2005-06

Homeland Security Affairs Journal, Volume I - 2005: Issue 1, Summer

Monterey, California. Naval Postgraduate School

Homeland Security Affairs Journal, Volume I - 2005: Issue 1, Summer
http://hdl.handle.net/10945/49819

Volume I, Issue 1: Summer 2006

Homeland Security Affairs

The Journal of the
Naval Postgraduate School Center for Homeland Defense and Security

Featured Theme: Prevention

ISSN 1558-643X http://www.hsaj.org

Homeland Security Affairs

Volume I, *Issue* 1 2005 *Article* 1

Summer 2005

Changing Homeland Security: The Issue-Attention Cycle

Christopher Bellavita*

*Naval Postgraduate School, christopherbellavita@gmail.com

Changing Homeland Security: The Issue-Attention Cycle

Christopher Bellavita

Abstract

The July 7, 2005 attacks on London inescapably direct public attention to our own transportation system. But eventually – as happened after the Madrid bombings in 2004 – public vigilance will wane. This can be seen as an affirmation of the profound trust Americans place in their public safety professionals. It is also the natural dynamic of the Issue Attention cycle, in which certain issues follow a predictable five stage process: pre-problem, alarmed discovery, awareness of the costs of making significant progress, gradual decline of intense public interest, and a post-problem stage. Before the London attacks, Homeland Security was on the cusp of the fifth and last stage. Unless the U.S. is attacked again, we will continue into Stage Five once the waves from the London bombing recede. In the absence of an active national consensus that terrorists are a clear and present threat to the lives of average Americans, the dynamics of the Issue-Attention Cycle are as inevitable as the seasons.

AUTHOR BIOGRAPHY: Christopher Bellavita is the Executive Editor of 'Homeland Security Affairs'.

KEYWORDS: pre-problem, discovery, awareness, decline, public interest, post-problem

The July 7, 2005 attacks on London inescapably direct public attention to our own transportation system. Everyone getting on a bus or train will look a little more carefully at objects that seem out of place or at people who look a bit suspicious. Public officials will call for more equipment, more people, and more spending for transportation security. It happened in the U.S. after the Madrid bombings in 2004. But eventually – as also happened after Madrid – public attention and vigilance will wane. Transportation security advocates will again have to battle for resources against competing homeland security interests.

The attacks in Madrid and London illustrate Homeland Security's slide from the apex of the national domestic policy agenda into the mundane world of grants, bureaucracy and interest groups. But this is not a bad thing. It is an affirmation of the profound trust Americans continue to place in their public safety professionals. It is also the natural dynamic of the Issue-Attention cycle.

More than 30 years ago, Anthony Downs wrote about a cycle that affects many domestic public policy problems.[1] Downs argued that certain issues follow a predictable five stage process: pre-problem, alarmed discovery, awareness of the costs of making significant progress, gradual decline of intense public interest, and the post problem stage. Before the London attacks, homeland security was on the cusp of Stage Five. After the attacks, it revisited Stage Two. Before too many months pass, it is likely to recall the difficulties of Stage Three, make a brief return trip through Stage Four, and – if there are no more attacks – settle into Stage Five.

We have been at war with the terrorists since September 11, 2001. They have been at war with us since October 23, 1983, when 241 U.S. service members were killed in Lebanon. During the almost 20 years before the nation formally joined the Terrorism Wars, homeland security was in Stage One of the Issue-Attention Cycle: the pre-problem stage. A relatively small group of people were alarmed by the rising threat of terrorism. As has been well documented in the post 9/11 era, most of those calls to pay attention were ignored.

After the pre-problem phase comes Stage Two: Alarmed Discovery and a euphoric enthusiasm to do something quickly about the problem. Alarmed Discovery is triggered by an especially dramatic event, such as September 11th. At this point, the rest of the nation discovers – or in the case of the London bombings, recalls – the problem. Political leaders rise up to demand and to oversee an immediate solution. They are driven by a can-do ethos that asserts no problem is too big or complex to be solved. We just need to get the right people working together as a team, come up with a plan, and simply fix the problem. Stage Two of the Cycle is characterized both by shock and by the unyielding confidence that we can do something to right the wrongs that allowed the problem to happen.

After September 11th, we saw the largest reorganization of the national government in over half a century. We allocated rivers of money to homeland security, even taking away funds from other public safety programs. Interestingly, very few states and cities – with the notable exceptions of New York City, Washington D.C., and a few other cities– made such dramatic structural or resource changes. This was an early signal that perhaps

most of the country is not as concerned about homeland security as are the jurisdictions with the most vulnerable targets

In Stage Three of the Cycle, there is a growing awareness of the costs of making significant progress. The nation has not been attacked in almost four years. We have spent more than 100 billion dollars on homeland security. Hundreds of thousands of people have now added "homeland security" to their job responsibilities.

Even so, books, articles and reports continue to point out how vulnerable our borders, ports, transportation systems, schools, public health, food supply, chemical industry, and infrastructure are to terrorist attacks. Our spending and our programs focus mostly on preparing to respond more effectively and efficiently to the next attack. We still do not have a national plan to prevent terrorism. We do not even have a shared vocabulary for prevention.

The executive branch of the national government is embarking on a multi-year effort to convince states and cities to obey the expanding dictates of Homeland Security Presidential Direction (HSPD) 8 if they want to continue to receive homeland security funding. More than one city is quietly doing the benefit cost analysis to determine whether getting homeland security money is worth the organizational and other costs to satisfy grant requirements. State legislatures are becoming aware that the national government expects them eventually to pick up a substantial share of homeland security spending. The private sector continues to balk at systematically collaborating with government to reduce critical infrastructure vulnerabilities. These are all Stage Three artifacts of the Issue-Attention cycle.

By Stage Four, the public – including public leaders– gradually loses interest in the problem. Some people become discouraged about how long it is going to take to "solve" the problem. Others become bored with it or move on to other, more immediately pressing, concerns.

There is substantial evidence that public interest in the terrorism problem has waned since 2001. In October 2001, 85% of Americans thought the next attack was imminent. In June 2005, a USA Today/CNN/Gallup poll reported that 64% of Americans believed we would not be attacked anytime soon.

Most Americans have little concern that they or their families will be victims of terrorism. A January 2005 CNN/USA Today/Gallup Poll found 90% of adults believed the chances of a terrorist attack in their community was "not too likely," or "not at all likely." In a May 2005 CBS poll, only 7% of adults nationwide thought terrorism was the most important national problem. A June 2005 ABC News/Washington Post poll reported only 12% of adults in the country believed the U.S. campaign against terrorism should be the top priority for the Bush Administration. The economy, the Iraq war, health care, and social security all ranked higher. Of the college seniors and graduates surveyed in 2005, only 13% were afraid of terrorism. Significantly larger majorities feared going into debt and being unemployed.[2]

Stage Five of the Cycle is the Post Problem Stage. The issue moves behind the public scenes and becomes the grist for homeland security's congressional, industrial, academic, and bureaucratic Complex. The professionals who populate that Complex develop and refine the strategies, programs and institutions formed in response to Alarmed Discovery.

Before July 7, 2005 we were on the cusp of Stage Five. Unless the U.S. is attacked again, we will continue into Stage Five once the waves from the London bombing recede. The American public is generally comfortable with the amount of attention government gives to homeland security. More than half the adults polled in a May 2005 NBC News/Wall Street Journal survey thought the national government was placing just the right amount of emphasis – not too much, not too little – on both homeland security and terrorism.

There are several reasons why a diminished public interest in homeland security is not a problem. For one thing, in the absence of an active national consensus that terrorists are a clear and present threat to the lives of average Americans, the dynamics of the Issue-Attention Cycle are as inevitable as the seasons. Homeland security has matured sufficiently to join the routine of public policy.

There is no particular reason why homeland security has to be the number one priority for America. Half the American people polled in the summer of 2004 thought we were safer now than we were on September 11th. Half thought we were not.

Clearly there are some states and cities where the threat of terrorism is not a theoretical exercise. They have people living in their communities who wish harm to our nation. They house targets which if attacked could kill hundreds of thousands of people or cause massive disruptions to the national economy.

But there are other communities where tornadoes, hurricanes, gangs, or methamphetamines are more immediate threats. In a world where you cannot do everything, these communities have chosen – by how they spend their money and attention – to manage the risks they can do something about, and to accept the risk of Al Qaeda-style and domestic terrorism. In the absence of any additional terrorist attacks, expect to see more communities join this group.

At a Spring 2005 conference of state legislators and judges, only two out of forty public officials attending a homeland security panel indicated that homeland security was one of their top concerns. As one legislator said, they have faith that the public safety professionals charged with securing the homeland are doing their jobs. "If they're not," he said, "then we need to get people in there who will."

One recent June evening, Interstate 5 near the bucolic and largely unpopulated California-Oregon border was shut down for several hours. Someone had reported a suspicious box by the side of the freeway, under the "Welcome to California" sign. The box turned out to be the cremains of an unknown person – ghastly enough, but nothing worse. This very minor incident involved the citizen who reported the box, law enforcement agencies, and other public safety agencies from two states that responded, collaborated, and communicated to resolve the issue. In the pre-September 11th world, it is likely the box would have stayed unnoticed until the next time the highway was cleaned.

Today, all over the country, agencies that had no history of working together are creating a new history. Government and private sector workers are more attuned to what is around them. Law enforcement officials who complained about never getting any information are now complaining about getting too much. That is progress.

We have only begun this epochal marathon called homeland security. There is much to criticize about the pace, philosophy, and means of making the nation safer. In a sense, it is disappointing that we need an attack on British subways and busses to generate more attention for our own transportation system. Homeland security has lost its prominence as an issue that rivets the imagination of an easily distracted public. But the terrorist threat remains real. And the magnitude of the work that remains to be done grows geometrically as knowledge about our vulnerabilities increases.

The Issue-Attention Cycle continues. The post problem stage of the Cycle becomes Version 2.0 of a new pre-problem stage. Anyone paying attention can hear homeland security specialists worrying about ports, public health, food supply vulnerabilities, and more.

The country will be attacked again – next month, next year, or in the next decade. After the Alarmed Discovery that follows the attack, there will be another period of "euphoric enthusiasm" to dramatically change what we are doing now.

Here is where homeland security's issue-attention cycle may depart from the conceptual template. Some of the "dramatic changes" that follow a horrendous attack could reshape forever, and in historically undesirable ways, the American ethos. It is the job of homeland security professionals to prevent that next attack. When the attack does happen, their job will be to remedy what has not worked. It will also be to hold on to the ideals that make our nation a unique experiment in world history.

Prevention means more than just preventing the next attack. It also means preventing the consequences of terrorism from turning us into the Lord of the Flies. The path of that cycle is dark.

---

[1]Anthony Downs, "Up and Down With Ecology: The 'Issue-Attention Cycle,'" *The Public Interest*, 28 (Summer 1972): 38-50.

[2] See summary of polling data at http://www.pollingreport.com/terror.htm. Greg Toppo, "Graduates fear debt more than terrorism," USA Today; May 19, 2005.

Homeland Security Affairs

Volume I, Issue 1 2005 *Article* 2

Summer 2005

Transforming Border Security: Prevention First

Robert Bach*

*Naval Postgraduate School, Center for Homeland Defense and Security, rbach20010@aol.com

Transforming Border Security: Prevention First

Robert Bach

Abstract

The events of September 11, 2001 caused the nation's leaders to accelerate existing border programs aimed at prevention. Traditionally, the "prevention" of border violations has involved interdiction (physically impeding any incursion while it is occurring), preemption (through routine screening to intercept illegal shipments, weapons, people, or other illicit cargo), and deterrence (where an action taken means a potential violator does not plan or even attempt an illegal entry). While effective in some cases, none of these strategies – together or separately – has evolved into a comprehensive, prevention-oriented approach to border security. The development of a prevention-led border strategy would involved at least four strategic shifts: aligning border security with global strategy; forging a new foreign policy; making progress on cooperation; and changing U.S. reactive approaches.

AUTHOR BIOGRAPHY: Dr. Robert Bach is an internationally recognized expert on immigration and border security issues. He recently served with the U.S. Department of Homeland Security, Border and Transportation Security Directorate, on air passenger, cargo and other screening initiatives, and policy and privacy development and coordination. From 1994 to 2000, Dr. Bach was Executive Associate Commissioner for Policy, Planning and Programs at the Immigration and Naturalization Service. He worked extensively on border and international issues, including anti-smuggling/trafficking issues, and cooperated with state and local officials and communities. His recent publications include peer reviewed articles entitled "Global Mobility, Inequality and Security;" and "Western Hemispheric Integration and Migration in an Age of Terror." Dr. Bach has been a senior fellow at the Carnegie Endowment for International Peace and the Inter-American Dialogue, and was a faculty member at the State University of New York at Binghamton from 1978 to 1997.

KEYWORDS: prevention, interdiction, preemption, deterrence, global strategy, foreign policy, border control

Long before September 11, 2001 strategists recognized that prevention was a priority among concepts of national security. Military strategy had generally accepted "forward deployment" of assets and influence as core tactics to deter opponents from taking aggressive actions and quickly interrupting them once they began. Law enforcement strategy has developed more slowly in adopting a preventive approach. Still, at least by the late 1980s and throughout the 1990s, the presidential directives of both Republican and Democratic administrations had ordered law enforcement agencies to deploy resources abroad to intercept and disrupt threats as far from the U.S. border as feasible. Under those directives, the Federal Bureau of Investigation (FBI), the Drug Enforcement Agency (DEA), and the Immigration and Naturalization Service (INS), among other domestic law enforcement agencies, initiated overseas operations and deployments.

The events of 9/11 pushed prevention to new prominence in both military and civilian law enforcement strategies. Forward deployment became active preemption, including regime change, as military forces landed in Afghanistan and Iraq. Domestically, Congress rushed to create The USA PATRIOT Act, granting law enforcement authorities greater investigative powers to search and pre-empt a terrorist attack from within the United States.[1] The Bush Administration revised its national security and counterterrorism strategies explicitly to elevate prevention to the Nation's first priority.[2]

Despite the significance that Congress and the president attached to the concept, however, prevention remains one of the least understood dimensions of the Nation's new security strategy. Nowhere is this more evident than in the Nation's efforts to transform its approach to border security. Within two months of 9/11, the president issued Homeland Security Presidential Directive #2 (HSPD-2) seeking to strengthen and shift border security strategies. The president returned to the topic of border security in at least three subsequent Presidential Directives. Yet, the role of prevention in border security strategies remains elusive.

The purpose of this article is to examine several of the primary border security reforms taken since 9/11 to understand and gauge progress toward making prevention the top priority. Not surprisingly, the violation of border controls that made the 9/11 attacks possible caused the nation's leaders to accelerate existing border program reforms. The Presidential Directives served to a large extent to wrench current border projects that had stalled amidst the nation's polarization over immigration policies from previous bureaucratic and political entanglements. Still, few of these rescued border initiatives satisfied the compelling requirements that making prevention a national priority demanded.

THE CHALLENGE

Post-9/11 border security strategies suffer from a familiar policy tale. In recovering from a crisis, institutions try to correct mistakes that led to the earlier events, only to ignore the potential for future, somewhat different ones. With the exception of a few illustrative initiatives, recent border security policies have attempted to accelerate and fully implement programs designed before 9/11. Valuable in their own terms, when complete the projects may well help to solve problems with international travel, visa and

immigration policy, and crossborder commerce. The question is whether they address the new risks and threats of the post-9/11 age of terror.

Given the nature of the 9/11 attack, and the weaknesses of border security that it exploited, moving first to close the obvious gaps in border security was entirely understandable. These early steps, however, reinforced an earlier reactive orientation in border security policies and competed against proposals for more prevention-oriented reforms. For example, HSPD-2, released on October 29, 2001, aimed at changing immigration policies by creating a capacity to deny entry, detain, prosecute and deport aliens associated with or suspected of engaging in terrorist activity.[3]

Federal agencies responded to the Directive by accelerating efforts to track, investigate, and prohibit activities inside the United States. The Department of Justice set up the Foreign Terrorist Tracking Task Force. Border security agencies expanded their investigative participation in FBI-led Joint Terrorism Task Forces. The INS barred international students already studying in the United States from courses that involved sensitive material. The Presidential Directive also urged agencies to develop and use advanced technologies to locate and apprehend suspected terrorists, or supporters of terrorism, inside the United States, even if existing legal restrictions on the use and analysis of data had to be overcome.

At this early date, perhaps the only forward-leaning prevention initiative involved the Directive's reference to developing "North American Complementary Immigration Policies." HSPD-2 called for immediate negotiations with Canada and Mexico "to assure maximum possible compatibility of immigration, customs, and visa policies." The goal was to establish a North American screening perimeter in which border agencies from all three countries would use comparable, if not the same, standards for inspecting individuals seeking to enter the region. Having secured the perimeter, subsequent action could facilitate movements across the two "internal" borders separating the United States from Mexico and Canada.

Although the direction was promising, the programmatic response was reserved and disappointing. Border agencies crafted a Smart Border Initiative, which essentially repackaged a list of incomplete immigration and customs projects started in the 1990s and reset accelerated schedules for deployment. The goal of most of the Initiatives' specific projects was to strengthen or "harden" the physical and virtual borders between the United States and its two neighbors. Little progress was made to standardize screening procedures among the three countries or even to begin to negotiate coordination of efforts.

Part of the problem in beginning to transform border security strategies was due to ambiguities in defining prevention. Prevention at the border called for tough choices about relationships with neighboring countries, which few were willing to take on in the absence of clearly defined goals and objectives. Before 9/11, prevention at the border typically meant interdiction – searching, locating, and physically stopping an effort to cross or to carry something across the border. Interdiction was the priority – physically impede any incursion while it was occurring. Within a broader scope of prevention, however, interdiction represented only one of several ways in which attacks or illegal behavior could be stopped.

Prevention, for instance, also refers to preemption – detecting and stopping an attack before it is attempted. In border security terms, active screening of information related to

travelers and cargo is a routine pre-emptive measure. For decades the U.S. Customs Service has employed cargo screening tactics as a way to intercept illegal shipments, weapons, people, or other illicit cargo within containers before they are shipped toward the United States.

Prevention at the border also refers to deterrence, although what is meant by deterrence has also been confusing. Generally speaking, in border security terms, deterrence means that because of an action taken, a potential violator did not plan or even attempt an illegal entry. Deterrence is by far the most valued form of prevention. Yet few agencies embrace it fully because of the inherent difficulty of defining and measuring deterrence in tactical and operational terms. The problem is not restricted to border agencies. Law enforcement personnel across the globe face similar challenges. They struggle to find a way to demonstrate the effectiveness of a deterrence approach when what appears to be required is to show that an illegal act did not occur because of a law enforcement agency's actions. Does the fear of arrest and detention, for instance, deter someone from deciding to leave their home, pay a smuggler, and attempt to cross the border illegally?

Border security strategies, before and after 9/11, have involved some measure of each of these three dimensions of prevention. Each has guided border security agencies toward different policy and operational outcomes. Together or separately, however, none has evolved into a comprehensive, prevention-oriented approach to border security. The discussion in the following sections highlights the limitations of each approach and identifies steps that could transform policies toward a more prevention-centric strategy.

Border Interdiction

In the early 1990s, the U.S. Border Patrol revised its strategic plan to emphasize a new objective -- "prevention through deterrence."[4] The new plan changed the strategic focus from a traditional policing model in which the object was to maximize the number of arrests of people who had already crossed the border illegally. The new objective was to ensure that no one crossed the border in the first place, stopping them physically right at the border if need be, or inhibiting their attempts to cross by increasing the expectation among potential crossers that they would be caught immediately. The intent was clearly to move away from a reactive, responsive-oriented approach toward a more pro-active, prevention strategy.

The new strategic plan began to change border control tactics. The Border Patrol launched a series of highly-publicized border operations during the 1990s – Operation Hold-the-Line, Gatekeeper, Safeguard, etc. – which involved "forward deployment" of agents and equipment as close to the international boundary as feasible. Rather than waiting for crossers to enter the United States and then physically interdicting them, the Border Patrol placed officers in high visibility locations close to the border, deployed lights in otherwise darkened areas that formerly were places of illegal entry, and broadcasted publicly the intent to dismantle crossborder smuggling activities.

Although the difference between deterrence and interdiction was minimized by the short physical distance at the border between officers deployed close to the international line and the potential crosser in front of them, the changed tactics began to have visible impacts in the areas of high operational concentration. Border Patrol apprehensions ("arrests") declined, smuggling rings were visibly disrupted, community perceptions of

the safety of border neighborhoods improved, and local leaders increased their support of the security strategy. The prevention orientation also reduced public perceptions of the prevalence of social disorder and chaos along the border. In turn, improved security opened opportunities for greater cooperation among agencies across the border.

For instance, building upon the realities and perceptions of increased border security, the Border Patrol's parent agency, the INS, was able to expand legal immigration initiatives. It expanded and improved border infrastructure that expedited legal crossings and reduced the long lines of vehicles and pedestrians waiting at ports of entry for inspection. The INS was also able to strengthen cooperation with Mexican and Canadian officials on these positive commercial initiatives and gain assistance on additional anti-smuggling prevention measures.

These prevention measures, however, stimulated criticism and opposition from diverse stakeholders. One of the lessons learned from the general law enforcement community when it has tried to implement similar prevention measures is that opposition comes initially from those who believe the strategy is too weak as well as from those who perceive it to be too intrusive in community affairs.[5] Hard-line opponents resist the concept that a decline in arrests can be a good outcome. In contrast, some community activists believe that the Border Patrol has no business enforcing immigration laws anywhere except along the physical line of the border.

The public controversy about the border strategy became part of a general criticism of the performance of the INS and other border security agencies. By 2000, the pace and effectiveness of the new Border Patrol strategy had slowed, having reached only the urban areas of El Paso, San Diego, Brownsville, and Nogales. Although the new strategy was still in force, the execution of the strategy waned. Previously disrupted smuggling rings retrenched in new areas along the border, cooperation with Mexico declined, and public support quieted. Even before 9/11, long lines returned at the ports of entry and arrests of illegal crossers between the ports of entry increased as border agencies returned to old tactical habits.

After 9/11, the Department of Homeland Security (DHS) faced the daunting task of reinvigorating the border strategy on both the Mexican and Canadian borders. Under mounting public pressures, the new Agency launched initiatives in Arizona to counter the weakest spot along the border – the area where execution of the earlier strategy had stalled. These new efforts, however, have not been successful in reducing the illegal flow or changing its composition and character. Part of the reason is that the Border Patrol and its new parent, Customs and Border Protection, have concentrated on interdiction rather than prevention. New performance incentives have reinforced the value of tactics that increase, not decrease, the number of arrests. The agencies' attention has also returned to efforts to track, locate, and detain illegal immigrants, and to maximizing the physical removal of unauthorized crossers after they have been prosecuted.

Reports of Al Qaeda's interests in smuggling terrorists or weapons across the Southwest border have only very recently begun to challenge the inherent limits of these latest border control strategies. An enforcement posture focused on intercepting smuggled persons after they have reached U.S. soil, and often after they have made it to an interior urban area, offers little protection and reassurance. Rather, it reinforces public perceptions that the border is "out of control" more generally.

A prevention-first strategy, especially for the Southwest border, should include a dramatic reinvigoration of the full, comprehensive approach to the border initiated with the 1994 Border Patrol Strategic Plan. Further improvement in the capacities of the Border Patrol is necessary, and they may come with the new American Shield Initiative (ASI) already embraced by Congress in the 2006 budget. Yet ASI or other operations will simply not suffice if they remain rooted in an approach preoccupied with interdiction, detention and removal rather than deterrence and prevention in general. A comprehensive plan requires renewed cooperation with Mexican officials on prevention, aggressive bilateral attacks on smuggling rings on both sides of the border, and a new spirit of engagement in promoting the economic well-being of residents all along the border.

