



DEFEATING TERRORISM



STRATEGIC ISSUE ANALYSIS Homeland Security Issues: A Strategic Perspective

Lieutenant Colonel Antulio J. Echevarria II

Conclusions:

- The new war being waged against America is a form of asymmetric warfare using terror tactics, not a standard terrorism campaign.
- DoD's role is evolving but will likely remain largely a supporting one in homeland defense.
- The new threat environment and the numerous "vulnerabilities" within the homeland require a new way of thinking about "threats" and how to address them.
- Assessments of critical infrastructure and key assets require updating.
- NMD will remain a critical component of homeland defense.
- The nation needs a Federal Defense Plan to complement the Federal Response Plan (FRP) that exists for consequence management.
- Unless current laws prohibiting the U.S. military from gathering intelligence on U.S. citizens are amended, the establishment of a "CINC America" is not recommended.

This paper provides a brief analysis of the U.S. homeland's current threats and vulnerabilities, outlines a general strategy for homeland defense and the war against terrorism, and discusses some salient issues related to command and control.

Assumptions.

- The U.S. will continue to wage a multi-lateral and sustained war against all terrorist organizations with "global reach" and their state (and nonstate) sponsors. Hence, homeland security requires a long-term perspective.
- Unless significant legislative changes occur, the U.S. military will perform most homeland security missions in support of other federal agencies.
- The U.S. will remain politically and economically engaged in the world. It will maintain sufficient military presence overseas to deter aggression and honor its alliance and treaty commitments.

Threats and Vulnerabilities.

Terrorism. Despite heightened awareness and increased security efforts since the tragic events of September 11, 2001, the U.S. remains vulnerable to a wide variety of terrorist attacks. On October 5, 2001, for instance, the Project on Government Oversight reported that America's ten nuclear weapons research and production facilities are still inadequately protected. A report recently published by the Henry L. Stimson Center revealed that the 850,000 sites that produce,

consume, and store hazardous chemical materials in the U.S. remain virtually unprotected.

Furthermore, while much attention remains focused on the war overseas, domestic terrorist organizations—e.g., the "Michigan Militia," the "Order," and the "Aryan Nations"—remain at large and dangerous. Until September 11, 2001, international and domestic terrorists had claimed 670 lives on U.S. soil in over 2,700 incidents, with white racist groups causing the majority (51 percent) of deaths. Domestic terrorist groups could well retaliate in response to the federal government's introduction of increased security measures in the aftermath of September 11.

Although the number of international and domestic terrorist attacks has declined in the 1990s, the lethality of those attacks has risen dramatically. This rising lethality can be looked at in one of two ways: 1) as the emergence of a "new" or "apocalyptic" brand of terrorism bent on producing mass casualties, or 2) as a new or "asymmetric" form of warfare that employs terror tactics. The first view tends to regard "terrorism" as an aggregate, placing disparate terrorist groups—such as the Aryan Nations, the IRA, and al-Qaeda—into a single category. In so doing, it obscures their ideological, political, and cultural differences. An understanding of such differences is critical to the development of effective strategies for defeating such groups. The IRA has shown a proclivity to employ small-scale attacks that do not involve large numbers of casualties and which

damage infrastructure such as power grids. These are clearly not the tactics of the al-Qaeda group. The motives of al-Qaeda, unlike those of the IRA or the Aryan Nations, have unique religious and cultural underpinnings which, if not understood, could result in an escalation of the current conflict or lead to other negative strategic consequences for the U.S., its allies, and coalition partners. Thus, a "one-size-fits-all" approach to terrorism could lead to an inappropriate strategy for defending the homeland and for conducting military operations overseas.

The U.S. Army and DoD would do better, therefore, to take the view that America is engaged in a new or asymmetric style of warfare perpetrated by certain states and nonstate actors who prefer terror tactics. This view permits the disaggregation of "terrorism" based on useful criteria such as political and cultural motives, enabling a better understanding of a particular group's strengths and weaknesses. It also facilitates development of a more integrated national security strategy, one that provides for a comprehensive defense of the homeland while also dealing with nonstate actors and their state sponsors. Third, it allows the U.S. Army to demonstrate the strategic relevance of its core competencies and its transformation programs. The Army should also stress how the campaign in Afghanistan has highlighted the limitations of an airpower-centric approach to warfare.

Chemical, Biological, Radiological, Nuclear, and High-Explosive/High-Yield (CBRNE) Weapons. CBRNE weapons continue to proliferate. Seventeen countries—including Iran, Iraq, Libya, and North Korea—have active chemical and biological weapons programs. While it remains difficult to manufacture, deliver, and activate certain types of CBRNE weapons, the apparent availability of "free-lance" expertise from the former Soviet Union combined with today's rapid pace of technological innovation suggests that potential adversaries will succeed in overcoming these difficulties sooner rather than later. The recent decision to increase the reserve of smallpox and anthrax vaccines is, therefore, encouraging.

