Heritage Lectures

Published by The Heritage Foundation

No. 824
Delivered February 3, 2004

March 17, 2004

Strategy and Security in the Information Age: Grading Progress in America's War on Terrorism

James Jay Carafano, Ph.D.

In the midst of the 1975 Cypriot Crisis, after a long day of arduous negotiation, American Secretary of State Henry Kissinger and British Foreign Secretary James Callaghan engaged in a profoundly melancholy and prophetic exchange.

> **KISSINGER:** You know, one respect in which all the humanitarians and liberals and socialists were wrong in the last century was when they thought that mankind didn't like war…. They love it.
>
> **CALLAGHAN:** Most of us like it for a day or two, but there is a handful who like it forever.
>
> **KISSINGER:** That's right. It doesn't mean that the humanitarians were wrong, it just means that life is harder than we thought….
>
> **CALLAGHAN:** I don't know what sort of an age we're passing through or going to pass through, but historians like yourself ought to give us a run-down on it sometime and tell us how you think this next half century is going to look.
>
> **KISSINGER:** I'll tell you…I'm glad I'm not going to be running part of it. It's going to be brutal.[1]

They were right. Twenty-five years down and 25 to go, we still live in a brutal world at war.

Talking Points

- The war on terrorism is a real war, and the U.S. can achieve victory by destroying the capacity of those who seek to terrorize innocents and by discrediting the legitimacy of terrorists who believe their violent acts will intimidate the populace.
- The war on terrorism will be a protracted conflict. Succeeding in this war will require strong leadership, an engaged citizenry, and a balanced strategy.
- Crucial parts of this strategy will be the integration of federal, state, and local agencies; cutting-edge information technology; and the Department of Homeland Security's science and technology plan.
- Adopting a "system-of-systems," or network-centric, approach to emergency preparedness will be a fundamental requirement for an effective national response to terrorists.

1. Henry Kissinger, *Years of Renewal* (New York: Simon & Schuster, 1999), p. 232.

This paper, in its entirety, can be found at:
www.heritage.org/research/homelanddefense/hl824.cfm

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

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

Nor has understanding the challenges of strategy and security changed much. Even in the information age, knowing war requires both historical perspective and cautious prophecy. I hope to provide a bit of each: defining the nature of the current conflict; summarizing what has been so far; describing future trends and challenges; and, finally, suggesting potentially fruitful areas of U.S.–Indian partnership in the exploitation of commercial information technology.

War by Any Name

To begin, it is worth taking stock of where we are. President George W. Bush declared a war on global terrorism in the wake of the September 11, 2001, terrorist attacks on New York City and Washington, D.C., sparking, among other things, a war of words over the appropriateness of his declaration. In the United States, pundits, politicians, scholars, and strategists debate whether we should *or even can* be at war with terrorists.

It is true that no country can top the United States when it comes to metaphor mania. "War," in particular, is a staple of American political discourse. We have declared war on everything from abject poverty to overweight pets. Few terms are more overused…but perhaps not in this case.

The main objections to declaring war on terrorism are two.

- *First*, there is no universal definition of terrorism, and thus no clear enemy.
- *Second*, combating terrorists, whoever they are, is not primarily a military operation, but a matter of law enforcement and social, cultural, and economic conflict. It is not "traditional" war, as one U.S. defense analyst declared, in the sense understood by military professionals. Wars, he argues, are supposed to have "clear beginnings and ends…[and] clear standards for measuring success in the form of territory gained and enemy forces destroyed."[2]

Both arguments are wrongheaded.

Every country in the United Nations may not have signed on to the Webster dictionary's definition of terrorism, but that does not mean that it does not exist and does not represent a terrible threat to world peace. After all, there is no universal definition of fascism, but that did not keep the allies from declaring war on the Axis powers during World War II.

Nor do terrorists seem concerned about definitional nuances. They have decided they are most certainly at war with us, and they think they are in a war they can win. In an interview before the September 11 attacks, Osama bin Laden declared, "We no longer believe in the great powers…. [W]e have heard from our brothers who fought in Somalia, American soldiers are weak and cowardly…. [T]hey ran away."[3] Al-Qaeda's leader frequently cited such incidents as proof that the United States could be attacked directly and could be defeated if bloodied.[4]

Additionally, arguing that this is not a "traditional" war is mere semantics. What is a real war? Only in the history books are war and peace divided into separate chapters with bombs and bugles separated in neat paragraphs from social, cultural, and economic strife. Real wars are a competition between two thinking, determined foes who may or may not elect to restrict themselves to traditional military instruments or respect quaint notions such as law, sovereignty, borders, or governments.