Border Screening

Border security strategies rooted in "prevention through preemption" primarily involve the use of information screening techniques. The purpose of screening is to identify and stop those who are in the act of committing a border-related violation before they have a chance to start. Federal border security agencies have long conducted screening of cargo and people approaching the United States through sea and air. These efforts expanded dramatically during the 1990s and were extended to travel and transportation routes that approached the border by land. In the early 1990s, for instance, the U.S. Customs Service and the INS merged separate screening initiatives into a single, advanced passenger information system to obtain and review information on travelers before they landed in the United States. The database and the core technology created for this system still serves border agencies today.

Though the infrastructure may be outdated, the concept of advanced passenger or cargo information remains sound. Such initiatives clearly serve to forwardly deploy the analytical capacities of border agencies. The more information on cargo and people destined for the United States that is received and analyzed before departure from the country of origin, the more effective and efficient processing of the decision to admit or not can occur. These advanced information systems also help to increase U.S. security influence abroad by framing international agreements that foster cooperation to enforce common standards for travel documents and cargo manifests.

During the 1990s, U.S. border agencies also began to collect biometric information on border crossers. Initially, the initiative involved fingerprinting apprehended illegal border crossers through a system known as IDENT. The system provided a two-fingerprint identity check the INS used to identify criminals among apprehended illegal migrants. In 1996, Congress also required the INS to begin to develop an Entry-Exit system that could match the identity of a person when he entered and left the United States. Both systems would substantially increase the ability of border security agencies to track international travelers and intercept anyone of special interest. Before 9/11, these systems had merged to form the backbone of the US-VISIT program, a widely proclaimed border inspection system that compares the fingerprints of international travelers upon entry to the United States with the same biometric taken upon their departure.

After 9/11, Congress and the Administration embraced US-VISIT as the primary innovation to create a border security screen against terrorism. Although the system was

not designed for that mission, Congress and DHS accelerated its deployment from airports to land ports-of-entry. In 2004, the 9/11 Commission's recommendations reinforced support for the program.[6] The Commission noted that US-VISIT helped to establish a sequence of "checkpoints" through which potential terrorists and terrorist supporters would have to pass on their way to and from the United States.

Without further review of the potential value of US-VISIT for this new anti-terrorism mission, the Administration fully embraced the Commission's recommendations. It issued another Presidential Directive, HSPD-11, that pushed DHS to demonstrate a resolve to fulfill the Commission's proposals by creating a comprehensive anti-terrorist screen.[7] Building on HSPD-6, which had already called for creation of and use of screening information, HSPD-11 called for development of a plan to build comprehensive, coordinated procedures to detect, identify, track, and interdict people, cargo, conveyances, and other entities and objects that posed a threat to homeland security.

Some of the proposals for the collection and use of screening information have sparked considerable public controversy, and support for screening efforts may have begun to dwindle significantly. Recently, both Senate and House Appropriations Subcommittees have deleted funding in the 2006 Budget for DHS' planned Office of Screening Coordination and Operations. The Office was designed specifically to manage information collection, coordination, screening, and risk assessment activities.

One reason for this decline in support is that border agencies have failed to convince Congressional and public stakeholders that these systems and activities are effective. Proponents inside the government often do not understand the limits and purposes of the advanced screening techniques and have oversold their promised effectiveness. Critics of information-based screening systems have also generally misrepresented their expected value in two ways. First, critics and proponents alike have concentrated on the value of these systems for border interdiction and overstated the expectation that they can target specific terrorists. Screening systems, such as US-VISIT, actually have a very low chance of detecting a specific target, partly because the number of terrorists is so small, compared to the entire population of international travelers or domestic air passengers, and partly because they are not built to make precise determinations of individual behavior. If a screening system as analytically immature as US-VISIT actually could identify specific terrorists with effectiveness, the nation would be in much less danger than most observers believe.

Second, critics in particular have misunderstood the more valuable preemptive and deterrent role of screening systems such as US-VISIT.[8] The typical, overused criticism of border screening systems is that they merely produce a "bubble effect" along the perimeter of the United States. Enforcement in one area, critics argue, simply displaces the problem, creating greater pressure in another location. The "border as balloon" metaphor may have been useful in a security situation where the threat was a homogeneous, relatively constant pressure. Today, however, the threats facing the border are highly differentiated, disconnected, and fragmented. They are often well-informed by organized, intelligent groups that have a capacity to strike or smuggle, but only in particular places against specific targets. Border security is now much more an intelligent environment demanding advanced risk assessment tools and strategic

operations than traditional encounters of mass force pressuring an outnumbered interdiction force.

The value of US-VISIT and other screening systems is not so much as a targeting tool or a broad physical screen against a large number of intruders as it is a source of information for effective analytical and intelligence work. Its primary value is to help assess and prepare the environment to give U.S. security agencies a much greater ability to preempt and deter potential aggression.[9] The biometric requirements for the system, for instance, aid U.S. consular officers abroad in their efforts to establish the identity and perform background clearance checks for visa applicants while they remain abroad. The recently reported drop in visa applications in some countries of concern apparently reflects, at least in part, fraudulent applicants abandoning their intended course of action.

DHS' Cargo Security Initiative (CSI) is another example of a screening system that can be used in limited fashion as a targeting tool or more expansively as part of a comprehensive prevention strategy.[10] The U.S. Customs Service began in the 1980s and 1990s to inspect cargo at the point of origin to intercept items of concern before they reached the United States. The expansion of this initiative to its current form forwardly deploys U.S. agents and influence abroad both to inspect cargo as it is loaded on ships and to collect and analyze information on the cargo at each point in the global transportation supply chain.

The compression of time and processing requirements along the U.S. northern and southern borders, of course, makes it difficult for information-based screening to be much more than an interdiction tool. The result is that the demand for timely inspection and facilitated movement across borders puts extreme pressure on efforts to stop each truck, car or person for inspection. Security, in this sense, interferes with crossborder commercial interests even when information collection and screening is intended as a prevention measure. The pressure is then to build more infrastructure, increase the number of inspectors, and use more intrusive technology to accelerate inspection.

Even in these situations, however, alternate, effective screening can be designed more as deterrence and preemption than interdiction at the physical point of border crossing. Pilot programs show that trucks and people can be inspected well before they reach the land port-of-entry. Technology can help provide credentials for pre-clearance, and expanded cooperation with neighboring countries can allow much of this pre-border crossing preparation to occur long before the issue becomes interdiction at the border. Yet faced with the perception that the border is out of control and screening systems are ineffective in targeting, the current policy response is to push for more interdiction capacity, requiring ever increasing personnel to physically close the border.

Interior Enforcement as Deterrence

A third strategic focus of border security involves an effort to achieve deterrence by making enforcement actions inside the United States a decisive disincentive to those who wish to cross the border without authority. The USA PATRIOT Act, for instance, provides new authorities to use immigration violations to help in its pre-emptive investigations of terrorism support networks and financial ties. The objective is to eliminate the ways in which immigration can foster and provide safe haven to potential terrorists.

In practice, however, the USA PATRIOT Act has further complicated the already hopelessly entangled relationships between counterterrorism actions and immigration enforcement. According to public reports, most terrorist investigations in the United States have not resulted in terrorist-related convictions, but ended with the use of immigration authorities to remove a person from the country.[11] Unquestionably, the capacity to remove a terrorist supporter from the United States is a valuable tool to say the least. Yet the public appearance and understanding of these cases is that federal authorities are using the extraordinary powers granted under the PATRIOT Act primarily to achieve immigration enforcement.

This entanglement of anti-terrorism and border control strategies is counterproductive because it undermines the preemptive focus of PATRIOT Act investigations. FBI Director Robert Mueller recognized the potential problem and went out of his way to reach out to immigrant communities to reassure them of the distinction between these security objectives. Yet the problem persists, primarily because domestic immigration enforcement – as traditionally conducted – focuses more on arrest and punishment than on creating a prevention-oriented deterrence strategy. Immigrant communities, rather than serve as sources of good information about potential activities, close up in fear of immigration authorities.

The contentious character of the enforcement of immigration laws in the interior of the United States results primarily from intrusion into local communities. In 2004, for instance, the Border Patrol led a series of raids in a local California community that sparked national controversy. While the operations were legal, the community reaction was so contentious, and the operations so ineffective, that DHS officials apologized publicly for the action and committed to a future policy of restraint.[12]

The controversy over how interior enforcement fits into border security strategy is long-standing. For much of the 1990s, Congress and the Administration debated competing approaches to interior enforcement that, for the most part, contrasted reactive with prevention-oriented strategies. A reactive approach focused primarily on three principles. First, enforcement at the workplace, often in the form of raids, would deter employers from hiring undocumented workers who, in turn, without jobs, would leave the community and return home. Second, borrowing from more general theories of law enforcement, significant penalties, including detention and substantial sentences, would convince migrants to return and stay home. Third, large programs of removal, and a high expectation or certainty of deportation, would eliminate the incentive to try to find work in the United States. Immigration enforcement, in this sense, should conform to tough law enforcement policies, such as California's Three Strikes law. Arrest, detention and removal would create a deterrent to future illegal migration.

In each area, however, interior enforcement comes up short of its goals. Arrests at worksites rarely leave migrants without other work options and many displaced workers return to the same employer. The number of interior arrests continues to climb, but so too does the number of illegal migrants. As both increase, the cost of detention and removal skyrockets. Removal and deportation also fail. The recidivism rate among deported migrants is reportedly very high. Stories from law enforcement officials tell of migrants who are removed from a workplace and deported, only to be seen two days later back to work at the same job.

Even illegal migrants who commit a crime while in the United States, and are imprisoned and subsequently deported, return to the same community in a relatively short period. In one study, over half of illegal migrant felons incarcerated in a California city's jail returned to the same city within two years after deportation – and were rearrested for a newly-committed offense.[13] With such rampant recidivism, traditional tactics do not affect the underlying problem but rather displace valuable resources from other strategies that may be more effective.

The alternative prevention strategy developed in the 1990s was inspired by community-policing innovations. Its primary goal was to deter illegal activities throughout a community, starting with those areas in which local communities and INS could cooperate, including local crimes, social disorder, and delinquency. As cooperation increased, the focus could turn to problems related to drug smuggling, human trafficking, labor abuse and fraud. Operations were also designed to protect victims of crime regardless of their status as local residents or newcomers.

The alternative strategy also concentrated on anti-smuggling operations, especially on U.S. residents complicit in organizing and assisting people to cross the border illegally. With these initiatives, domestic immigration enforcement was on the path parallel with investigations of organized crime. The objective was to hold accountable those who were responsible for the financial and employment connections that assisted migrants. Early investigations, using the wiretap authority granted INS by the 1996 law, demonstrated that fairly large employers in Georgia, Texas and the Midwest were directly involved in conspiracies to smuggle people across the Southwest border.

The alternative domestic strategy also aimed to transform the incentives and conditions of local labor markets in the United States that sustain a silent, yet profound, corruption of the U.S. political economy.[14] As deterrence, rather than a punishment-oriented strategy, the operational focus was on changing the conditions that existed before employers were charged and workers were arrested and deported. Employers were given tools to improve their level of compliance with existing laws, including an innovative information system that allowed them to check the legal status of newly-hired workers.

Like similar prevention measures taken in border communities, these innovations generated opposition from both sides of the political spectrum. As the history of community policing forewarned, community activists objected to an approach that tried to improve the relationships between local residents and immigration officials. Law enforcement critics, in contrast, objected to actions that did not obligate INS officers to arrest and deport individual migrants. Prevention steps appeared "too soft."

In the years following 9/11, DHS dropped a community-oriented approach to interior enforcement and tilted entirely toward an arrest-and-deport strategy. Reportedly, Bureau of Immigration and Customs Enforcement (ICE) leadership rejected the preventive approach, calling it "social work." In staff meetings, ICE leaders pressed agents to focus on high-profile prosecutions and convictions of other crimes. Apparently, even though protection against terrorism was quickly embraced as the top priority, prevention of terrorism did not include efforts to deter illegal immigration.

DHS now has the challenge of reengaging in preventive strategies toward border enforcement. Public pressure is mounting over both the perceived weaknesses of current operations and their high costs. So far, DHS appears to be continuing down the path of

ever-expanding detention and removal priorities. No evidence exists, however, that this time the path will lead to more effective outcomes.

The Administration has also proposed another familiar mitigation strategy related to illegal workers. Current proposals call for a new guestworker program designed to solve the workplace enforcement challenge by legalizing workers employed in certain industries. Very little in the proposal, however, seeks to change the circumstances that attracted employers to hire illegal workers in the first place, increase compliance with regulations, or create alternatives for employers or legally resident workers to reduce the demand for these workers. In the past, contract labor markets have given way, with time, to renewed illegal immigration. Without changing the underlying conditions, current proposals may not prevent a recurrence of existing problems.

STEPS TOWARD PREVENTION

In each area of border security strategy discussed above, program development since 9/11 has consistently pulled interdiction back on the stage as the top priority, often by replacing prevention-oriented approaches. DHS has moved back to reaction, mitigation, and recovery. Undoubtedly, transformation to a new, different set of priorities would be difficult and organizationally wrenching at a time when there are numerous issues competing for leadership attention. Still, the nation is not trying to solve border security problems of the past. It is trying hard to improve border security to help prevent the next attacks.

The value of prevention as the nation's first priority is not limited, of course, to an interest in border security. Rather, transformation of a border security strategy must be aligned with and live up to broader and more comprehensive principles of the nation's foreign and domestic policies. Prevention deserves its place as the nation's top priority because it encompasses both the necessity to achieve security and an ambition to improve the human condition throughout the global community. Ultimately, prevention is dependent on human freedom and, as Nobel Prize economist Amarty Sen reminds us, the existence of viable choices to achieve basic human security.

During the Cold War, containment strategy offered the world a set of these choices. Alliance with the free world brought participation in world trade, foreign aid, and open cultural expression. Opposition induced blockades and boycotts. Individuals throughout the world also understood that if they resisted Soviet-backed repression they would be encouraged and welcomed in the West. U.S. strategy aimed not only to stop opponents from aggression, but also consistently to encourage nations, groups, and individuals to opt for the path of freedom.

Understandably, since September 11, 2001, strategists have focused much more on suppression of actions than on expansion of choices. Yet, the success of the nation's security strategy will require taking action to create viable alternatives to the current conditions that give rise to terrorism, illegal immigration and other illicit efforts to defeat U.S. border controls. It will require a transformation of the nation's security plans and will not be achieved simply by solving challenges that face border inspectors and patrol officers.

Positive steps toward transformation call for a bold, bipartisan approach. The current Administration's democracy initiative, for example, aims to expand choices in parts of

the world that for decades have enjoyed few. Regardless of how far that initiative still must go, the objective to expand human freedom is sound. Steps toward transformation also embody the earlier priorities of former Democratic administrations that focused on adherence to fundamental human rights as requirements of participation with the United States in global initiatives.

In that spirit, moving toward a prevention strategy of border security will require new policies toward our neighbors, Mexico and Canada, and toward other migrant-sending countries. It will require new forms of cooperation, many of which have been resisted until now or not yet even imagined. Sending countries, for instance, will need to accept greater responsibility for the conditions of their citizens in migrant-origin communities.

Unfortunately, current understanding of crossborder and transnational movements is rooted in a philosophy and perspective that denies freedom and choice as essential strategic goals. Many social scientists, policymakers and advocates, for example, believe that the current forms of migration and border problems in general are inevitable conditions. Some social scientists, for instance, mistake progressive ideas about the severe constraints on opportunity from unequal labor market structures with historical determinism and lack of human accountability.[15] The Mexican Government routinely asserts that its current mismatch between job and population growth rates will "inevitably" cause emigration. Advocates in the United States, such as the Essential Worker Coalition, argue that particular groups of workers are necessary for certain segments of the economy. Inevitability and necessity, however, defy freedom. Prevention needs to be understood more fully in terms of a capacity to create options that outweigh the seemingly "inevitable" patterns and limitations of current circumstances. Without options, border strategy shrinks to debates on management tactics, arguments over interdiction and ever-escalating levels of punishment.

Among a wide range of next steps, transformation toward a prevention-led border strategy would involve at least the following four strategic shifts.

1. Aligning Border Security with Global Strategy: Transformation toward prevention requires a much more forward-leaning foreign policy toward countries of emigration. For many migrant-sending countries, this will involve a radical shift of orientation. U.S. immigration policy remains largely a Cold-War artifact. As mentioned previously, in the days of Cold War rivalries between East and West, the benefit of an alliance involved easier access to the U.S. market, regardless of the means, mechanisms or conditions. The Mexican Government, for example, continues to operate within this framework. It currently expects that its "special relationship" with the United States should lead to an exceptional migration agreement as part of its overall alliance with its neighbor.

In the 21st century, however, alliances involve non-state actors at sub-national levels as much as if not more than homogeneous state-to-state interests. Opposition is differentiated, decentralized, and asymmetric. As with commercial trade agreements, policies toward migration should increasingly reflect more than volume and ease of movement. They must include agreement on the standards of what crosses, who certifies and takes responsibility for its legality, and how to ensure compliance. Unlike in the days of the Cold War rivalry, sending governments must be willing and supportive of efforts to create viable options to illegal entry into a friendly neighboring country.

2. Forging a New Foreign Policy: Border security requires a realignment of policies with the nation's neighbors, especially Mexico. For decades, the Mexican Government has insisted that it has little responsibility for the enormous and sustained movement of its citizens across U.S. borders without U.S authorization. It has rested that perspective on an interpretation of a Constitution written almost a hundred years ago during an authoritarian moment when security and freedom in Mexico required the ability to escape tyranny. Today, Mexico is capable of creating options and taking responsibility for its citizens. Yet the government refuses to take even minimally effective public safety action to prevent its citizens from endangering themselves and families by accepting smuggling arrangements.

For its part, U.S. policy no longer needs to rely on slowly nurturing democratic reforms in Mexico to ensure stability. Mexico is now moving forcibly toward democracy and it is time to for the United States to forge a more forward-leaning partnership with reform elements in Mexico. The North American Partnership of 2005 could become a good initial step in these reforms if its implementation is prevention-oriented, and not just a framework to maintain the status quo.[16] At present, publicly-announced programs within the Partnership remain limited to familiar efforts to build a common screening perimeter and to coordinate emergency responses.

3. Making Progress on Cooperation: One of the challenges to achieving a prevention-oriented border strategy is the persistent inability to make cooperation work. Transformation of border security is a large, comprehensive task not to be reduced to improvement in single systems, deployment of greater resources, modernization of technology, or even new policies designed to change the volume and characteristics of migrants and travelers in general. A goal of creating "One face at the border," for example, is a solution to the management problems of the last fifty years. What is needed is a strategy for conducting border security in the 21st century.

A prevention strategy would include a network of allied, multinational customs and migration officers working together to enforce minimum standards at critical points of international travel. The Cargo Security Initiative described previously is a constructive step in that direction. It will benefit both the United States and the entire world trading system. Immigration officials could also deploy overseas, although there has been much more opposition to that move. In the late 1990s, however, five countries joined in a pilot program to test the value of such forwardly-deployed coordination. Officials from each of five countries were placed overseas working alongside officers in the sending and transit countries. The results showed that in just a few weeks of coordinated action, officers were able to prevent more people with false documents and identities from boarding planes for the United States than inspectors working only from their traditional position in U.S. ports of entry were able to detect in a three-month period.

Despite declarations of the need for shared responsibility for migration and border matters, the realities are that implementation of prevention measures strains governments' commitments. Even after the urgency of 9/11, coordination and joint decision-making on border security measures remain difficult. The United States and Canada, for example, are struggling to achieve even a limited agreement on coordinating with each other on decisions related to visa waivers for the new member countries of NATO.

4. Changing U.S. Reactive Approaches: The myth of workplace enforcement as a deterrent to illegal immigration highlights the way in which current strategies have a corrupting influence on U.S. domestic policy in general and labor policy in particular. An effective strategic choice should not be between "essential" and "non-essential" workers, as the reform debate in the United States currently poses the issue. A prevention priority must involve active pursuit of a range of alternatives for employers and workers alike, creating more opportunities and more options.

The difficulties in making these four initial strategic shifts underscore a deep-seated barrier to effective, prevention-oriented border strategies. Prevention requires trust, both between agencies that must share information, leads, and enforcement action, and more fundamentally among the public in each country that must perceive and accept legitimate and effective actions on both sides of the border. Even the three members of The North American Partnership lack the degree of social trust required to forge new, prevention-oriented cooperative strategies.

CONCLUSION

The 9/11 Commission faulted U.S. leaders for a failure of imagination in preventing the terrorist attacks. Unfortunately, in the realm of border security strategy, little evidence exists that federal leaders have reached beyond their commitment to hard work and accelerated implementation of long-standing initiatives and policies. Perhaps the Commission was wrong, and what is needed is only enhanced performance and more resources. Yet, the persistent call for a new prevention priority should challenge leaders to go beyond implementing border security programs correctly. The question is whether they are pursuing the correct programs.

Prevention, in the sense used throughout this article, is a concept that gives priority to imagination. It requires creation of alternatives to both existing conditions and widely-accepted perspectives. It also demands answers to the hardest questions. What would it take for a certain behavior not to occur? What would it take to give potential terrorists, and fraudulent travelers, viable alternatives? In this age of terror, the answers are consequential.

---

[1] *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001*(USA PATRIOT), Public Law 107-56, (October 26, 2001), section 414.

[2] *The National Security Strategy of the United States of America* (Washington, D.C.: U.S. Government Printing Office, September 2002).

[3] Office of the Press Secretary, "Homeland Security Presidential Directive/HSPD-2," (The White House, October 29, 2001).

4 U.S. Immigration and Naturalization Service, *Border Patrol Strategic Plan: 1994 and Beyond* (Washington, D.C., July 1994).

5 On the question of popular legitimacy for enforcement actions, see Mark H. Moore, "The Legitimation of Criminal Justice Policies and Practices" in *Perspectives on Crime and Justice: 1996-1997 Lecture Series* (Washington, D.C.: National Institute of Justice, Volume 1, November 1997), 47-63.

[6] The 9/11 Commission Report, *Final Report of the National Commission on Terrorist*

Attacks Upon the United States (New York: W.W. Norton 2004).

[7] Office of the Press Secretary, "Homeland Security Presidential Directive/HSPD-11," (The White House, August 27, 2004).

[8] Rey Koslowski, *Real Changes for Virtual Borders: The Implementation of US-Visit* (Washington, D.C.: Migration Policy Institute, 2005).

[9] *Enhanced Border Security and Visa Entry Reform Act of 2002*, Public Law 107–173, section 302 (May 14, 2002). *The Intelligence Reform and Terrorism Prevention Act of 2004*, House Report 108-796, Section 7208.

[10] See Stephen E. Flynn, "America the Vulnerable," *Foreign Affairs* 81, No. 1 (Jan./Feb. 2002), 60-74.

[11] See Mary Beth Sheridan, "Immigration Law as Anti-Terrorism Tool," *The Washington Post*, Monday, June 13, 2005, Page A01.

[12] See, for example, Elena Shore, "Immigration Raids in California Test Spanish-Language Media," Pacific News Service, June 17, 2004, www.IMDiversity.com.

[13] Immigration and Naturalization Service, "Internal Briefing," Office of Policy and Planning, 1999, author's notes.

[14] R.L. Bach, "Western Hemispheric Integration and Migration in an Age of Terror," forthcoming in Kristof Tamas and Joakim Palme (eds.), *Globalizing Migration Regimes: New Challenges to Transnational Cooperation* (Aldershot: Ashgate, 2005).