Critical (and Other) Infrastructure. In 1997, the Presidential Commission on Critical Infrastructure Protection (PCCIP) assessed the vulnerability of the nation's critical infrastructure. At that time, U.S. critical infrastructure included: 400 airports; 1,900 seaports; 6,000 bus and rail transit terminals; 1,700 inland river terminals; 1.4 million miles of oil and natural gas pipelines; and other banking, financial, and energy-related networks. The Commission

assessed the Energy, Physical Distribution, and Banking and Finance sectors as either well-protected or relatively resilient to an attack, while it regarded the Vital Human Services and Information and Communications sectors as highly vulnerable to cyber and physical forms of attack.

The PCCIP admitted that it did not know enough about water-borne pathogens and the threat they could pose if released into the nation's water supply. The American Waterworks Association (AWWA) maintains that the sheer volume, chlorine content, and multiple filtration systems built into major water supplies make them resistant to contamination by all but a few pathogens. At risk, however, are smaller water supplies.

Unfortunately, the PCCIP also completely overlooked the nation's agricultural infrastructure. While the U.S. Department of Agriculture (USDA) is confident that it can respond to "natural, accidental, and inadvertent introductions" of exotic diseases and pests into the food supply and agricultural system, it admits that it is incapable of addressing the "widespread intentional introduction" of such threats. The number of pathogens and other agents that could devastate U.S. livestock and crops are numerous and inexpensive to develop. Since the U.S. produces some 30-50 percent of many of the world's foodstuffs, an agricultural crisis could have global implications.

The PCCIP also failed to consider the entertainment and recreational industries—amusement parks, sports arenas, shopping malls, and other locations where large numbers of people gather. While not necessarily critical to the nation's ability to function, these are the types of targets that al-Qaeda and other such organizations seem inclined to strike. A successful CBRNE attack against Disney World or a major sports arena, for example, could result not only in thousands of casualties, but in adverse economic consequences as well.

The PCCIP's oversights combined with the rapid pace of urbanization and economic development, even since 1997, suggest that the Commission's assessment requires immediate updating. By way of illustration, in 1999 the National Infrastructure Protection Center (NIPC), an interagency office housed at the FBI, identified a list of just over 200 key national assets requiring protection. However, its FY01 report is expected to include a total of 4,385 key assets.

The Cyber Threat. In February 2000, the Director of the CIA testified before Congress that the foreign cyber threat was growing rapidly.

More than one dozen countries—including Russia, the PRC, and several states of concern—have developed, or are developing, the means to launch strategic-level cyber attacks. The interconnectedness of much of the nation's infrastructure means that a successful cyber attack against one sector will likely result in adverse effects in others.

Ballistic Missiles. Today, more than 25 countries possess ballistic missile programs, though only two, Russia and China, currently have missiles capable of reaching the U.S. The Rumsfeld Commission reported that North Korea and Iran could build ballistic missiles capable of striking the U.S. within 5 years of deciding to do so. Iraq could have the same capability within 10 years of such a decision. It is difficult, if not impossible, to know precisely when one of these states might take such a decision. North Korea, Iran, and Iraq have also been known sponsors of terrorism for some time. In other words, America's war against terrorism could lead in time to a confrontation with one or more states capable of targeting the U.S. with ballistic missiles.

Cruise Missiles. Cruise missiles include a wide variety of types, ranging from relatively inexpensive unmanned aerial vehicles (UAVs) to the more expensive U.S.-made Tomahawks. Intelligence estimates indicate that some 80,000 cruise missiles of numerous types will exist by 2010. More than 75 countries already possess some kind of cruise missiles, and the technology for developing them is proliferating rapidly. Many types in existence today can be concealed in and launched from standard shipping containers. On average, 1500 ships carrying standard containers navigate the Pacific and Atlantic oceans within cruise-missile range of the United States every day.

"Threats" versus Vulnerabilities.

Today's threat environment reflects the influences of a faster-paced and more interconnected world. In this environment, the traditional notion that "a threat = capabilities x intentions" remains valid for conventional warfare, but has serious deficiencies when applied to America's "New War." In the attacks of September 11, 2001, for example, terrorists demonstrated an ability to use common materials—box knives and airliners filled with fuel—rather than uniquely military "capabilities." The so-called capabilities of al-Qaeda and similar terrorist groups are, therefore, limited only by their imagination and their ability to gain access to the specific items they want to use.

Moreover, the general intention of such groups is self-evident, namely, to hurt the U.S. in

whatever way possible. Yet, the specific intentions of individual tactical cells—such as which targets will be attacked, when, and how—are much more difficult to divine and are clearly much more important. The traditional definition of "threat" essentially provided a useful calculus for the strategy of deterrence that characterized the Cold War. However, it is inadequate for the new security environment in which an enormous number of vulnerabilities exist, and where many of the players do not readily conform with the "rational-actor" model.

