years to develop the procedures that govern the implementation of new technologies, largely waiting for commercial technologies to mature, threats to evolve, and legal precedents to be established. This process will not serve for the challenges of the 21st century, where policy innovation must match, or indeed exceed, the speed of technological progress.

## Conclusion

The terrorist threat against the free world is serious and enduring. We need to jointly develop the means and the technologies needed to meet this threat.

The obstacles to creating an arsenal of counterterrorism technologies that are practical and affordable and overmatch the threat of 21st century terrorism are daunting. Creating a vision of these future technologies, implementing initiatives that broaden the market and make it more predictable and dependable, and developing policies that will

[17] William Schwabe, Lois M. Davis, and Brian A. Jackson, *Challenges and Choices for Crime-Fighting Technology: Federal Support of State and Local Law Enforcement* (Santa Monica, Cal.: RAND, 2001), p. xxi.

help to overcome the barriers to innovation are essential steps to harnessing technology to the future needs of law enforcement.

—*James Jay Carafano, Ph.D., is Senior Research Fellow for National Security and Homeland Security in the Kathryn and Shelby Cullom Davis Institute for International Studies at The Heritage Foundation. These remarks were prepared for delivery at a Middle East Police Exhibition Conference held at the Dubai World Trade Center.*