[15] R. L. Bach, "An Essay on Migration and Possibility: Commentary on the Human Development Report 2004," presented at a joint seminar of the United Nations Development Program and *Foreign Policy Magazine*, held at the Carnegie Endowment for International Peace, June 22, 2004. Also, see R.L. Bach in "Global Mobility, Inequality and Security," Chapter 4 in *Human Insecurity in a Global World*, Lincoln Chen, Sakiko Fukuda-Parr and Ellen Seidensticker, eds. (Harvard University Press, 2003), 65-85; also published in *Journal of Human Development*, 4, No. 2 (July 2003).

[16] The White House Office of the Press Secretary, "Security and Prosperity Partnership of North America Security Agenda," Washington, D.C., March 23, 2005.

Homeland Security Affairs

Volume I, Issue 1 2005 *Article* 3

Summer 2005

What is Preventing Homeland Security?

Christopher Bellavita*

*Naval Postgraduate School, christopherbellavita@gmail.com

What is Preventing Homeland Security?

Christopher Bellavita

Abstract

Almost four years have gone by since the United States formally joined the global war on terrorism. Yet something stops us from giving as much attention to preventing terrorism as we give to preparing to respond to the next attack. One reason is a homeland security system that is designed for response rather than prevention. Three fears hamper efforts to reconfigure that system: the fear of new behaviors; the fear of imagination; and the fear of emergence. Despite these barriers, we know more about prevention than most people in Homeland Security are aware of. The *Preparedness Guidelines for Homeland Security*, issued in 2003 by the DHS, identifies five elements of a cohesive prevention strategy: collaboration, information sharing, threat recognition, risk management, and intervention. These *Guidelines* provide a good initial framework for effective prevention. We can continuously improve the *Guidelines* by transforming them from a proprietary to an "open source" project within the public safety community.

AUTHOR BIOGRAPHY: Christopher Bellavita teaches in the Masters Degree program at the Naval Postgraduate School in Monterey, California. An instructor with twenty years experience in security planning and operations, he serves as the Director of Academic Programs for the Center for Homeland Defense and Security. Prior to joining NPS, Dr. Bellavita was the executive director of the Utah Olympic Public Safety Command. He received his Ph.D. from the University of California, Berkeley.

KEYWORDS: bias towards response, fear of new behaviors, fear of imagination, fear of emergence, collaboration, information sharing, threat recognition, risk management, intervention, Preparedness Guidelines

"I don't think you can win [the war on terror]."
– George W. Bush

"He was talking about winning it in the conventional sense ... about how this is a different kind of war and we face an unconventional enemy."
– White House spokesman Scott McClellan[1]

May 20, 2005 passed with little notice in America. It marked 1,347 days since the September 11th attack. The same number of days separated December 7, 1941 from the end of the Second World War. This "different kind of war" will not end. There is no politically palatable way for a leader to say, "OK, we won. The Global War on Terror is over. Everyone go back to Green."

Like its semantic relatives the War on Drugs and the War on Poverty, the Terrorism War will last as long as there are homeland security industries, bureaucracies, and congressional committees. And an enemy. There is no war on terrorism without terrorists – considered now, under U.S. law and sentencing guidelines, as anyone whose action "appears to be intended to intimidate or coerce a civilian population."[2] Since a terrorist can include criminals who fly planes into buildings, detonate bombs at sporting events, set SUVs on fire, release laboratory animals, and make methamphetamines, we will never run out of terrorists.

PREVENTION REMAINS OUR FIRST NATIONAL PRIORITY

Because we are in this for the long run, it is important to remember what we are trying to accomplish. The National Strategy for Homeland Security published in 2002 identifies prevention as the first of four goals. In April, 2005, Department of Homeland Security (DHS) Secretary Michael Chertoff reaffirmed the importance and priority of prevention when he told Congress our homeland security strategy was to keep terrorists "off the boards, prevent them from coming in, prevent them from shipping their stuff in, protecting our infrastructure and transportation if they do get in, and then if worse comes to worst, … being able to respond the *[sic]* mitigate the harm."[3] In word, if not in deed, prevention remains our first priority.

After more time than we devoted to Word War II, how are we doing? We have not been attacked in almost four years. By the end of 2005, we will have spent about 175 billion dollars on homeland security. Information sharing, while not perfect, has dramatically improved – at least among law enforcement agencies. We have a dozen homeland security-related national strategies; fifty-plus state and territory strategies; thirteen homeland security presidential directives; and a growing mound of implementation guides, cloaked by such New Deal-sounding acronyms as NRP, NIMS, NPG, NIPP, UTL, and TCL.

On the surface, our prevention strategy is working. Look under the surface however, and one is hard pressed to identify what that prevention strategy is.

HAS ANYONE SEEN THE TERRORISM PREVENTION PLAN?

> *The Committee is concerned that while terrorism prevention is a national priority, little is being done to create prevention expertise in our nation's first responders. This is in stark contrast to response and recovery training programs. Without a well-developed terrorism prevention plan, State and local agencies lack a key piece in the fight against terrorism.*
>
> – House Appropriations Subcommittee on Homeland Security, June 2004 [4]

Imagine a parallel universe where World War II is still going on. There is a strategy meeting in President Roosevelt's office. The Director of the Office of Civilian Defense is speaking:

"When the German's attack, Mr. President, here's how we'll be organized. We will use the National System for Managing Any Incident…."

"Wait," says the President, "First tell me how we will prevent the Germans from attacking."

"Well," says the Director, "our National System for Managing Any Incident has a strong prevention component. Everyone will work together and share information. But once we're attacked…."

"Stop. How do we prevent the attack in the first place?"

"Mr. President," says the Director, "You'll recall we have a National Response Plan, and…."

"I don't want to respond," says the President. "I want to prevent."

"The country has not been attacked since December 7th, Mr. President. And the Germans have never attacked our homeland. Our plans are working."

Almost four years have gone by since the nation formally joined the global war on terrorism. Yet something still is preventing us from giving as much – if not more – attention to prevention as we give to preparing to respond to the next attack.

One reason is money. The political economy of homeland security is biased toward response. A lot of money has been made selling equipment and services to first responders. There is a much more limited economic market for prevention. We do not know how much we are spending on prevention because we do not yet have a common understanding of what we do when we are preventing terrorism.

The Homeland Security Appropriations Subcommittee quotation, above, alluded to a "terrorism prevention plan." What is that? Where is it? Why is it taking so long to put together? What is preventing homeland security from preventing terrorism?

IT IS THE SYSTEM, NOT THE PEOPLE

> *"We've got to have a prevention strategy that is focused on finding those terrorists before they act. Very little, I will hasten to add, of what the Department of Homeland Security spends its money on these days is devoted to what ought to be a high priority. We've got to reconfigure in order to do that."*[5]
>
> – Christopher Cox, [Former] Chairman of House Committee on Homeland Security

It would be completely erroneous to say we do not have comprehensive national or local prevention plans because no one wants them. It would be foolish to blame any person or institution for the failure to make prevention the first priority in more than name only. There are many people at all levels of government who take with heart attack seriousness the prevention mission. But we have been at this longer than WWII, and we still do not have a cohesive – or articulated – national prevention strategy. Something is wrong.

Edwards Deming, the continuous improvement authority, used to say, "We are being ruined by the best efforts of people who are doing the wrong thing." To Deming, systems rather than people were the problem. "All that happens comes from the system, not the workers…," he said. "It's absolutely frightening, … just frightening."[6]

The same dynamic is festering in homeland security: the best efforts of the best people are being applied to the wrong things. As Christopher Cox, former Chairman of the House Committee on Homeland Security suggests, the homeland security system is not designed to support prevention as its first priority. It is designed to respond. It is leadership's job to reconfigure the homeland security system, to make the system's outputs conform to the priorities of our national strategy.

"Reconfiguring the system" does not mean simply reorganizing the Department of Homeland Security. A secure homeland is the outcome of national, state, local, private sector and citizen activities. It is not the sole responsibility of any national, state or local agency.

Deming argued for the preeminence of process. If you understand system processes, he said, you can figure out what needs to be done to continuously improve that system. Before trying to redesign the entire homeland security apparatus, however, it may be helpful to examine three systemic fears that get in the way of discovering how the activities of that system – the process – can match the espoused priority of prevention. They are the fear of new behavior, the fear of imagination, and the fear of emergence.

THE FEAR OF NEW BEHAVIOR

In late 2004, public safety executives from a mid western state participated in a homeland security tabletop exercise. The first scenario was designed to stimulate conversation about how to prevent a potential attack from happening. The discussion was low energy and uninspired. Participants were unsure how to talk about prevention.

But then an attack scenario was presented. The exercise moved into response and recovery. Participants became animated. They talked faster, had more detailed

knowledge, and were professionally confident. They demonstrated they knew what to do once an incident has happened.

The same pattern was repeated in more than a dozen similar state homeland security exercises: people participating in the exercises could not grab hold of "prevention" with the same emotion they poured into "response." The reason? The public safety leaders had a lot of experience responding to critical incidents. They had practically no experience sharing at least awareness that they were doing prevention.

New Roles, New Behaviors

Preventing terrorism is a new role for public safety agencies. They are used to responding to daily emergencies, not stopping acts of war. As a generalization, one can say they tend to avoid prevention because they already know how to do response. It is partially a learning problem. Adults and organizations prefer doing things they already know how to do – even if that means redefining the "new" so it looks like the old; hence the demand for new and better response equipment – whether or not it can be used or maintained.

The United States has the world's best disaster response system. With the possible exception of a wide scale biological or cyber attack, we can meet the challenge of any incident – no matter how horrendous. That does not mean we have finished improving our response system. But continuing to make response our de facto priority is like searching for lost car keys under a street light because the light is better there. We know much less about how to prevent. It is in this Terra Incognito we can make the most progress expanding our capability to secure the homeland.

We have a Roadmap for Prevention

While prevention may be a new public safety idea, we know more than most people in homeland security are aware of. In 2003, the DHS issued *Preparedness Guidelines for Homeland Security*. The *Guidelines* have three features that make it unique among the paniculated documents produced since September 11th. It was built from the ground up by first preventers. It was vetted by first preventers. It gave other public safety professionals practical advice about how to prevent terrorism. For some reason, the *Guidelines* are also largely unknown in the homeland security community.

The *Guidelines* identifies five elements of a prevention strategy: collaboration, information sharing, threat recognition, risk management, and intervention. Each of these elements is further divided into specific activities that support the prevention strategy. The two core elements of those *Guidelines* – collaboration and information sharing – cost comparatively little in monetary terms. They mostly require people, organizations and professions to change their attitudes and behaviors. The core elements work only when there is a committed effort to change. Their success is more a function of sociology than technology.

The *Guidelines* can be a foundation for developing local prevention plans. Some jurisdictions – in Kansas City, KA and Frederick County, MD, for example – have already used the *Guidelines* this way.

The *Guidelines* also can help with the thorny problem of how to measure prevention. The prevention activities included within each of the five elements are empirically

derived proxies for prevention. If the elements are present and working effectively in a jurisdiction, there is a greater likelihood a process is in place to prevent terrorism.

The *Prevention Guidelines* – or something similar – are as important to homeland security as the National Incident Management System (NIMS). The national government threatens to withhold funds to jurisdictions that are not "NIMS compliant." If prevention is so important, the Grant Threat strategy could be extended to agencies – and the private sector (perhaps with what amounts to a tax penalty) – that are not "prevention compliant." The *Prevention Guidelines* make concrete what it means to prevent terrorism.

THE FEAR OF IMAGINATION

The 9/11 Commission Report cited the failure of imagination as one of four failures revealed by the attack. The post 9/11 spending hemorrhage has fertilized imaginative technology – although there is no evidence the absence of technology contributed significantly to the September attacks. At the national level, there have been no especially imaginative innovations in policy, strategy or how we are organized to prevent terrorism. The NIMS is a modification of a thirty-year-old template for responding to emergencies. The lackluster "Vision for the National Preparedness Goal" reads like a "what-not-to-do" example in a government writing class. Merging 22 agencies into one is – although on a major league scale – a traditional organizational response to not knowing for sure what to do.

If this truly is, as presidential spokesman Scott McClellan asserts, "a different kind of war," we are still fighting it with old ideas, old structures, and old methods. Four years and counting. Where is the imagination that the 9/11 Commission called for? Here are two ideas: confront the American people with the reality of what terrorism can do to our society, and use free market ideas to predict the risk of specific attacks.

"… nameless, unreasoning, unjustified terror"

Prevention has to mean more than just stopping attacks. It also ought to mean preventing terrorists from achieving the goals their attacks are meant to accomplish. How would Americans react economically, politically, and socially if twenty suicide bombs went off within the same hour in shopping malls all over the country? What if smallpox starts to show up? Or if transit systems in our cities are attacked like London's or Madrid's? What if car bombs start detonating in American cities with the frequency they explode in Iraq? What happens if an airplane is shot down as it takes off from an American airport?

It would cost about 40 billion dollars to install missile defense systems on the nation's commercial air fleet over the next two decades to protect against shoulder fired missile attacks. Experts are split over the likelihood of such an attack. But there is general agreement that the central justification for even considering such an expenditure is because "of the enormous economic consequences that would result if the public were to lose confidence in flying.[7]" The terrorist target is not the airplane, or the mall, or the subway. Bin Laden has made his goal clear. The target is our economy: "We bled Russia for ten years until it went bankrupt and was forced to withdraw in defeat…. We

are continuing in the same policy to make America bleed profusely to the point of bankruptcy."[8]

Thomas J. Housel and Arthur H. Bell argue, in "Limiting the Impact of Terrorist Acts: Accessing the Wisdom Base of a Hardened U.S. Populace," that theAmerican people are insufficiently prepared to prevent the economic and social disruption such an attack would create.[9] History teaches that people as well as critical infrastructure can be hardened against terror. If the enemy wants to wreck our economy by making people afraid to take the subway or go to malls, part of our approach to prevention should be to undercut the power of the terrorist strategy by toughening people against what is likely to happen again in our lifetime. If we are in a real, not a symbolic, war, men and women and children will die. Trying to protect Americans from that truth – as we do with the casualties of the Iraq war – eviscerates one of the fundamental weapons in our prevention arsenal.

Stephen Flynn suggests we are in a "phony war" period similar to the eight months after the Germans invaded Poland in September 1939. Read or listen to what Winston Churchill told the British people: "I have nothing to offer but blood, toil, tears and sweat." His prediction was correct, but the residents of London went on with their lives in spite of daily Luftwaffe air raids. Compare that to the fuzzy way we have prepared American citizens for the next attack – and for what they can do about helping to prevent the attack and – more importantly – the consequences of an attack.

Placing Bets on the Second Attack

The most imaginative strategic idea for fighting terrorism we have so far seen was the Policy Analysis Market (PAM), incorrectly known as "terrorism futures." It was designed to use speculative markets to forecast geopolitical trends. People who did not know what they were talking about perceived it as a way to bet on terrorist attacks.[10] The PAM was an effort to create decision markets about the potential consequences of policy actions. It was premised on the assumption that markets are efficient and effective aggregators of information. Empirically, markets do a better job of assessing risks than reports or experts. It does not get much more American than calling on free market concepts to help prevent terrorism.

But what a ruckus this new idea caused. It was cancelled one day after the project came to the attention of the mainstream press. One might debate the pros and cons of decision markets as a way to look at prevention policies. But that debate never happened. Do we have such a surplus of ideas that we are incapable of withholding judgment long enough to listen to what the idea is before it is killed? What other innovative ideas about policy, strategy, and organization have been blocked by homeland security mind guards?

If public sector decision markets prove to be an advance on our current policymaking capabilities, homeland security will eventually adopt them. But who knows how much time will go by – how many questionable decisions made – before then. In theory, some of the initial stakeholder confusions and disagreements over NIMS, the Target Capabilities List, and other DHS efforts could have been minimized if decision futures markets would have been encouraged to weigh in. But we will never know.

The larger problem is not how the DHS writes rules. It is a system-wide bias against imagination. This can be addressed, in theory, by a commitment to "seek first to understand" ideas before killing them. Perhaps a small reserve of seed funds could be

used for "imagination grants." These would be provided to communities, states, the private sector, and national government agencies – anyone who has an inventive and intellectually plausible idea about how to expand our capacity to prevent terrorism.[11]

The 9/11 Commission called for institutionalizing imagination. That has not yet been done. It needs to be.

THE FEAR OF EMERGENCE

> *During the past three years, many federal agencies … have made efforts to secure input and comments from the state, tribal, and local public safety community. Unfortunately, these efforts are too often limited to participation in advisory panels and working groups that have little impact on policy development and instead are relegated to the role of providing post-development comments on completed, or nearly completed, policy proposals. Consequently, the ability of state, tribal, and local law enforcement to truly influence policy has been minimized.*[12]

The third fear is the dread of what happens if you stop trying to control everything. It is based on a proposition demonstrated by experience time and again: control is not a property of complex human systems. The social, political, and economic world is not a product of control. It is the resultant of an emergent, self-organizing process.[13] That does not mean homeland security professionals play no role in shaping the system. But they are partners, not controllers. Homeland security leaders can benefit from transforming their thinking from a hierarchical to a network mindset.

Envision the textbook pyramid of "How Our Government Works:" the national government is on top, telling the states what to do to the cities and counties. Using the relatively new policy mechanism of the "presidential law," otherwise known as Homeland Security Presidential Directives (HSPD), the national government now tells states and cities what they need to do to secure the homeland. States and cities have allowed this to happen for a variety of reasons – ranging from the perception that homeland security is little more than a way to get grant funds, to the authentic belief that it is the national government's job to set the homeland security agenda.

The national government, partly through default, partly through arrogance, and partly because of the career history of institutional leaders, has welcomed the opportunity to decide what is best for homeland security. Most homeland security guidance documents are the product of this hierarchical mentality. From the National Strategy through the HSPDs and the follow-on suite of implementation documents, the national government has been telling its subordinate units what to do.

Because this is the 21st century, however, it is symbolically necessary to get "input from the locals." But as recent reports from the International Association of Chiefs of Police, the Government Accountability Office, and the Congressional Research Service indicate, the well-meaning efforts at inclusion are largely unconvincing to those on the frontlines of homeland security.[14]

The dominant metaphor driving homeland security aspirations is "the well-oiled machine," steered by an informed central authority. It is based on the theory that if all

the parts – states, cities, private sector, citizens, and the national government agencies – are operating from the same design (e.g., the NPG, NRP, NIMS, TCL, and so on) we will have one integrated system that will achieve the national homeland security strategy.

There are two problems with the metaphor and with the behavior it encapsulates. First, the machine is not designed to do what it should do: prevent terrorism. It is designed predominantly to create and follow rules, and to spend money for response. Second, the exclusionary faith in hierarchy and control sustains a societal vulnerability our enemy has already exploited.

The enemy is networked. We are too, although we could get much better at it.[15] Most people in homeland security know that the way things really get done is through personal networks. But we still talk and act as if a smoothly functioning hierarchy ought to be our goal; blindly maintaining this almost-vestigial twentieth century idea gets in the way of preventing terrorism.

DHS policy says that money should go directly to states, to then be distributed to cities. Politically powerful communities have found ways of effectively bypassing states and going directly to DHS, at times via Congress, at other times by creating the right relationships with DHS and other agency leaders. Funding is as much the product of networks, as of hierarchies.

Review the collection of recent state homeland security plans.[16] Many of these plans were spurred by rather explicit DHS grant guidance. Yet there is extraordinarily wide variation in the plans. The best explanation for why plans were written as they were rests in understanding the network of people and agencies responsible for the plan, not the guidance from the national government.

Monitor how states and cities and counties will implement NIMS. For some communities, NIMS represents a modest extension of what they already are doing. For others it represents a welcome lever to get all agencies to use the incident management system. For still others, it represents yet another intrusive mandate to be worked around. One can predict that the future of NIMS will be the resultant of the same network processes that helped to shape the funding and the planning profiles. It will not be controlled by the national government – not because control is or is not a good idea, but because control is not a property of a complex human system like homeland security.

This is not an argument to eliminate hierarchy. It is a suggestion that since the present system is having such a difficult time pursuing prevention, try something different. Instead of struggling to control what happens in homeland security, use the power of self-organization to see what it can contribute to expanding our prevention capabilities. Use the creativity of communities, states, the private sector, and homeland security professional associations to evolve the next iteration of the *Prevention Guidelines.* Here is how that might work.

First the theory: Many DHS documents talk about the need for policies and strategies to "evolve" as time goes by.[17] "Evolve" is in quotes to emphasize that it has a meaning beyond the general one of "change." From a theoretical perspective, the evolutionary process is quite specific: it includes variation, selection, and reproduction.[18] The first requirement is for variation. The homeland security system already has lots of that – in spite of efforts to minimize unplanned variation. Another word for "selection" is "best practices" (or, more accurately, "smart practices"[19]). If there is an effective process for sharing smart prevention practices, it is informal and underground. It is possible to

develop a mechanism – beyond the DHS Lessons Learned website (www.llis.gov) – that targets a specific set of prevention ideas for possible selection by agencies willing to experiment. The next step is for jurisdictions to adopt – or reproduce – particular smart practices that do work in their environment. This is a naturalist rather than a mechanical model. It is relying on intelligent, co-evolution rather than on intelligent design by committee.

Now the practice: The co-evolutionary approach does not require developing any new implementation strategy. Instead, it represents taking the blinders away to see what is actually happening – networks are organizing homeland security, not hierarchies – and then cooperating with the reality of how things happen, rather than remaining faithful to an ideal about controlling complexity.

Possibly the best example of co-evolution in homeland security is fusion centers. They were not mandated. It just seemed like a good idea that agencies with something to contribute to situation awareness ought to talk with each other. That "variation" of the pre 9/11 compartmentalized intelligence structure was voluntarily selected and voluntarily reproduced by other states and communities.[20]

The target for the self-organizing experiment would be the DHS *Prevention Guidelines.* The 2003 *Guidelines* are not the last word in prevention. They need to be continuously improved as we learn more about what works. In early 2005, a draft Version 2 of the *Guidelines* was released by DHS – but then subsequently withdrawn. The DHS Lessons Learned web site could post the *Guidelines* as a "wiki" to allow broad input into the continuous improvement of what works in prevention.[21]

The idea is to make the *Prevention Guidelines* an "open source" rather than a proprietary project within the public safety community. It is analogous to the development of the Linux computer operating system, where "Given enough eyeballs, all bugs are shallow".[22] We should foster as much variation of the *Prevention Guidelines* as possible. Individual agencies would be encouraged to take the guidelines, adapt them to their jurisdiction, and add what they learn to the *Guidelines*.[23] Let the public safety market of ideas determine what can be done at state and local levels to prevent terrorism.

There have been endless documents produced by committees working inside cathedrals of homeland security orthodoxy. Let us discover if the revised guidelines for preventing terrorism can organize itself, using the wisdom of the "great babbling bazaar of differing agendas and approaches" that makes up homeland security.[24]

---

[1] Julian Borger, "President admits war on terror cannot be won," *The Guardian*, August 31, 2004. http://www.guardian.co.uk/international/story/0,,1293965,00.html [Accessed May 15, 2005]

[2] U.S. Code: Title 18, Part I, Chapter 113b, Sec. 2331. See also, George Bush, Executive Order 13224, September 24, 2001.