2. Jeffrey Record, "Bounding the Global War on Terrorism," U.S. Army War College, Strategic Studies Institute, December 2003, p. 4. See also Michael Vlahos, "Terror's Mask: Insurgency Within Islam," Johns Hopkins University, Applied Physics Laboratory, May 2002, p. 2.
3. Roland Jacquard, *In the Name of Bin Laden: Global Terrorism and the Bin Laden Brotherhood* (Durham, N.C.: Duke University Press, 2002), p. 260.
4. Since the mid-1990s, Osama bin Laden has repeatedly threatened violence against the United States to coerce withdrawal of U.S. troops from Saudi Arabia. However, in recent years his rhetoric has expanded to include a call for a campaign against U.S. interests in general. Magnus Ranstorp, "Interpreting the Broader Context and Meaning of Bin-Laden's Fatwa," *Studies in Conflict and Terrorism*, Vol. 21, No. 4 (October–December 1998), pp. 321–330. For an analysis of possible motivations that may have inspired the September 11 attacks, see Ahmed S. Hashim, "The World According to Usama Bin Laden," *Naval War College Review*, Vol. LIV, No. 4 (Autumn 2001), pp. 11–36.

We are at war. It is not a war that can hope to forestall every terrorist act, everywhere, but it *is* a war that can find victory in destroying the capacity of those who seek to transform transnational terrorism into a corporate global enterprise for the indiscriminate murder of innocents. It is also a war that can be won by discrediting the legitimacy of terrorists in the eyes of those who believe that their violent acts will somehow miraculously address political, social, religious, or economic injustice.

Organizing for Victory

In fact, the global war on terrorism will be like most wars. It will have casualties and sacrifices, victories, defeats, advances, and setbacks. Progress won't 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 United States and its friends and allies, 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 can take lessons from the Cold War on how to win a long, protracted conflict.

Organizing for victory requires strong leadership, an engaged citizenry, and a balanced strategy. We lacked all of these in the first years of the Cold War. Despite all the rhetoric, the Truman Administration was reluctant to compete with the Soviet Union. The President initially shelved NSC–68, the master plan for confronting the Russians. Defense budgets shrank.[5] Meanwhile, average Americans remained largely complacent—more worried about better jobs and new homes than the harsh realities of global competition.

The Korean conflict brought the Cold War home to Main Street. In came a new President, Dwight Eisenhower, with a strong mandate and a new strategy based on building a strong economy and preserving an open society, as well as an appropriate mix of offensive and defensive measures. Eisenhower recognized all three were essential for competing over the long term.[6]

Bush wants to be Eisenhower, not just making Americans safer, but laying the groundwork to win the long war against international terrorists. The President has a tough task ahead of him.

Here we can learn another lesson from the Cold War.

In the United States, the National Security Act of 1947 created a unified Defense Department and the CIA, the nation's two premier Cold War weapons. But, in practice, it took about a decade of reorganization and trial and error to figure out how to fight the Russian bear. The basic instruments used throughout the Cold War—NATO, the U.S. nuclear arsenal, and military assistance programs—all emerged during this formative period.

One of the instruments for this war will have to be a sound homeland security system. Just going after the terrorists won't be enough. In a world dependent on the free flow of goods, services, ideas, and people, no country can ever be confident that it can keep every terrorist from its shores.

To enhance public safety, the Administration drafted new strategies[7] and created an entirely new federal agency, the Department of Homeland Security. The U.S. Department of Homeland Security is the result of a reorganization proposed by President Bush after the 2001 terrorist attacks. He hoped that by centralizing the homeland security effort, the nation could be better protected from future attacks. This reorganization consolidated the activities of over 22 federal agencies into a single department. The department has broad responsibilities.

The National Strategy for Homeland Security issued by the Bush Administration in July 2002 identified six critical mission areas. These areas were established to focus federal efforts on the strategy's objectives of preventing terrorist attacks,

5. For an introduction to NSC–68, see Ernest R. May, ed., *American Cold War Strategy: Interpreting NSC 68* (Boston: Bedford Books, 1993).
6. See, for example, Robert R. Bowie and Richard H. Immerman, *Waging Peace: How Eisenhower Shaped an Enduring Cold War Strategy* (Oxford: Oxford University Press, 1998).
7. See, for example, The White House, *The National Strategy to Secure Cyberspace,* at *http://www.whitehouse.gov/pcipb.*

reducing America's vulnerabilities to terrorism, and minimizing the damage and recovering from attacks that do occur. The six critical mission areas are:

- Intelligence and Early Warning;
- Border and Transportation Security;
- Domestic Counterterrorism;
- Protecting Critical Infrastructure and Key Assets;
- Defending Against Catastrophic Threats (i.e., research and development); and
- Emergency Preparedness and Response.