National Missile Defense (NMD). America's war on terrorism will make NMD *more* important to U.S. security despite the fact that attacks so far have been largely "asymmetric." Since a long war against terrorism and its state-sponsors runs the risk of escalating into a war against one or more states of concern, the U.S. is effectively in a race against time to develop some type of comprehensive missile defense system. Reports that development of an NMD system will proceed are, therefore, encouraging. The U.S. should maintain a global perspective when it comes to missile defense, since an attack against an ally or strategic partner could adversely affect America's ability to protect its interests.

A Strategy for Defense. Most government-sponsored studies of homeland security have focused primarily on issues related to consequence management. Indeed, defense seems a nearly impossible task, given the large number of potential targets, the vast number of scenarios, and the overall financial expenditures that an effective defense would likely require. While consequence management is clearly important, the events of September 11, 2001, demonstrate that the absence of a comprehensive, preventive strategy for homeland defense can result in an enormous loss of lives and even greater financial costs than prudent defensive measures would have entailed.

One of the first actions that the Office of Homeland Security (OHS) should undertake, therefore, is to develop a comprehensive strategy for homeland defense. A Federal Defense Plan would provide a critical element in that strategy. DoD's strategists and war planners could provide valuable assistance in the development of both. One possible outline for a homeland defense strategy follows:

1. Prevention: Hardening potential targets—whether nuclear reactors or shopping malls—against attack. This measure will require thorough vulnerability analyses involving all forms of attack.

2. Active Countermeasures: Systematic surveillance and preemptive confrontation with known terrorist sympathizers and supporters, increased law enforcement and/or military presence, and an active publicity campaign designed to let terrorists know that the U.S. is prepared to respond.

3. Aggressive Intelligence: Proactive intelligence gathering, analysis, dissemination, and sharing among appropriate national (and international) agencies, allies and coalition partners, and state and local law enforcement authorities. This is the most essential and yet most complicated component due to legal constraints regarding the collection of intelligence on U.S. citizens.

4. Development of Indicators: A set of triggering events that could be used to focus intelligence efforts and/or initiate countermeasures.

5. Anticipatory Crisis Response: Multilateral, global response mechanisms designed in anticipation of terrorist attacks. This component would include coordination (particularly with Canada and Mexico), training, readiness evaluation, and rehearsals of what to do and how to do it in the event of an attack.

This model served the U.S. well in the Gulf War (1990-91) by helping military and civilian officials deter or defeat Iraqi terrorist attacks. It offers a clear reminder that effective homeland defense requires a global perspective, particularly with regard to intelligence.

Successful execution of any strategy will require effective management by an overarching organization, such as the OHS. While personal influence, individual leadership skills and direct access to the President will help, ultimately the OHS's effectiveness will depend upon the degree of budgetary and legal authority it has over the more than 40 federal and other organizations that play a role in homeland security.

Command and Control. Military command and control in homeland defense could take a variety of forms, from enlarging Joint Task Force-Civil Support to standing up a unified combatant command.

Recent studies that recommend against standing up a U.S. combatant command might have arrived at the right answer for the wrong reasons. One study split the overarching mission of homeland security into two parts: defense of the U.S. and support to civil authorities. The author saw little advantage in combining the two parts of the overall mission under one command, a command that, if current plans remain in effect, would not have assigned forces. Instead, he recommended that UCP'01 reflect a short-term fix

by (1) consolidating civil support functions at JFCOM through the realignment of DOMS from the Army to OSD and the Joint System, and (2) assigning NMD to SPACECOM.

However, such objections do not stand up to closer scrutiny. First, whether a synergy exists between the two homeland security missions—and whether this is a valid criterion for not putting them under a single command—are matters of judgment. One could combine both missions under one command to facilitate coordination and reduce possible conflicts over resources. Second, the fact that forces are not currently assigned does not necessarily preclude their assignment at a later date. The problem of defending the homeland is larger than the solution a revised UCP could provide. The nation needs a Federal Defense Plan to complement the Federal Response Plan that exists for consequence management.

A more compelling reason for not creating a "CINC America" is that current laws prohibit the military from collecting and storing intelligence on U.S. citizens. Until those laws are changed, a military combatant commander cannot gather the intelligence necessary to take proactive steps in defense of the homeland. Accordingly, a combatant commander would do little more than respond to "taskings" for military forces by the FBI or other lead federal agencies. It is far from certain that the courts would grant exceptions to the law, even under a wartime footing. At issue are privacy rights and civil liberties, the preservation of which remains an enduring vital interest of the U.S. and its citizens.

If legislative changes do not occur, then the establishment of a para-military civil defense force might offer a better long-term solution for defending the homeland. A civil defense force would not fall under the constraints of the Posse Comitatus Act and could perform a variety of functions, such as protecting key national assets and augmenting local law enforcement, border guards, customs officials, and the Coast Guard. It could come under the control of an organization similar to the OHS.



More information on the Strategic Studies Institute may be found on the Institute's Homepage at <http://carlisle-www.army.mil/usassi/welcome.htm> or by calling (717) 245-4212.