[3] Testimony by Secretary Michael Chertoff before the House Homeland Security Committee, Washington, D.C., April 13, 2005. Accessed June 12, 2005 at http://www.dhs.gov/dhspublic/display?content=4460

[4] Committee Report accompanying the *Department Of Homeland Security Appropriations Bill, 2005,* H.R. 4567. http://thomas.loc.gov/cgi-bin/cpquery/T?&report=hr541&dbname=cp108& [Accessed June 12, 2005]

[5] Chris Strom, "Lawmaker challenges companies to develop anti-terror technology," *Daily Brief*, Govexec.com, May 25, 2005. http://www.govexec.com/dailyfed/0505/052505c1.htm [Accessed May 27, 2005]
[6] Carla Lazzaresche, "In Endless Pursuit: A Hero in Japan, Deming Continues His Quest for Quality at Home," *Los Angeles Times*, December 5, 1993.
[7] Eric Lipton, "U.S. Is Set to Test Missile Defenses Aboard Airlines," *New York Times,* May 29, 2005. http://www.nytimes.com/2005/05/29/national/29missiles.html [Accessed June 1, 2005]
[8] Gal Luft, "Al Qaeda's economic war against the United States," *Energy Security*, January 24, 2005. http://www.iags.org/n0124052.html [Accessed May 28, 2005]
[9] Thomas J. Housel and Arthur H. Bell, "Limiting the Impact of Terrorist Acts: Accessing the Wisdom Base of a Hardened U.S. Populace," March 2005 (unpublished).
[10] Robin Hanson, "The Informed Press Favored the Policy Analysis Market," Department of Economics, George Mason University, May 5, 2005. http://hanson.gmu.edu/policyanalysismarket.html [Accessed May 19, 2005]
[11] Imagination grants would not duplicate the goals of the Homeland Security Centers of Excellence program. They would, instead, be short-term, small budget expenditures designed to support a skunk works type exploration of innovative ideas. For an example of a prevention-related idea worth exploring through an imagination grant, see the discussion of using "smart mobs" for homeland security at http://www.techcentralstation.com/021403A.html, and http://stephensonstrategies.com/stories/2004/09/29/10pointPlanToMakeSecurityM.html. Smart mobs are groups that use technology to behave intelligently or efficiently. Smart mobs could be used to augment public safety eyes and ears on transportation systems, at major events, and other public sites.
[12] International Association of Chiefs of Police, "From Hometown Security to Homeland Security," May 17, 2005:5-6.
[13] Steven Johnson, *Emergence* (New York: Touchstone, 2001) and Albert-Laszlo Barabasi, *Linked* (Cambridge, MA: Perseus Publishing, 2002).
[14]International Association of Chiefs of Police, "From Hometown Security to Homeland Security," May 17, 2005. Congressional Research Service, "The National Preparedness System: Issues in the 109th Congress," March 10, 2005: 29 30. U.S. Government Accountability Office, "Homeland Security: Much is Being Done to Protect Agriculture from a Terrorist Attack, but Important Challenges Remain," GAO report GAO-05-214 (Washington: March 8, 2005): 47 48.
[15] John Arquilla, David Ronfeldt (eds.), *Networks and Netwars: The Future of Terror, Crime, and Militancy* (RAND, 2001).
[16] For examples, see the Memorial Institute for the Prevention of Terrorism collection of state homeland security strategies at http://www.mipt.org/State-Homeland-Security-Plans.asp. Some have noted that many of the "plans" seem to be more concerned with how money will be spent than with what the state's homeland security strategy will be.
[17] *The Interim National Infrastructure Protection Plan* (Department of Homeland Security, February 2005), for example, talks about evolution more than a dozen times.
[18] For a review of the argument linking evolutionary theory to contemporary organizational issues, see Lawrence and Nohria, *Driven: How Human Nature Shapes our Choices* (Jossey-Bass, 2002).
[19] For the significant difference between best practices and smart practices, see Bardach, *A Practical Guide for Policy Analysis* (Chatham House, 2000).
[20] As of June 2005, six states had working fusion centers; another dozen states were in the process of developing them. See National Governor's Association, "Intelligence Fusion Center TA Request," June 2005 for a status report on state involvement with fusion centers. For another example of a multi-agency approach to collaboration that emerged from need rather than edict, see the Pasadena, Texas police department's Community Defense Unit, at http://www.ci.pasadena.tx.us/police/operations/CDU/CDU.htm.
[21] Wiki is an abbreviation for "What I Know Is." Wiki is a process that is used in collaborative networks on a website (or other hypertext document collection) that allows users to add content, but also allows anyone to edit the content.

[22] Eric S. Raymond, "The Cathedral and the Bazaar," *First Monday*, March 1998, http://www.firstmonday.org/issues/issue3_3/raymond/ [Accessed 1 June 2005]. Translated from computer talk, the quote suggests the more people who review something, the easier it is to find errors. James Surowiecki, in The Wisdom of Crowds," (Doubleday, 2004) makes a similar point. He applies the self-organizing/emergence logic to decision-making and decision markets and notes four conditions that have to be met before the judgments of many individuals are likely to be superior to expert judgment: diverse opinions, independence, decentralization and aggregation. All four conditions could be met in the experiment suggested here.

[23] Thomas J. Dailey, "Implementation of Office for Domestic Preparedness Guidelines for Homeland Security Prevention and Deterrence June 2003" (master's thesis, Naval Postgraduate School, Center for Homeland Defense and Security, March 2005).

[24] Eric S. Raymond, "The Cathedral and the Bazaar."

Homeland Security Affairs

Volume I, Issue 1 2005 *Article* 4

Summer 2005

Community Policing as the Primary Prevention Strategy for Homeland Security at the Local Law Enforcement Level

Jose Docobo*

*jdocobo@hcso.tampa.fl.us

Community Policing as the Primary Prevention Strategy for Homeland Security at the Local Law Enforcement Level

Jose Docobo

Abstract

Like traditional crime, terrorism is a local issue and is a responsibility shared among federal, state, and local governments. In the wake of September 11, local law enforcement has taken on a pivotal role in preventing and responding to future incidents of terrorism within the United States. The new policing model for terrorism and homeland security must address the areas of crime prevention, intelligence gathering, and information sharing. This will require a shift in the culture of law enforcement agencies, involving the creation of external partnerships, citizen involvement, problem solving, and the transformation of the organization. Adoption of the "homeland-policing" model presented in this article suggests that the community policing model serves as a solid framework for the development of an effective prevention strategy for homeland security by local law enforcement agencies.

AUTHOR BIOGRAPHY: Chief Deputy Jose Docobo has served with the Hillsborough County Sheriff's Office for over 24 years. He has served previously as a Detective in Special Investigations, Internal Affairs; as the Operations Corporal for the Enforcement Operations Department; as an Internal Affairs Sergeant at the Professional Standards Bureau; as Lieutenant, Captain and then Major, of the Inspectional Services Division; and as Colonel of the Enforcement Operations Department and Executive Support Department. Chief Deputy Docobo graduated with honors from the University of South Florida and holds a Master of Arts Degree from the United States Naval Postgraduate School in National Security Studies. He is also a graduate of the FBI National Academy, the Senior Executive Fellows Program at Harvard University, and the Secret Service Dignitary Protection School.

KEYWORDS: local government, prevention, community policing, crime terrorism, law enforcement agencies, partnerships, citizen involvement

Traditionally, local law enforcement has concerned itself primarily with preventing and solving crimes such as burglary, theft, and robbery — crimes that have an immediate and visible impact on the local community and affect citizen quality of life. In the face of unknown future terrorist threats, however, local law enforcement organizations will have to adapt existing policing strategies to fulfill the requirement of homeland security.

Over the years, law enforcement organizations have sought to address the causes and reduce the fear of crime in communities through the creation of effective partnerships with the community and other public and private-sector resources, the application of problem-solving strategies or tactics, and the transformation of agency organization and culture. In the wake of September 11, 2001, local law enforcement agencies throughout the country find themselves struggling to identify their responsibilities and define their future role in the effort to combat terrorism. The new policing model for terrorism and homeland security must address the areas of crime prevention, intelligence gathering, and information sharing. While these roles are not new to local policing, homeland security at the local level will require a shift in law enforcement's role if police are to ensure the safety and welfare of citizens.

While some have suggested that community policing can fit into the overall national strategy for homeland security, little research specifically identifies community policing strategies and their direct application to the national strategy for homeland security. Many of the objectives of terrorism prevention parallel current law enforcement policies with respect to local crime issues. Because of these similarities, individual, neighborhood, and community crime-prevention strategies should support law enforcement in the fight against terrorism.

COMMUNITY-ORIENTED POLICING

The United States Department of Justice has defined community policing as a philosophy that "focuses on crime and social disorder through the delivery of police services that includes aspects of traditional law enforcement, as well as prevention, problem-solving, community engagement, and partnerships."[1] Despite varying definitions of community-oriented policing, it is generally agreed that there are three key components to the community policing philosophy. These include the creation of and reliance on effective partnerships with the community and other public/private-sector resources, the application of problem-solving strategies or tactics, and the transformation of police organization and culture to support this philosophical shift. In other words, community policing is not in itself a tactic or strategy, but instead a philosophical approach to how policing is conducted. At its core, community-oriented policing is based on law enforcement and the community joining together to identify and address issues of crime and social disorder.

In a 2002 publication, the U.S. Department of Justice, Office of Community Oriented Policing discussed a series of community-oriented policing resources and practices that have a direct application to terrorism deterrence and prevention. These include the use of crime mapping with GIS systems, data collection and analysis protocols, and technologies that may be used as platforms for gathering intelligence to assess terrorism vulnerability. In addition, the community partnerships formed by police in the course of community-oriented problem solving provide a ready framework for engaging citizens in helping police to identify possible threats and implement preparedness plans.[2]

Rob Chapman and Matthew C. Scheider, Senior Analysts at the Office of Community Oriented Policing Services (COPS), suggest that community policing could play an integral role in homeland security. They contend that by applying the principles of organizational change, problem solving, and external partnerships, community policing can help police to prepare for and prevent terrorist acts, and respond to the fear such threats engender.[3] Community policing helps to build trust between the community and law enforcement, which allows officers to develop knowledge of the community and resident activity and can provide vital intelligence relating to potential terrorist actions. Local law enforcement can facilitate information gathering among ethnic or religious community groups with whom police have established a relationship. It will generally be citizens who observe the unusual – groups of men living in apartments or motels, or unusual behavior at flight schools – in their own community, and could be expected to report such observations to the local police. According to Chapman and Scheider, problem-solving models typically used in community policing are well-suited for preventing and responding to possible terrorist activity. Using existing data sources, agencies can conduct target vulnerability assessments and develop risk-management and crisis plans.[4]

Community Partnerships

Community policing is based on the notion that citizens should be empowered to prevent crime or the problems that lead to crime.[5] Establishing and maintaining mutual trust is therefore the central goal of community policing, as it allows wide law enforcement access to valuable community information leading potentially to the prevention and resolution of crimes.

The partnerships formed in support of community crime prevention efforts can also provide a framework for engaging citizens to help police identify possible terrorist threats and infrastructure vulnerabilities. Effective community policing involves not only developing partnerships between law enforcement and citizens, however, but also intergovernmental and interagency collaborations with state and federal agencies. These partnerships are essential for the collection and exchange of intelligence, the identification of threats and vulnerabilities, and the sharing of resources in the event of an attack.

Problem Solving

Problem solving is a broad term that describes the process by which specific issues or concerns are identified and the most appropriate remedies to abate the problem(s) are identified. Problem solving is based on the assumption that "individuals make choices based on opportunities presented by the immediate physical and social characteristics of an area. By manipulating these factors, people will be less inclined to act in an offensive manner."[6] The idea is that if the underlying conditions that create problems can be eliminated then so will the problem. Such conditions range from the type of individuals involved to the physical environment in which these problems are created.

Prior to the advent of community-oriented policing, problem-oriented policing was associated with the decentralization of responsibility and with lateral communication both within and outside the police department. Problem-oriented policing dealt with the conditions that cause a problem; this concept of policing required officers to recognize relationships that lead to crime and disorder and direct their attention to issues of causation.[7] Mark Moore asserts that thought and analysis is fundamental to problem-oriented policing in order to effectively respond to the cause of the problem.[8]

According to Spelman and Eck, problem-oriented policing converged on three main themes: increased effectiveness, reliance on the expertise and creativity of officers, and closer involvement with the community. These themes are implemented by attacking underlying phenomena that deplete patrol officers' and detectives' time, and educating officers to study problems and develop innovative solutions to ensure that police address the needs of citizens.[9]

Organizational Transformation

Community policing requires an organizational transformation inside the law enforcement agency so that a set of basic values rather than mere procedures guide the overall delivery of services to the community. Organizational transformation involves the integration of the community policing philosophy into the mission statement, policies and procedures, performance evaluations and hiring and promotional practices, training programs, and other systems and activities that define organizational culture and activities.[10]

In the community policing model, individual officers are given broader freedom to resolve concerns within their community. Individual officers are presumably the most familiar with their communities and are therefore in the best position to forge close ties with the community and create effective solutions. Community policing emphasizes employee participation; individual officers are given the authority to solve problems and make operational decisions suitable to their assignments. Officers are seen as generalists, not specialists.

ADAPTING COMMUNITY POLICING TO HOMELAND SECURITY

Like traditional crime, terrorism is a local crime issue and is a responsibility shared among federal, state, and local governments. Indeed, traditional crime and terrorism are inextricably linked. International and domestic terrorist groups are well-organized and trained, and demonstrate the sophistication of other, traditional organized crime groups. These groups commit ancillary crimes like fraud, money laundering, drug trafficking, and identity theft to provide the resources for their terrorism. The investigative approach to a terrorist event is similar to that of a traditional crime incident. Because of the similarities between traditional crime and terrorism, departments that have already adopted a community policing philosophy should find it a seamless transition to addressing terrorism and terrorism-related crime. Officers should already have the skills to analyze the terrorism problem, perform threat analysis, develop appropriate responses and reflect these efforts in the mission, goals and objectives of the department.[11]

In 2002, the Markle Foundation Task Force report stated:

> Most of the real frontlines of homeland security are outside of Washington D.C. Likely terrorists are often encountered, and the targets they might attack are protected, by local officials – a cop hearing a complaint from a landlord, an airport official who hears about a plane some pilot trainee left on the runway, an FBI agent puzzled by an odd flight school student in Arizona, or an emergency room resident trying to treat patients stricken by an unusual illness.[12]

In a more recent report, the Rockefeller Institute observed that "while much attention has been focused on the national government's efforts to address these [Homeland Security]

problems, there has been less consideration of the role of state and local governments, which play a critical role in preventing and responding to terrorist attack."[13] In the wake of September 11, 2001, however, local law enforcement has taken on a pivotal role in preventing and responding to future incidents of terrorism within the United States. This new role, like the adoption of community policing, will require yet another shift in the culture of law enforcement agencies.

Facilitating this shift, however, is the fact that community policing and homeland security have a great deal in common. Both neighborhood crime and terrorism threaten the quality of life in a community and exploit the fear they create. Despite creative ways to stretch public safety budgets, local law enforcement cannot sustain two separate missions of traditional policing and terrorism prevention. Community policing and homeland security can share the same goals and strategies. Creating external partnerships, citizen involvement, problem solving, and transforming the organization to take on a new mission are all key elements of community policing and should be part of a comprehensive homeland security strategy. The lesson learned from fighting traditional crime is that prevention is the most effective approach in dealing with crime, fear, and social disorder. Fighting terrorism is no different.

ORGANIZATIONAL TRANSFORMATION

The task of a wholesale re-engineering of American local law enforcement toward a counter-terrorism role is complex and unprecedented. If U.S. law enforcement is to move forward to a national role in homeland security, then practical, focused, and effective training must be a cornerstone of this transformation. Without appropriate and ongoing training of both current and new law enforcement personnel, homeland security will be dismissed as a passing concept instead of a cultural change in law enforcement strategy.

There are a number of community policing practices that can support efforts in homeland security. These practices include adopting the philosophy organization-wide, decentralizing decision-making and accountability, fixing geographic and general responsibilities and utilizing volunteer resources. Local law enforcement officers are most likely to come into contact with individuals who are either directly or indirectly involved in terrorist activities and are certain to be the first responders to any attack.

Empowering officers at lower levels with greater decision-making authority and responsibility for important decisions could be valuable in a crisis. During a terrorist event, there may be little time for decisions to move up the chain of command. Officers who are accustomed to making decisions and retaining authority may be better prepared to respond quickly and decisively to any event.

In terms of prevention, developing a flat organizational structure can help lower-level officers feel free to pursue leads regarding possible terrorist activity. In addition, officers who work in a fixed geographic area for an extended period are more likely to develop specific intelligence that may be a vital part of counter-terrorism efforts.[14]

Organization-wide Adoption

Homeland Security, like community policing, must be adopted agency-wide to realize its full potential and effectiveness. Integrating the homeland security responsibility into the agency's mission statement, goals, policies and procedures, training programs, and other systems and activities that define organizational culture, should reflect this adoption.

Training

Local agencies will need to expand beyond the rudimentary aspects of law enforcement training such as firearms, driving, unarmed defense and criminal law into one that emphasizes an analytical preventative approach. While law enforcement must continue to train for their roles as first responders in post-incident management and investigation, police must receive training and education in:

- Understanding the nature, dynamics, and operations of international terrorist groups that may operate in or against the United States, and how that translates into more effective patrol and investigative functions;
- Understanding the locations, movements, and plans of international terrorist cells that live and work in local communities;
- Gathering and analyzing intelligence on potential terrorist activities;
- Conducting threat assessments;
- Conducting inquiries and investigations into potential terrorists while safeguarding the constitutional rights of all people in the United States.

Most local law enforcement officers have never been in the intelligence business and therefore may not know precisely what information they should look at as indicative of terrorist activity or that may have value within a larger intelligence context. These signs are not necessarily obvious, but rather subtle, and would be discernible to a regular patrol officer or detective with proper training. Officers or detectives may have valuable information without even knowing it and may not know to share the information because they have never had adequate terrorism intelligence training.

Another area of training that law enforcement must commit to is public education. Although the majority of communities will never be impacted by a terrorist event, the threat of potential terrorist attacks can create fear and undermine the sense of community safety. It will therefore be critical that police take a leadership role in maintaining community confidence. This can be done by educating the public as to the nature of threats and actively responding to specific community concerns. For the public to respond to an alert, it needs to know what to watch for. Educating the public also garners support for government action in a crisis. Moreover, citizens educated about potential threats can assist law enforcement during alerts. The public would know what to look for, what to do, and how to respond.[15]

Decentralized Decision-making and Accountability

In community policing, individual line officers are given authority to solve problems and make operational decisions. Leadership is required and rewarded at every level; supervisors and officers are held accountable for decisions and the effects of their efforts at solving problems. Empowering officers at the lower levels will allow them the freedom to pursue leads or suspected terrorist activity, or to identify possible terrorist vulnerabilities within the community.

Fixed Geographic Accountability and Generalist Responsibilities

In community policing, most staffing, supervision, deployment, and tactical decision-making are geographically based. Personnel are assigned to fixed geographic areas for extended periods of time in order to foster communication and partnerships between individual officers and their community. Having fixed-geographic responsibility allows officers to develop more productive relationships with members of their community and, as a result, officers should be more attuned to rising levels of community concern and fear. By

virtue of these relationships, officers should be in a position to respond effectively to those needs and concerns. Community policing engenders trust and increases satisfaction among community members and police, which in periods of heightened unrest or crisis can translate to dealing more effectively with community fear.[16]

Utilizing Volunteer Resources

After the events of September 11, 2001, the idea of involving citizens in crime prevention has taken on new significance, with President Bush calling for greater citizen involvement in homeland security through initiatives such as Citizen Corps and Freedom Corps.[17] President Bush created these programs so Americans could participate directly in homeland security efforts in their own communities. This network of volunteer efforts uses the foundations already established by law enforcement in order to prepare local communities to respond effectively to the threats of terrorism and crime. In addition to creating the Citizens Corps and Freedom Corps, the president's plan is to enhance community-policing programs already in place, such as Neighborhood Watch, by incorporating terrorism prevention into its mission.

Community policing encourages the use of non-law enforcement resources within a law enforcement agency such as volunteerism, which involves active citizen participation with their law enforcement agency. Volunteer efforts can help free up officer time, and provide an effective channel for citizen input. It has long been recognized that many of the basic functions within a law enforcement agency can be accomplished by other than sworn deputies or civilian employees. Volunteer efforts can help free up officer time, and allow sworn personnel to be more proactive and prevention-oriented. In many jurisdictions around the country, citizens who have the time to volunteer in the community have offered their services to law enforcement agencies, freeing up law enforcement personnel to spend more time in a crime reduction role.

This community policing element dovetails perfectly with President Bush's Citizen Corps, which was developed to "harness the power of every individual through education, training, and volunteer service to make communities safer, stronger, and better prepared to respond to threats of terrorism, crime, public health issues, and disasters of all kinds."[18] There are four programs in Citizen Corps: Neighborhood Watch, Volunteers in Police Service (VIPS), Community Emergency Response Teams (CERT), and Medical Reserve Corps (MRC), all of which integrate well with the community policing philosophy. In fact, Neighborhood Watch has been an integral component of the community policing philosophy virtually since its inception.

Neighborhood Watch

This crime prevention program, which has a thirty-year history, engages volunteer citizen action to enhance security within local communities by encouraging citizens to report suspicious activity in their immediate neighborhoods. Citizen Corps hopes to double the number of neighborhood watch programs, while incorporating terrorism prevention into the program's mission. In the aftermath of September 11, 2001, the need for strengthening and securing our communities has become even more critical, and Neighborhood Watch groups have taken on greater significance. In addition to serving a crime prevention role, Neighborhood Watch can also be used as the basis for bringing neighborhood residents together to focus on disaster preparedness as well as terrorism awareness, to focus on evacuation drills and exercises, and even to organize group training, such as the Community Emergency Response Team (CERT) training.[19]

Volunteers in Police Service (VIPS)

This program provides training for civilian volunteers who assist local police departments by performing "non-sworn" duties, effectively freeing up officers to spend more time on critical functions. Since September 11, 2001, the demands on state and local law enforcement have increased dramatically. As a result, already-limited resources are being stretched farther at a time when our country needs every available officer out on the beat. The program provides resources to assist local law enforcement officials by incorporating community volunteers into the activities of the law enforcement agency and by using best practices to help state and local law enforcement design strategies to recruit, train, and utilize citizen volunteers in their departments.[20]

Community Emergency Response Teams (CERT)

This program provides civilians with training in emergency management planning and response functions to bolster the capacity of local communities to respond to disasters. President Bush has proposed a three-fold increase, to 400,000, of the number of citizens enrolled in CERT. Since its move into Citizen Corps, the program has added a new module that addresses terrorism preparedness. When emergencies happen, CERT members can give critical support to first responders, provide immediate assistance to victims, and organize spontaneous volunteers at a disaster site. CERT members can also help with non-emergency projects that help improve the safety of the community.[21]

Medical Reserve Corps (MRC)

The Medical Reserve Corps (MRC) Program coordinates the skills of practicing and retired physicians, nurses, and other health professionals as well as other citizens interested in health issues who are eager to volunteer to address their community's ongoing public health needs and to help their community during large-scale emergency situations. Local community leaders develop their own Medical Reserve Corps Units and identify the duties of the MRC volunteers according to specific community needs. For example, MRC volunteers may deliver necessary public health services during a crisis, assist emergency response teams with patients, and provide care directly to those with less serious injuries and other health-related issues. The Medical Reserve Corps (MRC) plays an integral part in our preparedness and response strategy. It provides an organized way for medical and public health volunteers to offer their skills and expertise during local crises and throughout the year.[22]

PROBLEM SOLVING TACTICS APPLIED TO HOMELAND SECURITY

Through programs such as Crime Prevention Through Environmental Design (CPTED), intelligence gathering, information sharing, and the use of GIS mapping and analysis, law enforcement can identify and conduct security assessments of critical infrastructure and other important private sector facilities. Security assessments can identify which facilities have the greatest potential as targets. Once identified, detailed risk management and crisis plans can be developed and implemented. The goal of problem solving in community-oriented policing is a fundamental shift from traditional reactive policing to one that preemptively reduces a facility's vulnerability to a terrorist attack.

Crime Prevention Through Environmental Design (CPTED)

Basic principles of CPTED include target hardening (controlling access to neighborhoods and buildings and conducting surveillance on specific areas to reduce opportunities for crime

to occur) and territorial reinforcement (increasing the sense of security in settings where people live and work through activities that encourage informal control of the environment).