The Department of Homeland Security has major responsibilities in each of these areas.

It is worth noting, however, that despite consolidation, many other federal agencies retain homeland security functions. The FY 2004 budget for the Homeland Security Department amounts to 58 percent of the federal homeland security budget, about $38 billion total. Together with Defense, Health and Human Services, Justice, and Energy, these five departments account for 92 percent of the homeland security budget, forming the core of the federal domestic security effort. Only seven other federal departments or agencies have received funds for homeland security programs that amount to $200 million or more.[8]

The level of homeland security spending is significant, though expenditures have not grown as fast as many expected. In the wake of 9/11, some lawmakers predicted federal spending would soon reach $57 billion a year.[9] The FY 2002 budget ($19.5 billion)[10] reflected little new spending and represented mostly shifting funds that had previously been accounted for under other accounts such as counterterrorism initiatives. In addition, supplemental funding in the wake of the 9/11 attacks increased spending for homeland security–related activities by an additional $10.7 billion.[11]

The FY 2003 and FY 2004 budgets were similar in size, setting baseline federal spending for homeland security in the United States at under $40 billion. Overall, federal homeland security spending increased by some 240 percent after the September 11 attacks. Stabilizing funding at current levels appears prudent. While enormous security challenges remain, allowing the many agencies involved some time to absorb these large increases makes sense.

Making the Homeland Security Department something more than a hastily assembled bureaucracy, establishing strategic priorities, and determining how best to integrate the capabilities of federal, state, and local agencies will take more than a year or two.[12]

Looking Ahead

The Department of Homeland Security is currently laying the groundwork for a national homeland security network for the long term. Two initiatives in this effort are particularly important for competing against terrorists in the information age.

Cutting-edge information technology (IT) is key to getting the most out of the new department and improving information sharing between federal, state, and local agencies—a critical strategic need.[13]

But buying too much technology too fast, without an established information architecture and a clear

8. James Jay Carafano and Steven M. Kosiak, "Homeland Security: Administration's Plan Appears to Project Little Growth in Funding," Center for Strategic and Budgetary Assessments *Backgrounder*, March 12, 2003, at *http://www.csbaonline.org/4Publications/Archive/U.20030312.Homeland_Security_/U.20030312.Homeland_Security_.pdf*.
9. William Mathews, "The Politics of Security," *Armed Forces Journal*, February 2003, p. 8.
10. Carafano and Kosiak, "Homeland Security: Administration's Plan Appears to Project Little Growth in Funding."
11. *Ibid*.
12. State and local governments also spend a significant portion of their budgets on homeland security and related public safety activities. Spending in these areas has increased significantly since the September 11 attacks, though the full scope of state and local expenditures is uncertain, as is the impact of cutbacks by state and local governments resulting from budget shortfalls caused by a downturn in the U.S. economy. See Council on Foreign Relations, *Emergency Responders: Drastically Underfunded, Dangerously Unprepared*, 2003, pp. 33–34, at *http://www.cfr.org/pdf/Responders_TF.pdf*.
13. See, for example, U.S. General Accounting Office, *Homeland Security: Efforts to Improve Information Sharing Need to Be Strengthened*, GAO–03–760, August 2003.

understanding of requirements, as well as safeguards for security and privacy, could cause IT costs to balloon out of control. Even with a well-designed program, the funding implications are substantial. Merging computer and communications systems together could easily top $10 billion. Integrating operations with emergency responders nationwide could run another $18 billion.

With an annual department budget of around $29 billion, such costs could easily crowd out other essential programs. In addition, failing to provide safeguards for security and privacy could lead to political pitfalls, damaging the fledgling department's credibility and effectiveness.

Thus, one of the key ongoing efforts is the creation and implementation of the department's enterprise architecture. The department's Chief Information Officer, Steven Cooper, announced the completion of a preliminary enterprise architecture in September 2003.[14] The document has not yet been publicly released. A review of the final, approved architecture and how well its priorities are reflected in the President's FY 2005 budget request, to be released this week, will be key indicators for determining progress in this area.