Local agencies will have to get involved in community planning through programs like CPTED to ensure that future growth and construction of facilities minimizes the vulnerability to terrorist acts. The conceptual thrust of CPTED is that the physical environment can be manipulated by design to produce behavioral effects that will reduce the incidence and fear of crime, thereby improving the quality of life. These behavioral effects can be accomplished by reducing the propensity of the physical environment to support crime.[23]

Intelligence Gathering

For years, local law enforcement agencies have complained about federal agencies failing to appreciate the role of law enforcement in intelligence activities. At a time when asymmetric terrorist threats pose some of the biggest threats to our communities, however, we cannot afford not to have local law enforcement more fully integrated into the National Homeland Security Strategy.

The challenge here will be two-fold. First, it will require a philosophical change in federal law enforcement to break down the barriers of compartmentalization and accept local agencies as full partners in the national security intelligence infrastructure. Secondly, local agencies need to receive the necessary training and analytical resources. The challenge will come not in obtaining additional human resources, but in training existing personnel to recognize information or behavior of individuals or groups of possible threats, and the ability to disseminate that information with others in a manner that would allow for the intervention of any future terrorist acts.

Geographic Information Systems (GIS) Mapping and Analysis

Many of the innovations implemented through community-oriented policing require a geographic focus, and emphasize the importance of integrating GIS mapping technology into problem-solving strategies. Technological advances in computer mapping have propelled crime mapping and analysis to the forefront of crime prevention and community policing. Computerized crime mapping allows law enforcement agencies to plot crime data against a digitized map of a community, city, or region. Crime-related data can then be compared and analyzed with other external data sources.[24]

COMMUNITY PARTNERSHIPS

Since September 11th, it has become apparent that Homeland Security is not an effort that can be conducted by law enforcement alone. Instead, an effective Homeland Security strategy must include partnerships not only with other law enforcement organizations, but also with businesses, citizens, emergency management, public health, and many other private and public organizations with a stake in terrorism prevention and response. Partnerships need to be expanded to take advantage of the many skills necessary to plan for, mobilize, and respond to terrorist acts. For homeland security, this means building trust with Arab-American and Islamic-American communities, not with empty promises but by demonstrating how law enforcement can protect them in their neighborhoods, workplaces, places of worship, and other public spaces.[25]

There is often some misconception that in community-oriented policing, “community” is defined by certain geographical boundaries. Daniel Flynn suggests that law enforcement agencies look beyond traditional geographical boundaries and that agencies also look at areas

or groups with shared character or identity and those with common problems or concerns. Flynn points to ethnic, cultural, and racial communities, as well as businesses, schools, and churches.[26] In community-oriented policing, the police are only one of the many local government organizations responsible for responding to community problems. In community-oriented policing, other government agencies are called upon and recognized for their abilities to respond to crime and social disorder issues. Community-based organizations also are brought into crime prevention and problem solving partnerships with law enforcement. Encouraging citizen involvement in programs such as neighborhood watch, youth education, and other activities with law enforcement has been found to increase social cohesion among citizens and decrease fear of crime.[27] The emphasis on building community partnerships encouraged by community-oriented policing may also help reduce citizen fear of terrorist events.[28]

The prevention of terrorist activities requires not only effective communication between local and state agencies and the federal government but, perhaps more importantly, with the community. By building community partnerships facilitated by community policing, law enforcement can develop responses aimed at reducing levels of fear. While citizen fear of terrorist events is somewhat different from fear of crime, some of the same techniques and programs can be used in its reduction. Citizen awareness campaigns can inform citizens about what police and government are doing to prepare for and prevent a future attack.[29]

Working with the Media

In any terrorism strategy, the media will play a crucial role in defining the nature, scope, and level of threat in critical situations, in disseminating information, and in calming the population. According to *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*, one way to blunt the "behavioral, attitudinal, and emotional responses" to terrorism is to influence the human response through an effective program of communications.[30]

Through relationships and partnerships cultivated with reporters and producers, the local media will look to law enforcement as an important partner in delivering accurate and relevant information to the public. While government cannot control how people will react to a terror attack, officials can help shape attitudes and behaviors by providing helpful information as well as seek assistance in obtaining information that may be relevant in the prevention or investigation of a terrorist incident. Making information available about measures taken to prevent or defend against an attack will give citizens a greater sense of control over uncertain situations and tend to lower the level of public fear.[31]

Neighborhood Watch, Business Watch and Worship Watch Programs

Neighborhood Watch as a crime prevention tool has been in place around the country for many years. Recognizing that the detection of criminal activity is not a job law enforcement can do alone, Neighborhood Watch has served as extra eyes and ears in the community to report suspicious activity or crimes to law enforcement. As the detection of suspicious behavior is an integral part of homeland security, using this already established program should be part of an agency's overall homeland security effort. Through the Neighborhood Watch program, law enforcement can:

- Act as a liaison with each current Neighborhood Watch group. This includes developing more efficient methods of communication between law enforcement and these groups in order to provide a better exchange of up-to-date crime prevention and homeland security

information. In turn, the interest level of Watch members would increase and keep groups active.

- Recruit new Neighborhood Watch groups. Experience has shown that in areas where Neighborhood Watch groups are active, crime is generally lower and support for law enforcement higher.
- Review daily all crime-related calls for service records in their assigned area. Police officers will be looking to identify problems areas that can be addressed with prevention efforts. This includes working with crime analysts and district enforcement personnel seeking unified approaches in reducing crime by prevention.
- Meet with crime victims and other citizens to offer services to reduce their potential of becoming a victim in the future. The main activity supporting this task is conducting crime prevention programs and security surveys to residential areas.
- Act as a conduit for homeland security initiatives to encourage citizens to be observant and watchful by reporting things that seem unusual or out of place.

Managers and business owners make risk management decisions for their businesses every day. These risks encourage them to seek new opportunities to profit. Allowing crime an opportunity to exist is not one of these risks, since no chance for profit exists when crime is present. Crime results in monetary loss, inventory loss, and a loss to the reputation of the business. Most importantly, crime can impact the personal safety of employees and their customers. This makes crime prevention good for business from both a human and financial standpoint.

The Business Watch Program is modeled after the Neighborhood Watch Program and establishes a formal communication network between law enforcement and businesses countywide. Business members are alerted to the potential of crime and are encouraged to look out for the community.

Law enforcement can provide members with training to educate owners, managers, and employees to be able to recognize and report any suspicious activities or crimes. Such training ranges from preventing shoplifting and robbery to learning how to be a good witness, and many other topics. The key focus of each deputy is the delivery of proactive crime prevention and homeland security services to the business community.

Worship Watch was originally designed to bring crime prevention awareness and law enforcement services to all religious communities regardless of their religious beliefs by providing programs on personal safety, home security, drug awareness, auto theft, and many other subjects of interest to the public. Since September 11th special emphasis has been placed upon religious institutions that, as a result of current world events, may be at a greater threat level because of their religious beliefs.

Citizen Academies

Community-oriented policing is based on the premise that citizens should be empowered to enhance their quality of life and prevent or eliminate crime and the problems that lead to crime.[32] Everyone benefits when community members understand the role and function of their police department and become active proponents of law enforcement.[33] One such initiative used by law enforcement agencies is the citizen academy. Citizen academies have been effective in educating members of the community about the mission, goals, objectives, and programs of the police department. Citizen academies should be expanded to address the issue of terrorism and the role that the community can play in assisting law enforcement with

information gathering, identification of target vulnerabilities, and volunteer opportunities directly supporting the homeland security strategy.

HOMELAND POLICING

For the past ten years, community-oriented policing has served as the impetus for law enforcement agencies to establish a closer relationship with citizens to identify threats within the community that create a climate of fear and social disorder. The emphasis in community policing on community involvement and problem solving clearly establishes a solid foundation upon which homeland security efforts should be built. At a time when local law enforcement agencies have to deal with additional homeland security responsibilities and shrinking budgets, there could be a tendency to reduce community policing efforts, which are still often thought of as a "frill." Under these circumstances, it is important that law enforcement agencies not revert to the "traditional" approach to policing. Instead of de-emphasizing community-oriented policing efforts, law enforcement agencies must realize that a strong community-oriented policing philosophy within the agency provides a strong basis for preventing and responding to terrorism and its goal of creating fear in the community. Local law enforcement must realize that their efforts are integral to any national homeland security strategy and that community-oriented policing could be their most effective strategy in dealing with terrorism prevention and response in their community.

The "homeland-policing" model presented here suggests that the existing community policing model does serve as an effective framework for the development of an effective prevention strategy for homeland security by local law enforcement agencies. Results of a 2004 survey of all local law enforcement agencies in the state of Florida showed that a significant correlation exists between what agencies do in their day-to-day activities with respect to community policing and homeland security. For example, agencies that use GIS to conduct crime mapping and analysis also frequently use GIS to conduct terrorism target mapping and analysis, and agencies that use their web site to disseminate crime prevention information also frequently use it to disseminate homeland security information. In short, results showed that factors associated with adopting a community policing philosophy among agencies and implementing homeland security strategies within agencies are highly related.[34]

---

[1] United States Department of Justice, Office of Community Oriented Policing Services. "What is Community Policing," http://www.cops.usdoj.gov/default.asp?Item=36 [Accessed July 4, 2005].
[2] U.S. Department of Justice, Office of Community Oriented Policing Services, COPS INNOVATIONS, "A Closer Look, Local Law Enforcement responds to Terrorism: Lessons in Prevention and Preparedness," Washington, D.C., 2002.
[3] Rob Chapman and Matthew C. Scheider, "Community Policing: Now More than Ever," Office of Community Oriented Policing, U.S. Department of Justice, Washington, D.C., 2002
[4] Ibid.
[5] Dennis J. Stevens, *Case Studies in Community Policing,* (Upper Saddle River, NJ: Prentice Hall, 2001), 9.
[6] Kenneth J. Peak and Ronald W Glensor, *Community Policing and Problem Solving: Strategies and Practices* (Upper Saddle River, NJ: Prentice Hall, 1996), xvi-xvii.
[7] Herman Goldstein, *Problem-Oriented Policing* (New York: McGraw Hill, 1990), 32-34.
[8] Mark H. Moore, "Problem Solving and Community Policing: A Preliminary Assessment of New Strategies of Policing," *Modern Policing Crime and Justice Volume 15*, eds. Michael Tonry and Norval Morris (Chicago: University of Chicago Press, 1992), 99-158.

[9] John E. Eck, W. Spelman, W. D. Hill, D. W. Stedman and G.R. Murphy, "Problem Solving: Problem Oriented Policing in Newport News," (Washington, D.C.: Police Executive Research Forum, 1987), 3-4.
[10] United States Department of Justice, Office of Community Oriented Policing Services, "General Elements of Community Policing," www.cops.usdoj.gov/print.asp?Item=477 [Accessed May 24, 2004].
[11] Matthew C. Scheider, Robert E Chapman and Michael F. Seelman, "Connecting the dots for a proactive approach," *Border and Transportation Security America,* Quarter 4, 2003, 159.
[12] Markle Foundation Task Force, *Protecting America's Freedom in The Information Age: A Report of the Markle Foundation Task Force* (New York, New York, October 2002), 10.
[13] The Rockefeller Institute of Government, "The Federalism Challenge: The Challenge for State and Local Government," *The Role of "Home" in Homeland Security: Symposium Series,* Number 2, March 24, 2003.
[14] Matthew C. Scheider and Robert Chapman, "Community Policing and Terrorism," *Journal of Homeland Security,* April 2003, http://www.homelandsecurity.org/journal/articles/Scheider-Chapman.html [Accessed October 31, 2004].
[15] Eric Taylor, "The New Homeland Security Apparatus, Impeding the Fight against Agile Terrorist," *Cato Institute, Foreign Police Briefing* No. 70, June 26, 2002, 5.
[16] Matthew C. Scheider and Robert Chapman, "Community Policing and Terrorism."
[17] President George W. Bush, Citizen Corps, http://www.whitehouse.gov [Accessed May 14, 2004].
[18] Citizen Corps Mission Statement, United States department of Homeland Security, http://www.citizencorps.gov/councils/ [Accessed October 31, 2004].
[19] Neighborhood Watch, United States Department of Justice, http://www.usaonwatch.org [Accessed November 1, 2004].
[20] Volunteers in Police Service, United States Department of Justice, http://www.policevolunteers.org/ [Accessed November 1, 2004].
[21] Community Emergency Response Teams, Department of Homeland Security, Federal Emergency Management Agency, http://training.fema.gov/emiweb/CERT/, [Accessed November 1, 2004].
[22] Medical Reserve Corps, United States Department of Health and Human Services, http://www.medicalreservecorps.gov/ [Accessed November 1, 2004].
[23] Timothy D. Crowe, *Crime Prevention Through Environmental Design* (Woburn, Mass: Butterworth-Heinemann, 1991), 28-31.
[24] Cynthia A. Mamalian and Nancy G LaVigne, "The Use of Computerized Crime Mapping by Law Enforcement," National Institute of Justice, U.S. Department of Justice, Office of Justice Programs, January 1999, 1.
[25] Williams Lyons, "Partnerships, information and public safety: community policing in a time of terror," *Policing: An International Journal of Police Strategies & Management,* 25, No. 3 (2002): 532.
[26] Daniel W. Flynn, "Defining the community in community policing," United States Department of Justice, Community Policing Consortium, Washington, D.C., July 1998. http://www.communitypolicing.org/publications/cfm, [Accessed April 28, 2004].
[27] Gary W. Cordner, "Community Policing: Elements and Effects," Roger G. Dunham and Geoffrey P. Alpert, eds., *Critical Issues in Policing.* (prospect Heights, Il: Waveland Press, 1997), 451-468.
[28] Matthew C. Scheider and Robert Chapman, "Community Policing and Terrorism."
[29] Ibid.
[30] Committee on Science and Technology for Countering Terrorism, Division on Engineering and Physical Sciences, National Research Council, "Making the Nation Safer: The Role of Science and Technology in Countering Terrorism," (Washington, D.C.: National Academy Press, 2002), 270. http://www.nap.edu/html/stct/index.html [Accessed November 7, 2004].
[31] Ibid, 272.
[32] Dennis J. Stevens, *Case Studies in Community Policing*, 9.
[33] Daniel P. Carlson, *When Cultures Clash: The Diverse Nature of Police-Community Relations and Suggestions for Improvement*, (Upper Saddle River, N.J.: Prentice Hall, 2002), 115.
[34] Jose M. Docobo, "Community policing as the primary prevention strategy for homeland security at the local law enforcement level," (masters thesis, Naval Postgraduate School, 2005), 60.

Homeland Security Affairs

Volume I, Issue 1 2005 *Article* 5

Summer 2005

Building a Contingency Menu: Using Capabilities-Based Planning for Homeland Defense and Homeland Security

Thomas Goss*

*familygoss@aol.com

Building a Contingency Menu: Using Capabilities-Based Planning for Homeland Defense and Homeland Security

Thomas Goss

Abstract

Terrorist threat actors are both cunning and adaptive, relying on surprise to overcome security measures. For this reason, military and security planners must embrace a more flexible, comprehensive, and comprehensible approach to contingency planning – a method based on neither threats nor scenarios exclusively, but rather on integrating these two approaches into a planning process based on capabilities. Using the concepts of "lines of operation" and "capabilities" as dynamics to define and explain potential and likely interactions, the capabilities-based planning method proposed in this article produces a menu of options for decision-makers that are directly related to specific threat capabilities and linked to specific resources. The question "who is the threat?" is reworded as "what could the threat do?" allowing exploration of a much broader range of eventualities and giving Homeland Defense and Security planners a defined and detailed threat to plan against.

AUTHOR BIOGRAPHY: Lieutenant Colonel Thomas Goss is an active duty officer in the U.S. Army currently serving on the International Military Staff at the North Atlantic Treaty Organization (NATO) Headquarters in Brussels, Belgium. For the last four years, LTC Goss has been a Strategic Plans and Policy officer working on issues of Homeland Defense and Homeland Security while assigned to North American Aerospace Defense Command (NORAD) and U.S. Northern Command in Colorado Springs, Colorado. LTC Goss received a Ph.D. in History from Ohio State University and recently graduated from the Naval Postgraduate School with a master's degree in Homeland Security.

KEYWORDS: prevention, planning, capabilities, lines of operation, threat definition

INTRODUCTION: The Vital Task of Planning for the Worst

"Within a few hours [on September 11, 2001], the threats to our world had become exponentially more complex," the New York City Fire Commissioner concluded in the *FDNY Strategic Plan 2004-2005*, "[and] the Fire Department, in turn, needed to adapt."[1] The challenge for homeland defense and homeland security organizations is uncertainty as to what to adapt to, with a threat being too ambiguous and diverse to easily identify. For military planners at United States Northern Command, counter-terrorism planners at the Department of Homeland Security (DHS), and strategic planners in police and fire departments, there are many questions: What exactly is the threat? What part of this threat is our responsibility? What capabilities will we need to detect and to stop these threats? The next concern is often the perplexing question: how do I explain this plan to my boss? Because terrorist threat actors are both cunning and adaptive, relying on surprise to overcome security measures, military and security planners must embrace a more flexible, comprehensive, and comprehensible approach to contingency planning – a method based on neither threats nor scenarios exclusively, but rather on integrating these two approaches into a planning process based on capabilities.

The process of contingency planning and resource allocation poses one of the greatest current challenges for those responsible for protecting the United States because of the severity and diversity of the threats and the required timeliness of any defensive operations and security responses. The *National Strategy for Homeland Security* recognizes this by designating "manage risks and allocate resources judiciously" as guiding principles and goes on to declare, "because the number of potential terrorist acts is nearly infinite, we must make difficult choices about how to allocate resources against those risks that pose the greatest danger to our homeland."[2] At this task, military and security planners have struggled to develop a comprehensive and comprehensible planning system using existing approaches of traditional threat-based planning that focus on the "who," and scenario-based planning that address the "what." To present senior decision-makers with timely and effective contingency plans, planners need to transition to a more flexible and dynamic capabilities-based planning method that focuses on the "how" and can thus frame required capabilities and overcome uncertainty concerning the threat.

PROBLEMS WITH CURRENT PLANNING METHODOLOGIES

The *National Security Strategy* identifies the vital function of having a formal and deliberate process of threat assessment, yet such process has yet to gain wide acceptance. Conceptually, there are three fundamental approaches to conducting a threat assessment, focusing on the "who," the "what," and the "how" of the threat. In a traditional threat assessment, analysts address the "who" of the threat: the threat actor(s), their "order of battle," and their most likely courses of action. The second conceptual approach looks at the "what" of the threat: what part of the threat is a specific agency's responsibility to defeat, and what aspect of the threat planners should address through threat scenarios.

One of the critical products for decision-makers in concept development is the "intelligence estimate" or "threat assessment." As current DOD doctrine asserts, "intelligence should provide the commander with an understanding of the adversary in terms of the adversary's probable intent, objectives, strengths, weaknesses, probable course-of-action, most dangerous course-of-action, values, and critical vulnerabilities."[3] Based on this threat assessment and strategic guidance, planners develop a single course of action with branches and sequels. This traditional

planning process results in decision-makers selecting a single contingency plan with a "throw the switch" type of action. Traditional military planning process can thus be seen as a single decision chain, which was effective during the relatively stable strategic environment of the Cold War when even complex plans for major theater wars could go years with only slight modifications.

However appropriate this traditional approach is for a threat like the North Korean military, threat-based planning produces only guesses in the face of state-sponsored and non-state threat actors that the U.S. faces currently. This is due, in turn, to such things as a dearth of intelligence on Al Qaeda's organizational structure and operational capabilities. Without knowing how many "cells" are operating, how they receive operational guidance, and where specifically they plan to strike, planners have little on which to build plans. While intelligence successes in the global war or terrorism have been filling in the blanks on many such questions, the absence of a template will continue to frustrate those who seek to apply a traditional "who" approach to the unprecedented threats to the United States. Taking a traditional threat-based planning approach in an asymmetric and unprecedented threat environment can be inherently frustrating because of the absence of enough hard intelligence and results in continued inability to template a terrorist "order of battle" or determine courses of action.

After 9/11, many homeland security planners tried a different approach to contingency planning by using a "scenario-based" planning process that focused on what events could happen. This approach was based on "what if" drills that postulated a limited number of threat actions and then wargamed agency responsibilities for potential counters. The process of this scenario-based approach was best seen at the Salt Lake City Olympics, and shows the advantages of this method of planning: it is simple to execute and modifiable based on the scenarios selected. These "what if" contingency plans have the additional benefit of not requiring a detailed threat assessment, as issues and questions concerning the threat can be mitigated by making assumptions to fit the scenario. Though conceptually simple, and therefore attractive for initial planning efforts, this approach does have weaknesses because effective "scenario-based" planning requires certainty about possible scenarios and a limited number of scenarios to plan against.

An inherent problem with this "what if" method is unavoidable: scenario-based planning produces plans only for the contingency scenarios selected. These problems were revealed in 2002 when DOD facilitated a Homeland Security and Homeland Defense series of tabletop exercises to wargame existing contingency plans in what became known as the "Nine Scenarios." The goal of this planning exercise was to clarify DOD responsibilities during the establishment of the DHS. During initial meetings, there was little agreement as to what scenarios to utilize because of lack of consensus on the most likely "what ifs" – a return to the need for "actionable intelligence" to discern what, how, and where the terrorists were going to strike next. As a result, nine very broad scenarios such as "attack on a port" and "biological attack" were selected, and multiple branches and variations of each scenario were developed. The process was reduced to a discussion of what would be the most challenging scenarios (a lengthy list of extreme contingencies) and a conscious dismissal of any attempt to determine a limited and manageable number of likely "what if" contingencies. The end result was disagreement on reasonable scenarios and little progress on wargaming and planning due to an inability to get past discussions on the scenarios themselves. This is precisely what planners are told to avoid: "fighting the scenario."

The DHS recently attempted to overcome this challenge by formalizing a set of standard threat scenarios. This form of "universal threat" planning is designed to be the foundation for the

development of all "national preparedness standards from which homeland security capabilities can be measured."[4] Because of the current counter-terrorism focus and concern for potential mass casualty attacks, DHS introduced a formal threat baseline of "threat scenarios" that city planners are to use to evaluate their current level of manning, equipping, and planning for prevention and recovery capacity. While utilizing a scenario-based planning process, even the introduction to these "planning scenarios" stresses the need for capabilities-based planning and "for domestic incident preparedness to proceed through a capabilities-based approach."[5]

This effort has run into resistance from homeland security planners who claim that "one size does *not* fit all." The scenario-based approach makes claims of flexibility with "ways that allow them to be adapted to local conditions," but offers a framework of set tasks and agency roles that cannot be easily modified.[6] City planners and decision-makers are quick to point out that each city is in fact unique in its infrastructure, assets, resources, and vulnerability. The challenge for any scenario-based approach is to be able to plan with certainty that the scenarios developed will be the scenarios faced. That certainty is a rare and perishable commodity in the diverse planning community that addresses the multifaceted and ambiguous threats to the U.S. Homeland.

Therefore, neither "threat-based" nor "scenario-based" planning will work effectively for homeland defense or homeland security planning because the asymmetric threat cannot be used as a template.[7] Advocates of capabilities-based planning assert that it is this strong potential for the threat to achieve surprise by asymmetric means that makes threat-based and scenario-based planning a poor match for the needs of emerging planning challenges like homeland defense and homeland security. This is because:

- Threat-based planning is very susceptible to threat deception, causing the U.S. to mischaracterize and often underestimate the threat;
- Planners traditionally tend to "mirror image" threats when little hard intelligence is available which is only effective for symmetric threats;
- Large bureaucracies like DOD tend toward "group think" and discourage the unconventional thinking required to understand and assess asymmetric threats;
- Resource constraints tend to focus time and money on traditional big ticket weapons systems and discourage development of capabilities for the "unproven" asymmetric threats.[8]

The memories of 9/11 and the fears of unprecedented terrorist capabilities combine with these uncertainties to drive homeland defense and homeland security planners to search for a planning process that avoids these pitfalls.

DEVELOPING A CAPABILITIES-BASED PLANNING METHODOLOGY

To address the perceived growing complexity of the global security situation for the United States, the Department of Defense (DOD) is advocating "capabilities-based" defense planning to achieve a broad portfolio of military capabilities that will perform robustly in uncertain future environments.[9] As first formalized in the 2001 DOD *Quadrennial Defense Review*, a capabilities-based approach "focuses more on how an adversary might fight rather than specifically whom the adversary might be or where a war might occur."[10] To accomplish this broad goal, DOD planning focuses on strategic planning and is expressed in the newest Defense Planning Scenarios used to predict future contingencies. Strategic documents at DOD (e.g. *Strategic Planning Guidance*, *Contingency Planning Guidance,* and *National Military Strategy*) have started adopting this concept by focusing planning "on how adversaries will fight in the

future rather than on which specific adversaries we may fight." While not formalizing any definition of what the words "capabilities-based planning" mean (much less how to do it), each document addresses capabilities-based planning as a goal and a mechanism to overcome the nebulous nature of the strategic environment.

The genesis for this approach to planning was strategic thinking at the RAND Corporation's National Defense Research Institute. The author of much of the conceptual work behind the current push for capabilities-based planning is Paul K. Davis at RAND, who defines capabilities-based planning as "planning, under uncertainty, to provide capabilities suitable for a wide range of modern-day challenges and circumstances, while working within an economic framework."[11] Though focused on DOD force structure planning rather than campaign planning, Davis believes this new approach to Defense planning is not antithetical to threat-based planning, nor does it solely signify a shift in emphasis from threat to capabilities. Rather, it satisfies the need for increasing variability in Defense planning cases and in the key planning factors for friendly and enemy forces, to better account for uncertainty. For this approach, the question "who is the threat?" is addressed as a reworded question "what could the threat *do*?" to allow exploration of a much broader range of eventualities.[12] This helps planners to define capabilities needed rather than individual numerical solutions to narrowly defined, highly scripted individual cases because capabilities-based planning treats the threat as a continuum, within prescribed limits, rather than as a set of single-point values.

A working definition of "Capabilities-Based Planning" modifies these initial DOD and RAND characterizations in order to address the requirements of homeland defense and homeland security contingency planning for a flexible process that resembles a conceptual "menu" approach to planning. A capabilities-based planning process can therefore be defined as an analytical process of assessing strike means, capacity, and likelihood of all potentially hostile actors, with an emphasis on recasting intelligence uncertainty into a modular "menu" of potential threat capabilities. This planning process results in a solution framework emphasizing "building blocks" of capabilities that could be tailored to meet persistent general threats or a specific emerging threat.[13] By bracketing potential hostile capacities with assumptions of likelihood, planners can define and codify amorphous threats, develop a list of required capabilities and required authorities and policies to counter anticipated enemy actions, and retain flexibility in response to changes in the strategic threat environment. Each new piece of new intelligence further refines what threat capabilities exist and any "actionable intelligence" triggers the execution of pre-planned defense and security capabilities already identified and enabled.

Additionally, because the objective of any planning process is to facilitate senior level decision-making on resource allocation and risk assessments, both the process and the resulting plan must be clear to senior decision-makers. This ensures both senior leader involvement and the ability to make sound choices. By leveraging senior leader involvement, a comprehensible planning process should also clearly identify risks and recommendations on mitigation strategies to increase chances of success. The result of this planning process also must provide a linkage between the plan and required resources to identify decision points to decision-makers. The last requirement of an effective plan is a linkage between the plan and the organization's exercise and training program to provide the mechanism to validate and modify the plan.

DEVELOPING A CAPABILITIES-BASED THREAT ASSESSMENT

A new conceptual approach that combines the strengths of threat-based and scenario-based thinking needs to be found to structure and assess threats in homeland security and homeland

defense contingency planning. A solution to this challenge can be found in the concepts of "lines of operation" and "capabilities" as dynamics to define and explain potential and likely interactions. As opposed to the spatial or temporal divisions of the battle space by borders, or domains like air and seas, and phasing like build-up, defense, and offense, homeland defense campaigns are shaped by a reactive concept to threat actions and the division of the threat into potential lines of operation. "Lines of operation" are defined by the Department of Defense as "lines that define the directional orientation of the force in time and space in relation to the enemy."[14] For homeland defense and homeland security operations, these lines of operation can be modified to address distinct and related methods of both attack and defense such as "maritime attacks" or "attacks on continuity of government."

These lines of operation for the threat can then be defined and depicted in terms of specific capabilities. The Department of Defense dictionary defines a "capability" as "the ability to execute a specific course of action (a capability may or may not be accompanied by an intention)."[15] Having a capability implies the ability to perform a set of tasks required to accomplish the mission requiring the capability. This intentionally very broad definition covers both capabilities involved in strategic organizational issues (like force sizing and procurement) and operational issues (such as tactics and weapon performance). For this article, a capability is defined as the ability to perform a specified task within the conditions and performance standards accepted for that mission set. Therefore, the capability to conduct a "swarm boat attack" includes the ability to plan and execute multiple simultaneous attacks on maritime targets using small boats with an expectation of causing significant damage to the targets. However, it is important to highlight that this does not imply that the group with this capability has the plan or the intent to use this specific capability in their next attack.

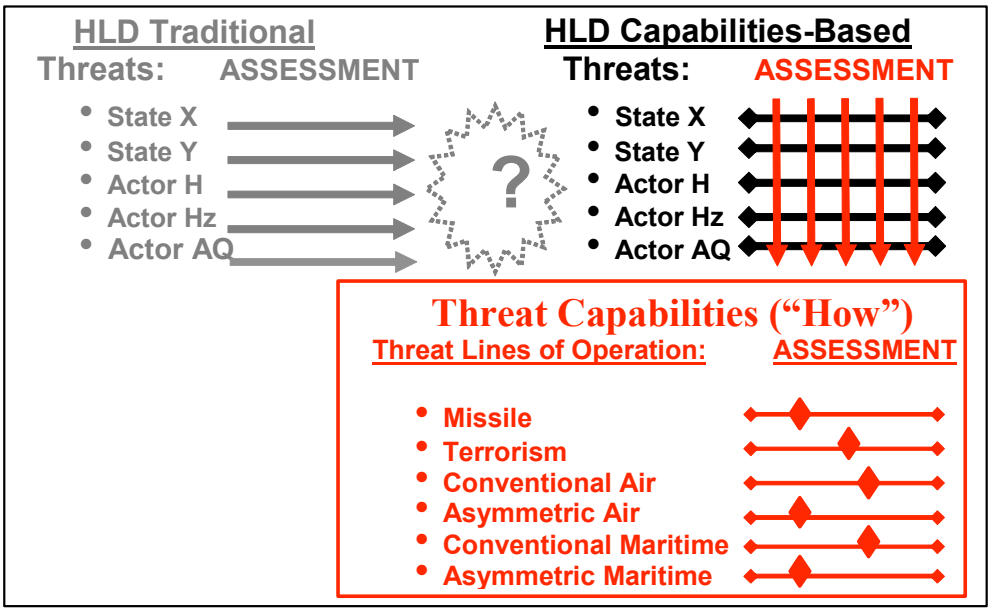


Figure 1
A Capabilities-Based Approach to Threat Assessment

In terms of identifying the threat, this "how" approach aims to produce a matrix of possible (and likely) threat capabilities that need to be countered by assessing the threat by capability and not by group or actor (see Figure 1). For example, with multiple actors possessing the means and

the will to conduct terrorism in the U.S. Homeland, the focus of assessment is not Al Qaeda, but any potential terrorist group; i.e., what terrorist acts (or capabilities) are possible? Now the question becomes manageable within current information limits because the intelligence analysts are no longer predicting what or where Al Qaeda will strike next, but how any terrorist could strike. In this manner, a capabilities-based threat assessment is done by first assessing what types of threat lines of operation are possible to bring threat capabilities against the U.S. (ballistic missiles? terrorism? air attack?). Then for each type of threat faced, threat lines of operation or "red lines" of threat capabilities can be developed to identify specific methods to deliver threat capabilities. Even this rudimentary level of analysis can assist planners in providing a framework for the threat environment. The combination of "lines of operations" and "capabilities" inherent in capabilities-based planning allows an intellectual structure to address the many challenges in homeland defense planning.

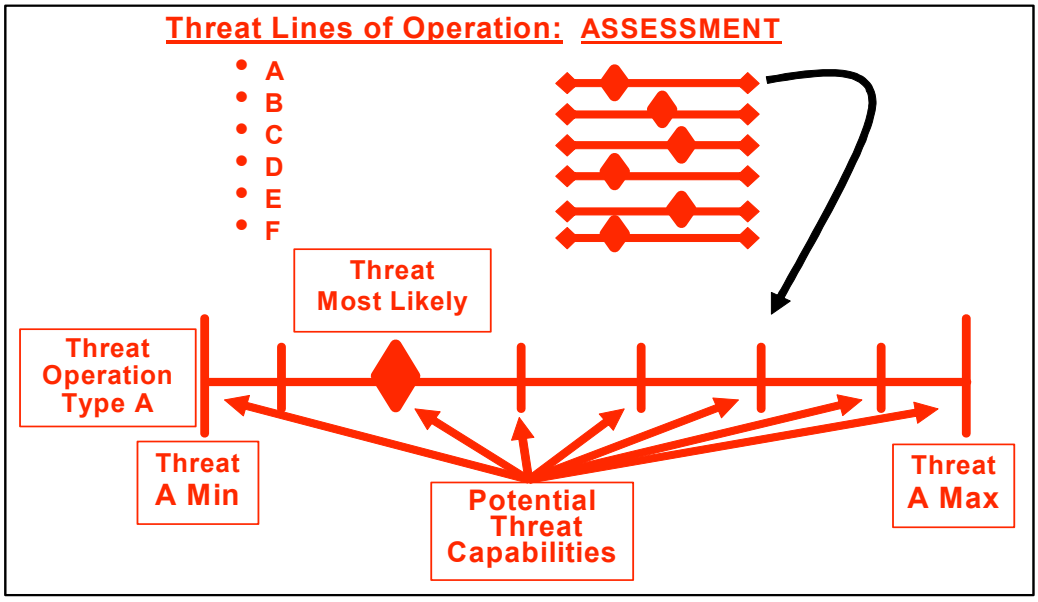


Figure 2
Developing Threat Lines of Operation and Threat Capabilities

The same assessment can then be done for each threat type to identify possible hostile capabilities. In building these threat lines of operation, or "red lines," intelligence can be used, not to dictate what exactly trans-national terrorist groups and rogue states are most likely to do, but rather to determine the range of possibilities – the maximum and minimum threat each group poses to the U.S. Homeland (see Figure 2). For example, the threat of ballistic missiles is both complex (due to the technical nature of the method) and well-understood (due to the limited number of threat actors and the physics involved). However, what exactly is the threat? If the threat of strategic attack is developed as a threat capability type, a relatively simple example of a threat line of operation emerges. Even though missile defense rests on hard data of numbers and ranges, developing a maximum and minimum limit to this threat "red line" helps frame the answer to the threat question and helps missile defense planners by scoping the challenge (and defining the required homeland defense capability). For example, the minimum threat to the U.S. Homeland is not zero (the potential for accidental launch or North Korean strategic miscalculation ensures that) and the maximum is not the combined strategic arsenals of China,

France, Great Britain, India, Israel, North Korea, Pakistan, and Russia. While intelligence information may reveal glimpses of the ideology and goals of various threat actors, the simple formula of "threat ideology plus capabilities equals likely targets and courses of action" cannot be used as a tool for threat assessment because ideology is difficult to assess and often can lead to simple – and incorrect – predictions of threat actions.

Problems with an ideological approach can surface on two levels during the threat assessment. First, a single group's ideology (often the group judged to be the most dangerous) can be superimposed on all threats, artificially narrowing potential threat courses of action and possibly overlooking equally likely capabilities. For example, the perceived aim of Al Qaeda is often offered as achieving the goals of "fundamental Islamists," but the numerous diverse groups under this label have disparate and often contradictory ideological objectives. Additionally, there is the complex and difficult problem of accurately determining a threat group's ideology from the outside, based on partial and limited information. For these reasons, the key for a viable assessment framework is to focus broadly across potential threats rather than on the perceived ideology of a single threat actor.

By building a spectrum of specific and distinct threat capabilities along a single line of operation, analysis of current intelligence on each threat actor can help to define what constitutes "likely" threats and anticipated means of attack, and can shape the minimum and maximum of the threat along the developing threat "red line" (see Figure 3). Intelligence can also guide the designation of a "most likely" attack method for each group and a collective "most likely" capability (seen in the red diamond on the threat "red line") for the entire threat line of operation. The result is a coherent and comprehensive threat assessment for a threat such as the notional "transnational air attack" line of operation depicted in Figure 4. Bracketing potential hostile capacities with assumptions of likelihood facilitates narrowing planning into manageable (and often affordable and acceptable) realms. Other possible threat capabilities associated with this threat type – regardless of which threat actor processes this capability or method of attack – are then posited between these assumed limits.

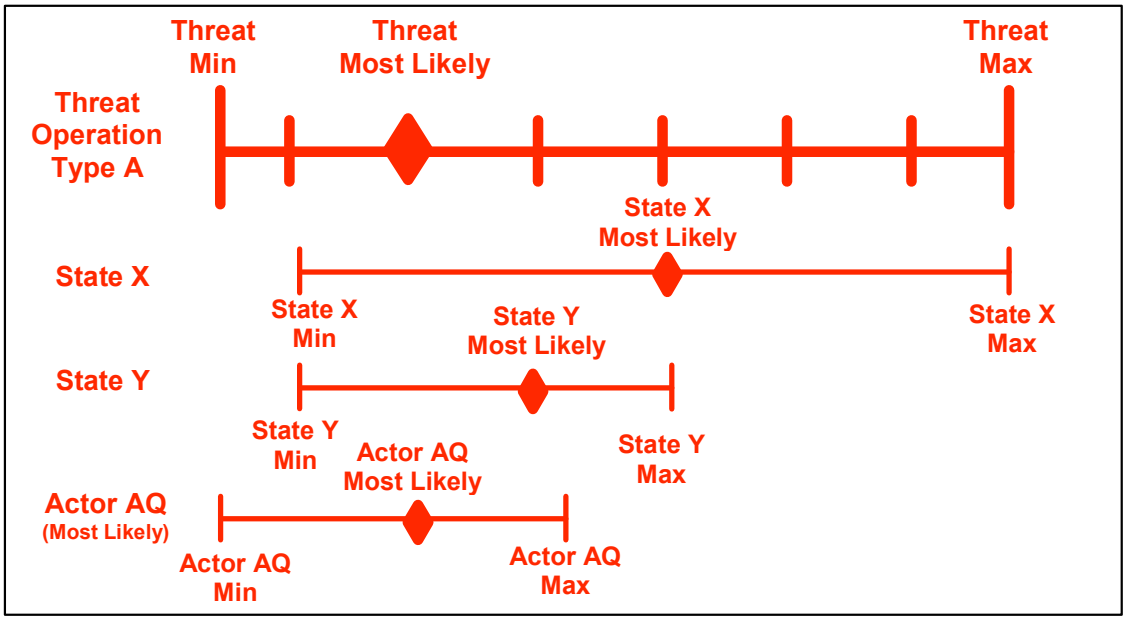


Figure 3
Developing an Assessment of Threat Capabilities

This "how" process also has the advantage of being conceptually simple, though complex and detailed in practice and open to constant conceptual refinement. An example of a simplified (and notional) capabilities-based threat assessment can be seen in the transnational air attack threat line of operation in Figure 4. This line of operation for the threat would be built to include all unconventional asymmetric air threats aimed at the U.S. Homeland, but tailored for the responsibility and role of the organization conducting the assessment. In this way, while each numbered capability point is subject to challenge and dissection, the holistic nature of the threat and what needs to be countered are graphically represented. Then current intelligence on various threat actors would determine the most likely threat threshold as seen by the red diamond depicted as capability G7. The "transnational air attack" line of operation (if conducted with actual intelligence available), would answer questions regarding the threat while being flexible to changing conditions on threat actors, intent, and capabilities.

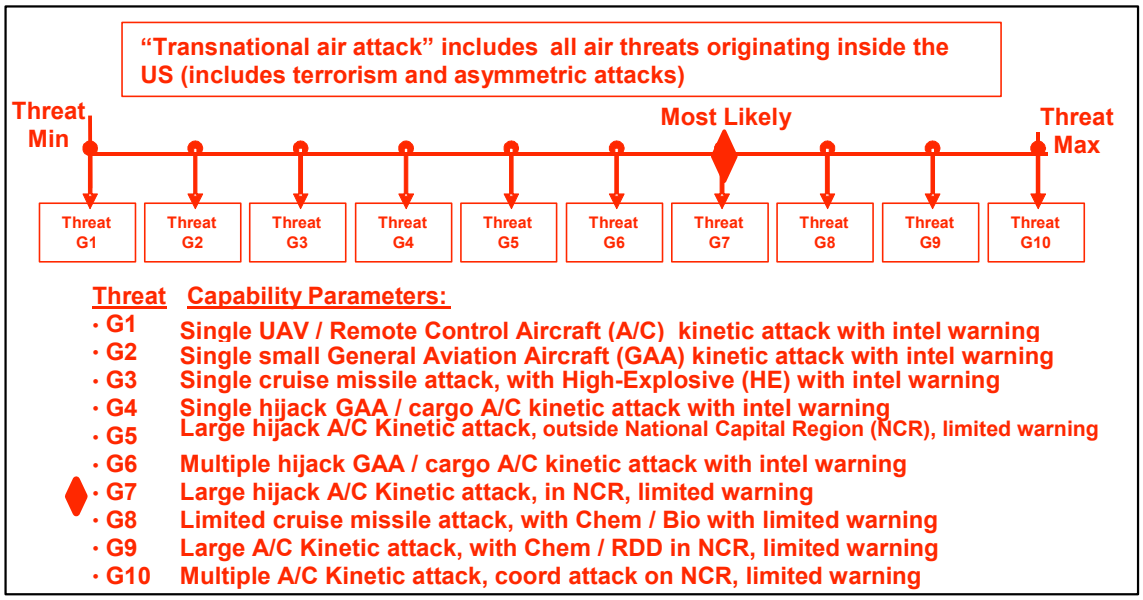


Figure 4
Example of Capabilities-Based Threat Assessments (Illustrative Purpose Only)

This capabilities-based approach to threat assessment can also work for Homeland Security-type threats where agency responsibilities overlap. An example of a simplified capabilities-based homeland security threat assessment can be seen in the transnational threat line of operation involving land attacks as depicted in Figure 5. In this example, eight threat capabilities are determined to be the potential "how" the enemy might attack and the three lowest magnitude capabilities (H1, H2, H3) are determined to be the most likely. This threshold "red diamond" of assessed probability can be adjusted by intelligence "chatter" or perceived changes in vulnerabilities (for example, during a special event). While focusing planners on the most likely threat, this capabilities-based assessment also depicts other, less-likely threats (H4 – H8) that must be addressed in contingency planning due to their greater magnitude and potential impact. While greatly oversimplified, these "red line" examples show enough assessment of the threat that planners can identify and develop defensive lines of operation and capabilities needed to counter these threats.

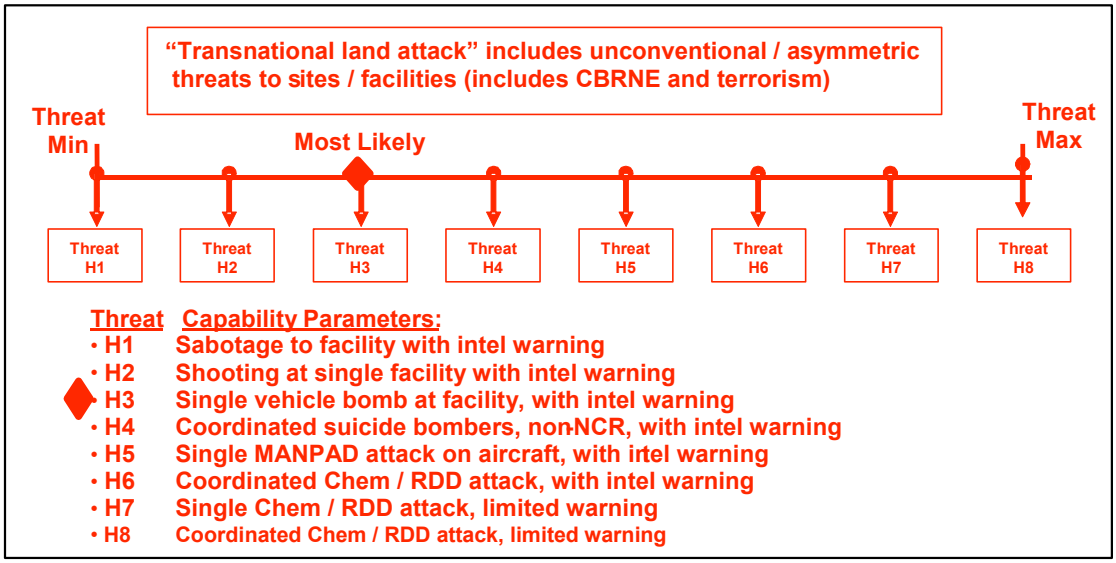


Figure 5
Example of Capabilities-Based Threat Assessments (Illustrative Purpose Only)

While this "how" assessment is a distinct process from traditional approaches to threat assessment, this focus on threat capabilities integrates the strengths of threat-based ("who") and responsibilities-based ("what") approaches. From threat-based, all available hard data on the threat can be integrated into an assessment of likely capabilities and maximum and minimum threats. This threat-based data is also required to define what each capability entails and its capacities and limitations (for example, defining what constitutes a "Vehicle Borne Improvised Explosive Device" or "VBIED" and what its possible delivery means). Additionally, assessments of current intelligence indicators and hostile leadership communications can focus efforts on certain threat lines and certain threat capabilities. As a result, the knowledge of the threat from a "threat-based" approach can be integrated into the proposed approach in the development of likelihood of the use of threat capacities and in determining the limits of these threat capabilities.

At the same time, each threat capability addressed on a threat line of operation ("red line") can be seen as an individual scenario that can be wargamed within a larger framework. Integrating the value of this type of "what" approach, each threat capability (i.e., capability point on a threat "red line") can be exercised as a possible scenario for planners and senior leaders to wargame agency responsibilities and required authorities. Certain "red lines" and threat capabilities can be identified as being a specific agency's responsibility because these assumptions have now been formalized and a mechanism identified to validate these divisions of responsibility. In this way, capabilities-based threat assessment is a viable and synergistic process of answering the simple and fundamental question "what is the threat?" by focusing on "how" a threat could attack the U.S. Homeland. Furthermore, this process is scalable and the resulting assessments could be as complex, or as simple, as the planning needs dictate.

DEVELOPING A CAPABILITIES-BASED MENU OF OPTIONS

The key to the capabilities-based plan is a direct linkage between threat capabilities and required friendly capabilities to counter them. As the threat has been assessed into a set number of capabilities and defined with a minimum and maximum potential threat, the friendly line of operation required to counter the threat can be bounded into a similar set of capabilities bounded by the same minimum and maximum as depicted in Figure 6. Then, each threat capability is examined to determine what can be done to negate this capability and prevent its successful execution by treating each as a distinct and individual threat scenario. For each specific threat capability to be successfully executed, certain threat actions must be taken in sequence concerning planning, preparation, transit, and execution, all of which can be wargamed even with a limited amount of knowledge. From this discrete and defined scenario of potential threat actions, an individual "blue" capability plan can be. The parameters of each capability data point can be expressed as planned protective and preemptive measures directed generically against the possible threat attack method.