Another key event will be the public release of the department's Science and Technology Directorate's science and technology plan, which will lay out its research and development priorities. The plan consists of a series of program analysis documents that basically outline what the requirements are that need to be done in the major portfolios, such as cyber security and chemical, biological, radiological, and nuclear threats.

The largest share of research dollars, some 30 percent, is in the area of defenses against biological weapons attacks, but information technologies research is also prominent, particularly in the area of developing sensor networks.[15]

On the other hand, in areas such as cyber security, the directorate plans to rely heavily on private industry to develop and adopt new technologies. The directorate's work in this area will most likely be relatively modest and coordinated closely with the National Science Foundation and the National Institute of Standards and Technology.[16]

The directorate's science and technology plan is due for public release soon and is being used to serve as the basis for the department's FY 2005 budget request. The expectation should be that the lion's share of near-term funding will be for well-established technologies that can be developed and fielded in one to two years (only about 10 percent will be for truly forward-looking research) and that most of these funds will be expended through formal solicitations rather than unsolicited proposals.

The level of funding will likely remain constant for the foreseeable future. Total budget for the Homeland Security Department's Science and Technology Directorate in FY 2004 was $918.2 million (some $874 million of that will go toward programs). Funding for the Homeland Security Department's Science and Technology Directorate is likely to remain level in fiscal 2005.

The Department of Homeland Security will not be the only federal agency with significant IT projects. Virtually every federal department faces significant challenges.[17] However, cost overruns, poor management, and fielding delays have made both the Administration and Congress wary of significantly ramping up IT investments.

Options and Opportunities

Over the long term, as the United States and, indeed, the global community better define security needs, I think there will be significant growth in the development of IT domestic security programs. In particular, there will be a very important role for

14. Steven I. Cooper, Testimony before the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, Committee on Government Reform, U.S. House of Representatives, October 8, 2003.
15. Rick Merritt, "Sensor Nets Top R&D List for Homeland Security Agency," *EE Times*, December 31, 2003, at *http://www.eetimes.com/story/OEG20031231S0006*.
16. Ted Leventhal and Greta Wodele, "Homeland Security Science Division Will Tackle Cybersecurity," GovExec.Com, December 4, 2003, at *http://www.govexec.com/dailyfed/1203/120403tdpm2.htm*.
17. See, for example, Department of Transportation, "Top Management Challenges," Report Number PT–2004–006, December 5, 2003, pp. 15–17.

defining systems architecture and linking disparate technologies together.

Given the complex and demanding requirements of responding to a determined, protracted, and potentially catastrophic terrorist threat, the fundamental requirement of an effective national response system may be to adopt a "system-of-systems," or network-centric, approach to emergency preparedness.

Network-centric operations generate increased operational effectiveness by networking sensors, decision makers, 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 in the response to emergencies from the local to the national level.

Such a system might produce significant efficiencies in terms of sharing skills, knowledge, and scarce high-value assets, building capacity and redundancy in the national emergency response system, as well as gaining the synergy of providing a common operating picture to all responders and being able to readily share information. Network-centric systems might be especially valuable for responding to large-scale or multiple weapons of mass destruction attacks, where responders will have to surge capacity quickly, adapt to difficult and chaotic conditions, and respond to unforeseen requirements.

Over the long term, there will likely be demands for such systems, not just in the United States, but in other countries as well. I would argue that the United States needs to internationalize its efforts to develop homeland security systems. Since emergency responders around the world face similar problems, whether they are responding to a natural disaster or an intentional chemical or biological weapons attack, the United States should broaden the scope of its efforts to jointly develop and share appropriate technologies with friends and allies so that we are all better prepared to deal with the common threat of transnational terrorism.

The United States already has had some successful bilateral technology sharing of counterterrorism tools with individual countries, such as Israel. However, while the mechanism for developing and transferring defense technologies on a military-to-military basis is fairly mature, the United States lacks a sophisticated approach to sharing technologies and lessons learned for civilian homeland security needs.

Countries with sophisticated IT industries, such as the United States and India, should enter into a serious dialogue to determine what a future homeland security technology development regime might look like. It would require, among other things, a technology clearinghouse 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.

Working jointly on system-of-systems technologies for homeland security could provide the right set of options and opportunities to enhance the security of all free nations. 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.

—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 presented at the National Association of Software and Services Companies' India Leadership Forum on February 3, 2004, in Mumbai, India.