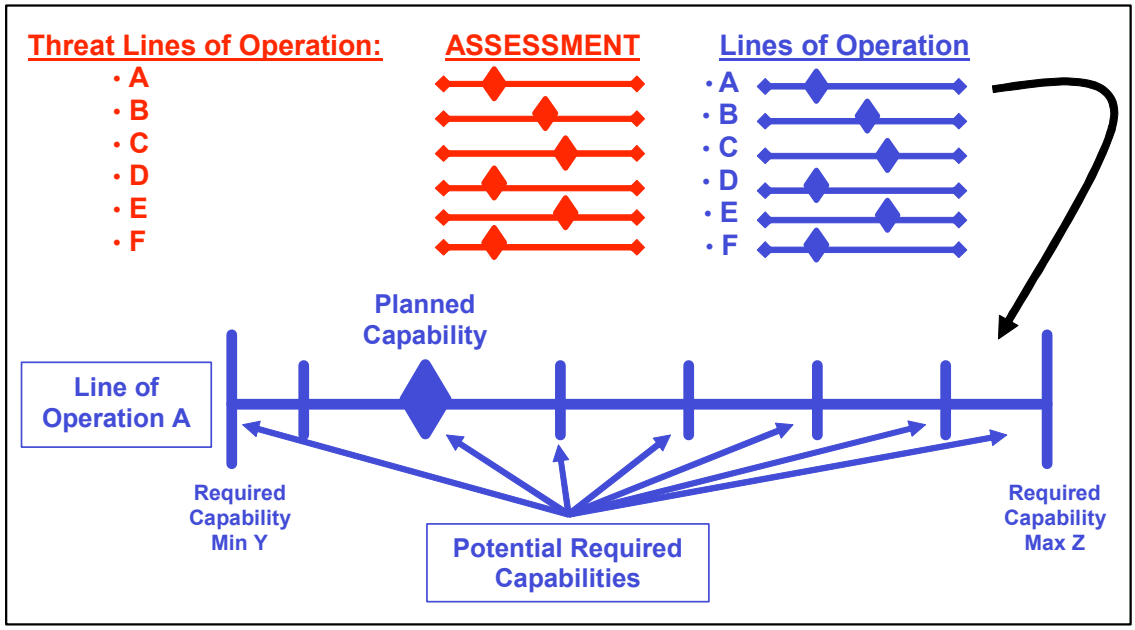


Figure 6
Capabilities-Based Planning Concept

While the intelligence assessment of threat capabilities sets the red diamond (likely threat), the experience and judgment of senior decision-makers establish the appropriate blue diamond or "planning threshold." This is not simply a matter of matching the anticipated likelihood of threat attacks. Decision-makers may decide either to over-match the threat by placing the blue diamond at a higher magnitude than the red or by accepting a greater risk by lowering the level of resource commitment. Additionally, setting the planning threshold at a certain point does not necessarily negate or ignore all threat capabilities along the higher end of the threat lines of operation because planners can still establish contingency plans for the emergence of a set of all of these less-likely, but higher magnitude, threat capabilities. In this way the planning threshold, or "blue diamond," just differentiates between "Be Prepared To" type tasks with dedicated resources and

unresourced contingency tasks, without eliminating any likely threats from planner attention and decision-maker consideration.

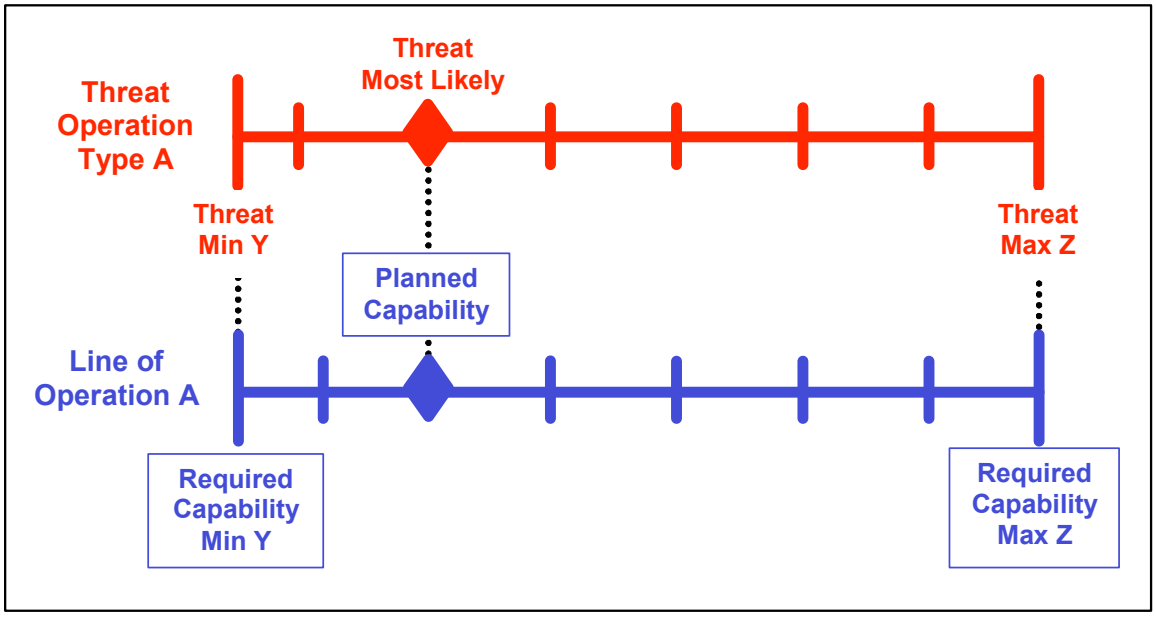


Figure 7
Countering Each Threat line of Operation

The development of individual lines of operations and specific capabilities can also be a method to integrate diverse capabilities and coordinated multiple organizations into a joint response. Planners from subordinate or outside organizations can develop independent and preventative lines of operation with unique and redundant capabilities assigned to counter the assessed threat capabilities (red lines with data points). Following any guidance on assignment of tasks and overall mission(s), leadership intent, and end-state objectives, planners can then produce their own organization's assessment of required capabilities (blue lines with data points) and resources required at each blue data point. Because capability experts are asked what they can *do* to counter a specific threat capability, detection, prevention, and defensive activities can be integrated into a single capability package and expressed as a single capability data point along the appropriate friendly line of operation (i.e., collected at a single point along a "blue line"). However, the strength of this approach also is that each capability point can be simplified and expressed to senior leadership for the difficult decisions on resources and risk.

An example of this approach is how a "blue line" could be developed against the notional "transnational maritime threat" line of operation. Because each of the labeled capability data points along the threat line of operation is a specific maritime threat scenario, homeland defense and homeland security planners can address each in turn to determine what their own organization could do to counter that individual asymmetric maritime threat aimed at the U.S. Homeland. For example, to counter the most-likely threat capability, planners would assess all possible preventative actions within their assigned area that could be used to defeat an attack by a single boat-bomb with limited warning. The resulting matrix of specific actions would include detection measures such as harbor patrol, prevention measures such as waterside obstacles and buoys, and defensive measures such as armed guards on board selected vessels and a more

heavily armed quick response force. The resources required for this capability would be identified, as would the warning time required to generate non-standing capabilities and the requirement for standing detection mechanisms to provide that warning time. While this example is grossly oversimplified, planners could use this approach to whatever level of detail required and then wargame each red capability against the proposed response to determine any shortfalls.

This example also demonstrates the inherent flexibility and adaptability of this approach to planning because the discovery or suspicion of a new threat capability or the emergence of a new threat group with an innovative line of operation against the United States would dictate the addition of blue points or possibly even entire new blue lines of operation. But this could be done during wargaming or even during crisis action planning without disrupting the larger concept of operation and planning approach. Decision-makers could also remove red lines and threat capabilities as threats are degraded or responsibilities shift between organizations. Resetting the "planning threshold" for each defensive line of operation can also be adjusted based on the latest threat intelligence queuing and decision-makers' judgment of the environment. This inherent flexibility and the cyclical nature of capabilities-based planning help integrate contingency planning and current operations by removing the distinction between how the two are expressed and assessed.

Because each friendly capability is matrixed individually, the process of determining resource requirements is relatively simple yet dynamic in response to a changing environment. The resources needed for each individual capability along each line of operation can be added and, after removing possible resource duplication, the total cost in personnel, equipment, and funding can be easily calculated. Because each capability data point can be considered as its own scenario and can be made as detailed as required with specific parameters and shaping assumptions, the resource requirements for each can be determined by asking the simple question, "what type and level of resources does your organization need in order to counter this specific threat?" For senior decision-makers and operators alike, this establishes a key linkage between resources and assessed threats in a straightforward manner.

Additionally, this process will reveal any required "enablers" (staff support tasks, standing or pre-designated command and control relationships, pre-approved authorities for using force, concept of employment for any alert forces, or coordinated surveillance tasks) needed for the planned capabilities (blue lines) to be executed. This can be done through internally wargaming the prevention plan at each capability point to determine what non-resource requirements – in communications, coordination, and authorities for example – were shortfalls or roadblocks to successful execution. This type of structured, but flexible, mini-scenario assessment and discussion can also facilitate coordination of which organization can most effectively deliver enablers and capabilities for prevention. By combining required resources with needed enablers, the cost of each "menu" item can be easily determined and clearly expressed as building blocks in capability to facilitate senior decision-makers' assessment of where the planner threshold should be established.

A CAPABILITIES-BASED VERSUS RESOURCES DECISION-MAKING APPROACH TO RISK

While this planning process allows for the identification of resources required at each point on blue lines of operation to deliver the needed capabilities, setting the planning thresholds allows senior decision-makers to have a deliberate mechanism to allocate resources and assess risks. This capabilities-based planning method addresses the concerns of the current USNORTHCOM

combatant commander by calculating and expressing the answers to the two key decisions "what do these resources buy?" and "where and how much is an acceptable level of risk for this Plan?" As seen in Figure 11, the process of matching threat capabilities and counter capabilities intentionally facilitates this decision-making judgment on resources versus risks by expressing the "building blocks" of capabilities as requiring a set number of resources to mitigate the risk of the threat capability they are built to counter. When the planned (and resourced) threshold is placed to match the most likely assessed level of threat, that number of dedicated resources can be stated as counter to that level of risk, as well as less robust threat capabilities (i.e., a preventative capability for multiple truck bomb attacks could claim to address the threat of a single truck or car bomb). However, planners may recommend, and decision-makers may select, either to assume a greater degree of risk by moving the "Planned Capability" threshold to the left (only addressing lower magnitude threat capabilities) or to increase the resource commitments to "buy down" the risks of less-likely, but greater-magnitude threat capabilities (see Figure 8).

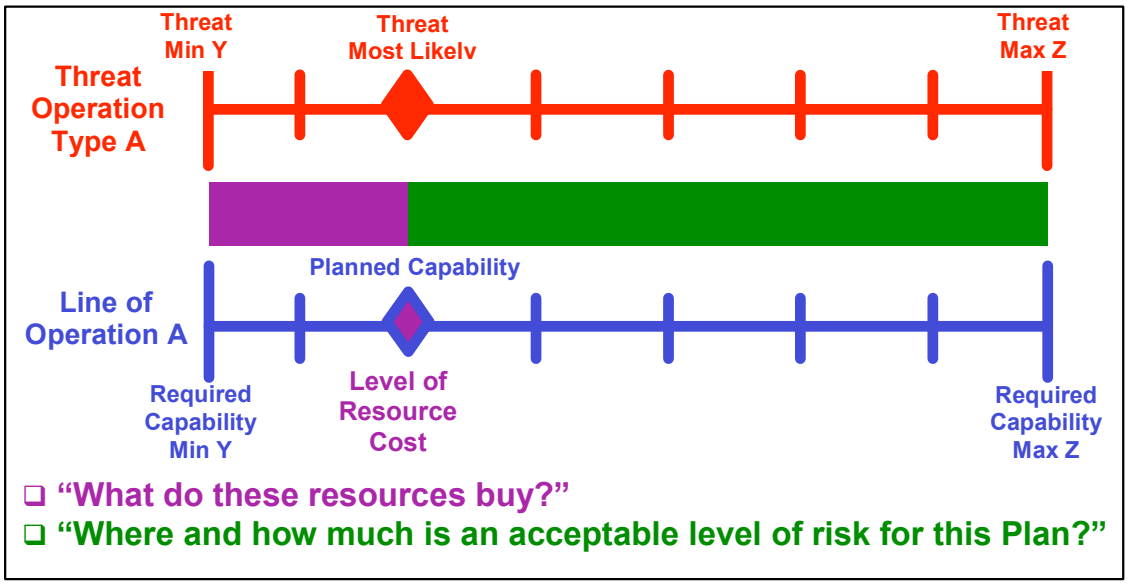


Figure 8
Assessing Resource Levels and Risks

As seen in the simple graphic above, this planning method addresses one of the major challenges by providing a formal mechanism to simplify complex contingency plans for presentation to senior decision-makers. By overlaying threat lines of operation ("Red Lines") with preventative lines of operation ("Blue Lines"), this can be done without oversimplifying resource and risk decisions or confusing the linkage between assessed threats and planned counters. While the intelligence assessment will determine the most-likely threat level and the placement of the red diamond on a threat line of operation, this approach appropriately places the decision of establishing the planned capability threshold or blue diamond where it belongs: in the hands of senior decision-makers. But unlike more traditional approaches to homeland defense and homeland security planning, now this decision is better facilitated and the risk-versus-resources trade-offs are better understood.

This approach also can be used to identify and mitigate mismatches in capabilities. As depicted in Figure 9, this is conceptually as basic as comparing likely threat capabilities and

available prevention capabilities. Where no counter capabilities exist, mitigating long-term risks requires investment and research strategies to develop what is necessary. Once the red lines and blue lines are compared to determine other shortfalls, mitigation strategies can also be developed on short-term risks. There are three possible ways to address a capabilities mismatch: increase preventive capabilities (move "Blue Diamond" to the right); degrade attack threat capabilities (force "Red Diamond" to the left); or accept risk for threat capabilities (identified as short-term shortfalls). The salient point of the analysis portrayed in Figure 9 is that this approach allows for a method of both developing and expressing these mismatches to senior decision-makers.

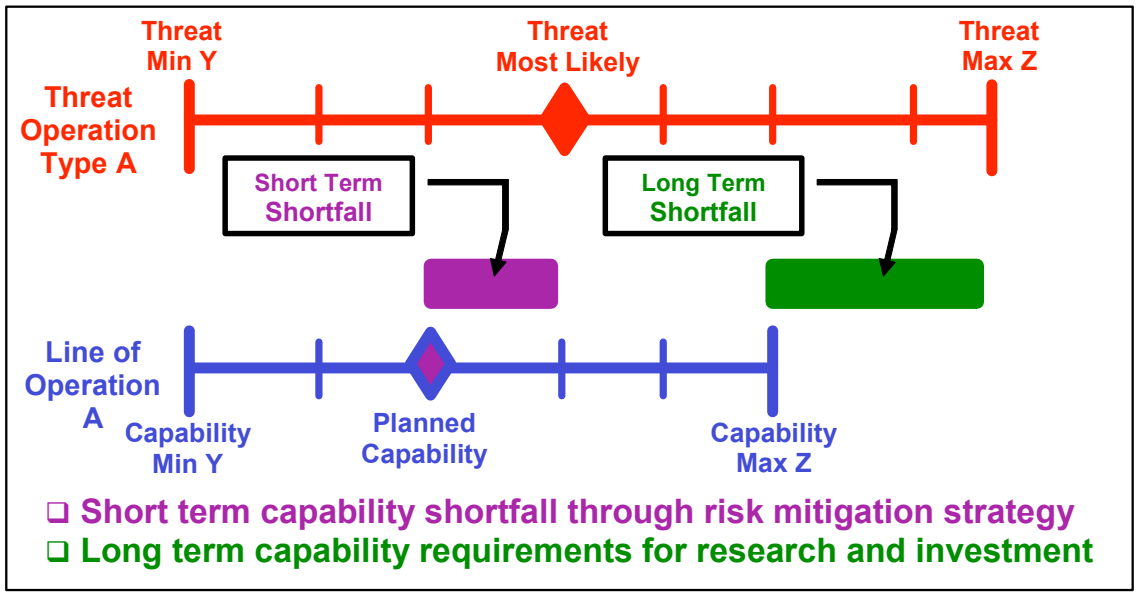


Figure 9
Determining Capabilities-Based Shortfalls

This capabilities-based approach to planning introduces both flexibility and adaptability by helping planners to define a menu of required capabilities rather than numerous, individual solutions to narrowly-defined, highly-scripted scenarios. Capabilities-based planning treats the threat as a continuum, within prescribed limits, rather than as a set of single-point values. This highlights one weakness in the concept: a more specific intelligence warning is required to determine the "where" and the "when" of the threat attack and the detailed tactical planning of where counter-capabilities need to be executed. But modified and tailored capabilities packages could also provide a general deterrence value by demonstrating an ability to counter threat lines of operations. The end result is a comprehensive "menu" of options to prevent and defeat attacks, expressed as a list of potential lines of operation against the threat and a list of specific capabilities required to meet and overcome inherent challenges in homeland defense and security planning.

CONCLUSION: The Adaptability of a Capabilities-Based Contingency Methodology

As required by the defensive mission of protecting the United States, capabilities-based threat assessment allows a greater focus on the "how" and not the "who" of the threat. Planners need to identify the threat of a truck bomb, for example; it matters little to defense and security planners

which group actually recruited the driver or rented the truck. By using a capabilities-based approach to threat assessment, the question "who is the threat?" is reworded as "what could the threat *do*?" to allow exploration of a much broader range of eventualities and give homeland defense or homeland security planners a defined and detailed threat to plan against. This alone would be welcome in nearly all contingency discussions on protecting the U.S. against terrorist threats as a method to overcome challenges of uncertainty haunting current homeland defense and security planning efforts.

One of the fundamental advantages of the capabilities-based planning process is that it is explicit. In expressing the threat assessment and resulting capabilities menu, the planning process model is rendered transparent. Assumptions and choices are tested and challenged in order to constantly revise, update, and improve the contingency plan. The planning process should integrate the needs and experience of senior decision-makers by presenting plans in a comprehensible format and allowing iterative involvement at every level of management and across different agencies and organizations. Capabilities-based planning can fulfill this requirement by formulating plans that can be expressed and adapted as both a menu of options and a rheostat of degrees of preventive response – all dictated by changes in intelligence warning. This approach to contingency planning exceeds the overall objective to overcome uncertainty with flexibility in planning.

Capabilities-based planning can therefore be seen as a way to combine the strengths of the threat-based and scenario-based planning methods while maintaining the required level of flexibility given the evolving nature of the threat. Because of the diffuse threat environment and the great probability of the enemy's use of surprise, each piece of new intelligence further refines what threat capabilities exist. Any "actionable intelligence" triggers the execution of pre-planned defense and security capabilities with required resources already identified and enabled. Secretary of Defense Donald Rumsfeld described this concept well when he wrote,

> It's like dealing with burglars: You cannot possibly know who wants to break into your home, or when. But you do know how they might try to get in. You know they might try to pick your lock, so you need a good, solid, dead bolt on your front door. You know they might try breaking through a window, so you need a good alarm. You know it is better to stop them before they get in, so you need a police force to patrol the neighborhood and keep bad guys off the streets. And you know that a big German Shepherd doesn't hurt, either.[16]

While all this may seem like common sense (as most quality planning is), a plan's effectiveness is limited by how comprehensive and comprehensible the resulting plans and briefings are – whether the plan is to stop a burglar or terrorists. The proposed capabilities-based planning method accomplishes this by producing a menu of options for decision-makers that is directly related to specific threat capabilities and linked to specific resources.

---

[1] Fire Department of New York City, *FDNY Strategic Plan 2004-2005* (New York City Fire Department, January 1, 2004), ii.

[2] U.S. Department of Homeland Security, *National Strategy for Homeland Security (NSHLS)*, July 2002 (Washington, D.C.: US Government Printing Office, 2002), 3.

[3] When military planners use the words "threat assessment," they are not just referring to any information or intelligence about potential opponents or enemies. They are also referring to the formal process of how this intelligence is analyzed and portrayed. Considering that the level, scope, and specificity of the intelligence to be assessed is often beyond the control of the planners, which approach or process is taken in the analysis phase is all the more critical in shaping the intelligence product sought: a "threat assessment." The importance of this military function is the common theme of current military doctrine on intelligence. See Department of Defense, *Joint Publication 2-0: Doctrine for Intelligence Support to Joint Operations*, 09 March 2000. (Washington, D.C.: US Government Printing Office, 2000), I-4.

[4] Homeland Security Council, *Planning Scenarios: Created for Use in National, Federal, State, and Local Homeland Security Preparedness Activities*, July 2004 (Washington, D.C., 2004), iii.

[5] Ibid., vi.

[6] Ibid., iii.

[7] *NSHLS*, 2.

[8] These four challenges for threat-based planning are detailed in the chapter "Responding to Asymmetric Threats" in *New Challenges, New Tools for Defense Decisionmaking,* edited by Stuart Johnson, Martin Libicki, and Gregory F. Treverton (RAND Corporation Publication MR-1576-RC, 2003), 43-44.

[9] To address the challenges of the post-9/11 world, Secretary of Defense Donald Rumsfeld described his way ahead by stating that the leadership of DOD had, "decided to move away from the old 'threat-based' strategy that had dominated our country's defense planning for nearly half a century and adopt a new 'capabilities-based' approach -- one that focuses less on who might threaten us, or where, and more on how we might be threatened and what is needed to deter and defend against such threats." Donald H. Rumsfeld, "Transforming the Military," *Foreign Affairs* Volume 81, Number 3 (May/June 2002).

[10] Department of Defense, *Quadrennial Defense Review Report* (Government Printing Office, 30 September 2001), iv.

[11] Paul K. Davis, *Analytic Architecture for Capabilities-Based Planning, Mission Systems Analysis, and Transformation* (RAND Corporation Publication MR 1513, 2002), 1.

[12] According to DOD Defense Planning Scenario development, "Capabilities-Based Planning is a method of Defense planning that examines a wide range of variability in factors, in order to achieve a broad portfolio of military capabilities that will perform robustly in an uncertain future environment." This unclassified quote is from a classified DOD briefing dated July 2003 from the Office of the Secretary of Defense that accompanied the staffing of the Defense Planning Scenarios.

[13] This "building block" approach is addressed as a key element in capabilities-based planning in Davis, *Analytic Architecture for Capabilities-Based Planning*, 4.

[14] U.S. Department of Defense. *Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms*, 12 April 2001 (Washington, D.C.: US Government Printing Office, 2001), 246.

[15] Ibid., 60.

[16] Rumsfeld, "Transforming the Military"

Homeland Security Affairs

Volume I, Issue 1 2005 *Article* 6

Summer 2005

American Naval Power and the Prevention of Terror

David Longshore*

*david.longshore@worldnet.att.net

American Naval Power and the Prevention of Terror

David Longshore

Abstract

Under the new "Joint Force" concept of operations model, the U.S. Navy has taken on added prevention responsibilities that include strategic and operational responses to asymmetric warfare. It is becoming evident that this Joint Force concept does not require an unduly large number of operational units in order to effectively support the nation's terrorism prevention mission. The lessons learned from the Navy's adoption of this concept, and its continuing evolution, are of considerable value to homeland security practitioners who are responsible for preventing terrorist activity within their respective jurisdictions. Communities should seek to develop surge capacity in their strategic and tactical theaters, conducting exercises to diagnose and strengthen this critical response component. Local organizations should consider three mission areas of prevention – interdiction, response, and redundancy – and develop qualifiers that can be applied to evaluating these areas. Furthermore, the Navy's emphasis on interagency cooperation and mission interoperability offers an example that can be followed by local homeland security jurisdictions.

AUTHOR BIOGRAPHY: David Longshore served as Director of Special Programs at the New York City Mayor's Office of Emergency Management (NYCOEM) between 2000 and 2004. He was among the first responders to the World Trade Center disaster on September 11, 2001, and played an integral role in coordinating the City's response to numerous emergencies, including the crash of American Airlines Flight 587, the 2001 anthrax attack, and the 2003 Northeastern Blackout. The author of several books, plays, and short stories, including A Deadly Sign (1993), Crooked Titians (1995), the Encyclopedia of Hurricanes, Typhoons, and Cyclones (1998; Second Edition, 2000), and Hello, Lyndon (2002), Mr. Longshore holds a B.A. in History and English, summa cum laude, from Amherst College, and an M.A. in Security Studies (Homeland Security and Defense) from the Naval Postgraduate School in Monterey, California.

KEYWORDS: naval, joint force, strategic response, operational response, surge capacity, interdiction, redundancy, interagency cooperation, mission interoperability

INTRODUCTION

In the years since the terrorist atrocities of September 11, 2001, the United States Navy has embarked on a comprehensive and innovative course of strategic and operational evolution designed to enhance the nation's ability to prevent acts of terrorism. In terms of its range and capabilities, the U.S. Navy has historically been one of the most versatile of the armed forces and its continuing transition, from its traditional blue-water mission of strategic deterrence to the new "Joint Force" concept of operations model dictated by the realities of asymmetric warfare, signifies the strategic validity of asymmetric response in terrorism prevention systems.[1] Despite budgetary constraints, the downsizing of ship numbers, rapidly evolving technology, and the persistence of outmoded strategic and public perceptions as to the role of sea power in the 21st century, the U.S. Navy has successfully adopted an overarching mission of transformation – generally known as *Sea Power 21* - that has consequently placed it in a much stronger position to operationally conduct terrorism prevention operations under the nation's homeland defense and security mandates.[2]

The Navy's dual-pronged approach to this transformational program has resulted in some controversial side effects (such as a reduction of the number of commissioned vessels necessary to achieve strategic and operational requirements) and a realignment of existing task force units. Not surprisingly, some of these shifts in doctrinal and operational direction have sparked concern and even criticism on the part of military experts and naval strategists.[3]

But as is becoming evident, the Navy's new Joint Force concept does not require an unduly large number of operational units in order to effectively support the nation's terrorism prevention mission. The key elements in terrorism prevention have been incorporated into the design and implementation of the Joint Force concept, and a much greater emphasis on mission configurability has resulted. This, in turn, has yielded enhancements in efficiency and effectiveness, and the cost savings that go along with them.[4] In 2005, the Navy possessed at least 25% more operational availability than it had in previous years, principally due to the provisions of the Fleet Response Plan (FRP).[5]

In addition to the practical value of analyzing the Navy's transformational techniques, the course that the Navy has charted in order to increase its preventative effect on terrorism illustrates that large institutions with many sea-miles of collective experience and tradition to their credit can successfully undertake reform and refinement programs without undue damage to operational morale and effectiveness. Indeed, the Navy's most effective response to the Joint Force mandate has been one of integration, expanding its former role of *strategic* deterrence to include a form of *tactical* deterrence, while never entirely abandoning the doctrinal teachings and strategic experiences that have shaped its history and given it cohesiveness.

Because the Navy's added prevention responsibilities now include strategic and operational responses to asymmetric warfare the lessons learned from its continuing evolution (as well as the systems, organizations and strategies employed in achieving that transformation) are perhaps of considerable value to similar homeland defense and security efforts in the nation's civilian public safety communities, many of which operate in paramilitary mission areas. Some of these lessons – such as doing more with less – are fairly generic occurrences in all jurisdictions, while others (like the *Sea Shield* mission area within the *Sea Power 21* concept) are an adaptation of the terrorism prevention

paradigm that is unique to the Navy's capabilities but which can be, in part, adapted for local terrorism prevention operations.

THE PREVENTION OF TERRORISM

Before analyzing the Navy's current role in terrorism prevention, a common definition of terrorism prevention as it exists in asymmetric strategic and tactical thought should be established.[6] Probably the most applicable analysis of why prevention doctrine is of such strategic value in countering asymmetric threats is found in the work of Martha Crenshaw, who posits that "The decline of terrorism appears to be related to the interplay of three factors: the government response to terrorism (which is not restricted to preemption or deterrence), the strategic choices of the terrorist organization, and its organizational resources."[7] Crenshaw's strategic interplay indicates that prevention strategies are applicable to all three factors that may deter or dissuade terrorist activity, and that this versatility of approach results in a unified tactical result. In Crenshaw's second and third principles, the strategic use of prevention results in tactical deployments that force the terrorist organization to undergo innovation; it is during and after these challenging periods of innovation that organizations are most likely to either abandon terrorist tactics, or dissolve.[8]

Based upon the larger strategic concerns of terrorism prevention, there are three specific mission areas within the homeland security matrix that address terrorism prevention's tactical objectives: Interdiction, Response and Redundancy. These mission areas have been extrapolated from several homeland security documents, primarily the doctrinal *National Strategy for Homeland Security* and the *National Strategy for Combating Terrorism*.

Interdiction can be defined as the timely application of response and support assets to the interruption of a terrorist organization's objectives. Equally well known as the "preemption concept," and variously defined by the studies of Corrado and Davis (1986), Cillufo and Tomarchio (1998), and Rose (2000), interdiction has grown in definition and objective to include active response mechanisms, such as information gathering and intelligence analysis, and the deployment of specially trained and equipped counterterrorism teams.[9] The *National Strategy for Homeland Security* stipulates the expansion of the interdiction discipline through the recognition that "Actionable intelligence is essential for preventing acts of terrorism. The timely and thorough analysis and dissemination of information about terrorists and their current and potential activities allow the government to take immediate and near-term action to disrupt and prevent terrorist acts…"[10] According to the *National Strategy for Combating Terrorism*, the, "…prevention of catastrophic terrorism is dependent upon interdiction of people and materials."[11] Interdiction can occur at any point in the planning and execution phases, and is preferably conducted during the early stages of a terrorist operation, before any opportunity for expansion or implementation is realized.

Response is the ability of a jurisdiction to deploy personnel and other resources to the amelioration of terrorist events. While many terrorism scholars tend to categorize response as a part of interdiction, (it is through response that terrorist acts are interdicted or thwarted) our definition of response focuses on peri- and post-event factors. In other words, the speed, efficiency, and efficacy by which response assets in a particular jurisdiction respond to unfolding acts of terrorism essentially determines how successful

that event is in achieving its destructive objectives. If, for instance, a jurisdiction were understaffed or under-equipped, it would be that much easier for terrorist organizations to exploit those weaknesses – and they can only be considered gaps – in conducting acts of terrorism. In this way, rapid and effective response is a form of deterrence in that terrorist organizations are less likely to attack a particular locale or jurisdiction if it is generally known (or determined by terrorist surveillance operations) that a rapid response will reduce the death toll, or quickly douse the resultant fires, or repair critical infrastructure nodes. The *National Strategy for Combating Terrorism* recognizes the importance of response in the prevention of terrorism by observing that, "…solid plans, preparations, and immediate response remain key to mitigating acts of terrorism."[12]

The third and final pillar of prevention theory – *redundancy* – is also the newest. Redundancy refers to that capability, whether on the federal, state, or local level, that deters or prevents attacks through the need to debilitate multiple locations or assets in order to achieve the terrorists' objectives. The *National Strategy for Homeland Security* contains extensive provisions for improving redundancy through the increased protection of critical infrastructure facilities. "Protecting America's critical infrastructure and key assets will not only make us more secure from terrorist attack, but will also reduce our vulnerability to natural disasters, organized crime, and computer hackers."[13] This versatility of approach is, in itself, a redundancy, and potently illustrates how vital a critical node the redundancy component is to the prevention strategy.

THE NAVY AS A STRATEGIC DETERRENT

The U.S. Navy's mandate to fully participate in the prevention of terrorist attacks on the American homeland necessitated a rethinking and redesign of many of its principal strategies and tactics. Before September 11, 2001, the U.S. Navy essentially had one primary mission: strategic deterrence. Strategic deterrence theory perhaps found its most significant – and successful – role in the nuclear deterrence strategies of the Cold War (1946-1986).[14] As manifested by the Cold War example, where the United States and the former Soviet Union stridently sought the numerical and tactical advantages inherent in the number of nuclear warheads and their respective destructive capabilities, the strategy of deterrence was most effectively realized from a position of size or strength. Studies conducted by Geis and Huston (1983) on the role of bystanders as defined by the Good Samaritan laws in California indicate that the physical size of participants plays a significant role in the successful outcome of such activity. "The important variable…was the size and strength of the bystander, *vis à vis* the victim."[15]

During the 1980's, it was critical to the Reagan Administration's interpretation of the strategic deterrence policy that the United States deploy a large navy, including a potent, submarine-borne ballistic missile capability. From a conventional viewpoint, the "600-ship Navy" served to counter the Soviet Navy's overly-ambitious strategy of possessing enough warships to seize control of the world's oceanic trade routes and thereby deny the use of the seas to the West. Moreover, in a symbolic sense, a navy with a seemingly endless supply of ships was a swing element in the strategic deterrence concept, as it indicated to the USSR that the U.S. possessed the technology, industrial skill, and financial resources to address wide-scale conventional as well as nuclear threats. It was, perhaps, this versatility of strategy and tactic that ultimately gave the deterrence policies of the Reagan and first Bush Administrations' their winning edge.

But since the collapse of the Soviet Union and the end of the Cold War, the need for the U.S. Navy to maintain a large, expensive and exclusive strategic deterrent has clearly diminished. It is an irony of victory; by so ably winning the Cold War and removing for the time being any challenge to the preeminence of the U.S. in global military and economic affairs, the U.S. Navy essentially decommissioned not only many of its ships, but the very strategies that had defined its operational objectives, and even its public perception, since the opening days of the Cold War.

THE NAVY AS TACTICAL DETERRENT

In devising its strategy for the new century, the Navy realized that it would prove of little benefit to the nation's overall security to completely abandon its strategic deterrence concepts – any more than it is necessary for local police departments to give up traditional crime fighting duties in order to effectively prevent acts of terrorism. In implementing the provisions of *Sea Power 21*, the U.S. Navy has repeatedly signaled its understanding that while the strategies and tactics of naval warfare may change over time, the primacy of effective, mission-specific sea power remains a constant. This strategic realization has permitted the Navy to adopt the Joint Force concept and evolve in operational dexterity by expanding its historical emphasis on strategic deterrence to include what can be considered a new interpretation of tactical deterrence.[16]

The Navy is certainly familiar with asymmetric strategies and tactics. In 2000, one of its vessels, the USS Cole (DDG 67), was the target of an asymmetric attack that left 17 service personnel dead and an important combatant unit out of commission for several years. In January 2001, the Navy released its investigation of the Cole attack, which noted that "the commanding officer of Cole did not have the specific intelligence, focused training, appropriate equipment or on-scene security support to effectively prevent or deter such a determined, preplanned assault on his ship."[17] Although the bulk of the Navy's terrorism prevention efforts came into existence after September 11, 2001, the bombing of the USS Cole spearheaded a new awareness of asymmetric threats within the Navy hierarchy. As early as February 2001, the Task Force on Antiterrorism and Force Protection, conducted under the aegis of the Secretary of the Navy (SECNAV), established the preliminary framework by which improved force protection could be achieved. This program included a changing of the mindset that informed force protection precepts, as well as a number of asymmetrical tactic changes, including improved pre-deployment training, enhanced threat and situational awareness, and in-theater support for U.S. naval vessels entering new ports.[18]

To correct the vulnerabilities in organization, capabilities and tactics evidenced by the attack on the USS Cole, the Navy's *Sea Power 21* doctrine and its resulting Concept of Operations (CONOPS) framework have integrated the three mission areas of terrorism prevention – Interdiction, Response and Redundancy – into its respective mission areas. As history has shown, and *Sea Power 21* recognizes, naval supremacy is not principally achieved through superior numbers but through superior tactics, logistics, and discipline. In this way, *Sea Power 21* provides for the preventative deployment of the very same asymmetric strategies and tactics that would be used by the nation's opponents.

It first accomplishes this by dividing its warfare capabilities into four primary tactical qualifiers, namely: speed, agility, precision and persistence. These qualifiers (which are

essentially evaluative in nature and fairly self-explanatory) are then applied to three mission areas known as "Sea Strike," "Sea Shield," and "Sea Basing."

The first of these mission areas, "Sea Strike," indicates that the Navy's time-honored role as the nation's first-line means of projecting strategic deterrence has not been omitted from the *Sea Power 21* doctrine. As its moniker indicates, Sea Strike provides for the projection of strategic deterrence and its influence on the prevention of terrorism through deterrence aimed at nation-states that serve as terrorist havens. "Sea Strike," Sea Power 21 reads, "is the ability to project precise and persistent offensive power from the sea." This "precise and persistent offensive power" has clearly been of invaluable use in the vast air campaigns over Afghanistan and Iraq, which were launched from U.S. Navy aircraft carriers. By assisting in the removal of governments and regimes that harbor and provide succor to terrorist organizations, the U.S. Navy's "Sea Strike" mission is providing a powerful strategic and tactical deterrent for the prevention of future terrorist attacks.

The second component in the *Sea Power 21* doctrine, dubbed "Sea Shield," is perhaps where the Navy's new mission most closely adheres to the prevention of terrorist and other asymmetric attacks as interpreted by civilian homeland security operations. "Sea Shield integrates forward-deployed naval forces with the other military services, civil authorities, and intelligence and law-enforcement agencies.…Homeland defense will be accomplished by a national effort….We will identify, track, and intercept dangers long before they threaten our homeland." The Sea Shield component also contains provisions for the implementation of the Fleet Response Plan (FRP) which stipulates operational support for the nation's allies in detecting, disrupting and denying terrorist organizations – and by extension, any asymmetric opponent – the use of the world's oceans.

Homeland Security's emphasis on developing and implementing enhanced intelligence capabilities, which are critical to the efficacy of the Interdiction mission through improved situational awareness, have been included within the Sea Shield rubric. "Maritime patrol aircraft, ships, submarines, and unmanned vehicles will provide comprehensive situational awareness to cue intercepting units." As advocated by Sea Shield, situational awareness extends to the use of sophisticated equipment to nullify the danger of secondary or tertiary devices being deployed as part of a terrorist or asymmetric operation. "When sent to investigate a suspicious vessel, boarding parties will use advanced equipment to detect the presence of contraband by visual, chemical, and radiological methods."[19]

The third of *Sea Power 21's* mission areas, Sea Basing, "…enhances operational independence and support for the joint force." Primarily logistical in design and purpose, Sea Basing further addresses asymmetric possibilities as they pertain to communications, computer security, and infrastructure protection. Since the Navy's mission is growing more asymmetric in nature, it is not unrealistic or impractical to apply asymmetric doctrine to its tactics and strategies. One of the most effective ways in which the Navy can counter asymmetric threats is therefore through redundancy, and the Sea Basing concept provides for surge capacity in the event major offensive or defensive activities are required.[20] This surge capacity includes providing a sufficient degree of logistical support to forward-operating nodes, including up to ten aircraft carrier task forces simultaneously.[21] The Sea Basing concept further provides for the repositioning of existing Navy assets, such as establishing a homeport for one of the USS Nimitz (CVN

68) class aircraft carriers in Hawaii or the American protectorate of Guam. Some naval officials have advocated that the permanent deployment of a carrier task force in Guam will serve as a deterrent to terrorist activity. "If you were a week away or two weeks away, that provides an opportunity to do something," Admiral Arthur J. Johnson, commander of US Navy forces in the Marianas Islands, said of terrorist tactics. "Just by having the capability in the neighborhood, it forces people, transnational terrorists, to redo their calculus."[22]

The Navy's assumption of terrorism prevention duties under the Joint Forces precept has led to tangible improvements in interagency coordination and mission interoperability. In the first six months of 2005 alone, the Navy conducted half a dozen deployments in support of the global alliance against terrorism, including participation in the North Atlantic Treaty Organization's (NATO) Response Force Maritime Group and Operation Active Endeavor, NATO's overall response to asymmetric warfare and terrorist activity. The Navy conducts similar interoperability exercises in the Pacific Ocean, most recently with Singapore as part of the Cooperation Afloat Readiness and Training (CARAT) program. On June 6, 2005, while conducting Maritime Security Operations (MSO) in the Indian Ocean, the USS Gonzalez (DDG 66) thwarted an attack on a motor vessel by a band of pirates operating in Somalia's littoral environment. MSO "…sets the conditions for security and stability in the maritime environment and complements the counter-terrorism and security efforts of regional nations. MSO denies international terrorists use of the maritime environment as a venue for attack or to transport personnel, weapons or other material."[23] As evidence of the effectiveness of the MSO mission area, Navy officials point to an April 2004 incident where an explosives-laden dhow, en route to the oil terminals at Khawr Al Amaya and Al Basrah, was intercepted by MSO units. Although the dhow exploded with the loss of three U.S. service personnel, its ultimate objective was denied, thereby preventing a much greater loss of life and the asymmetric destruction of a vital energy infrastructure node.[24] Clearly, mission interoperability, along with a strong naval presence, does serve to prevent or limit acts of asymmetric warfare and their immediate effects.

NEW CAPABILITIES

Changes in doctrine, strategy and tactics are only part of the U.S. Navy's assumption of the Joint Forces paradigm. New mission areas require new capabilities, some of which are organizational in direction, and some that are more resource and equipment-oriented. The U.S. Navy presently possesses the most sophisticated warships in existence. The *Sea Power 21* doctrine stipulates that it do so and the continued achievement of its Joint Force mission requires nothing less than full compliance. It has been the Navy's new mission of preventing and responding to asymmetric threats that has driven the development and construction of some of its most innovative combat units. While these new vessels do possess capabilities that will allow them to fully participate in the Navy's traditional strategic deterrence mission, their greatest success may be realized in an asymmetrical operational theater.

In a keel-laying ceremony held in early June of 2005 at a Wisconsin shipyard, the Chief of Naval Operations, Admiral Vernon Clark, joined the widow of an Army sergeant killed in action in Iraq and posthumously awarded the Congressional Medal of Honor, in sponsoring the newest of the U.S. Navy's ships, the USS Freedom (LCS 1).

With its sleek appearance and broad operational parameters, the USS Freedom represents an entirely new type of vessel for the U.S. Navy - the Littoral Combat Ship (LCS). Measuring some 378 feet in length and displacing approximately 2,000 tons, the Freedom and its sister units are designed to operate at high speeds and with maximum maneuverability in brown-water or shallow littoral (coastal) environments. The first new class of naval vessel to be introduced in over a decade, the LCS is intended to tactically counter a flotilla of asymmetric threats, including mines, conventional-powered submarines, and swift surface combatant vessels. Each LCS will operate at speeds in excess of 40 knots, and can operate in drafts of less than 20 feet. While the first generation LCS program calls for four units to be placed into service between 2007 and 2009, an additional nine, second flight units are due to be commissioned between 2010-2012. Eventually, the U.S. Navy intends to operate up to between 60 and 100 LCSs as part of its ongoing transformation into a 21st century fighting force.

But in a very real sense, the true significance of the USS Freedom lies in its name, in what it represents to the evolving strategies of sea power in the first half of the 21st century.[25] Because of its unique and diverse array of capabilities, the LCS introduces new resources that will better enable the U.S. Navy to counter the tactics associated with asymmetric warfare, as well as the more traditional forms of combat at sea. And with this enhanced ability comes the U.S. Navy's freedom from many of the outmoded doctrinal tenants that have long typified our nation's strategic and tactical relationship with sea power.

In addition to the LCS and a new series of Mark V special operations craft, the Navy is constructing a new class of surface combatant called the DD(X). Viewed as a potential successor to the relatively-new Arleigh Burke (DDG 51) destroyer class (to which the USS Gonzalez and the USS Cole belong), and bristling with technology that is adaptable to a future fleet of cruisers, the DD(X) will (when commissioned between 2009 and 2011) bring new levels of asymmetric versatility to the defense of the world's oceans. Fitted with an integrated all electric propulsion system, dual band radar, a peripheral vertical launch system, and a hull design that enhances speed and mobility, the DD(X) and its mission reconfigurable siblings will greatly improve the Navy's ability to conduct blue and brown-water Sea Shield operations aimed at interdicting and preventing asymmetric attacks on the American homeland. Additionally, it will bring greater precision to land warfare and the special operations that frequently accompany terrorism interdiction and response campaigns.[26] Illustrations of the proposed DD(X) class show a vision of the nation's seagoing future that looks not unlike a submarine operating on the surface. It is perhaps largely symbolic in import, but it is an interesting feature of the DD(X) class that well over half of the vessel will exist below the waterline, hampering its participation in some littoral theaters, but providing for unprecedented protection while engaged in blue-water and anti-ship missile operations. In what may prove an asymmetric defense capability of the first order, the DD(X) design permits the vessel to use its environment for protection and added tactical stealth. Because these qualities are powerful tools in any Interdiction or Response operations, the DD(X) as conceptualized will serve as an effective terrorism prevention safeguard.[27]

There have also been several calls for a renewal of the Navy's conventional-powered submarine building program, with the intent that these vessels would prove an effective counter to asymmetric attacks launched from quiet-operating submarines. So far the

Navy has resisted this, most probably because anti-submarine warfare operations can be more effectively addressed by the LCS and DD(X) concepts.[28]

CONCLUSIONS

The U.S. Navy's experience in adopting its most recent program of transformation contains a number of lessons for homeland security practitioners who are responsible for preventing terrorist activity within their respective jurisdictions.

The development of new mission areas within the Navy has indicated the importance of obtaining and deploying equipment that can in fact support these mission areas. While it is true that the U.S. Navy possesses considerable resources, these are proportionally no greater in relation to its evolving mission than they would be for state and local jurisdictions with more finite terrorism prevention responsibilities. Where the Navy has been successful in this regard is in avoiding the tendency to allow strategies, rather than more specific tactical objectives, to determine operational and equipment needs.

The Navy's experience has also shown that communities should seek to develop surge capacity in their strategic and tactical theaters, and conduct exercises to diagnose and strengthen this critical response component. The Navy's Fleet Response Plan (FRP) is a sound conceptual model that state and local jurisdictions can adopt for their own homeland security surge requirements. As the Navy has evidenced, surge capacity is an important tactic in asymmetric operations, be they part of a larger military action or taken in response to an event on the state and local levels. Its ability to double capacity for short periods of time (in what the FRP refers to as the "emergency surge" response level) establishes a benchmark standard which organizations with similar homeland security and public safety responsibilities can augment.[29]

When developing strategic and tactical programs, local organizations should consider the three mission areas of prevention, and develop evaluative qualifiers that can be applied to the Interdiction, Response, and Redundancy mission areas. *Sea Power 21* stipulates four operational qualifiers - speed, agility, precision and persistence – while other applicable qualifiers might include timing, diligence, organization, and diversity.[30] Like the Navy, jurisdictions and organizations that adopt evaluative criteria or standards will find it easier to define and refine their terrorism prevention strategies and tactics.

The Navy's emphasis on interagency cooperation and mission interoperability is another example that can be followed by local homeland security jurisdictions. In addition to drills and exercises designed to familiarize players with equipment capabilities and operating protocols, the Navy's Maritime Security Operations (MSO) program enhances the nation's asymmetric response capabilities by forging a working coalition between the Navy and its maritime partners. According to Vice Admiral David Nichols, who coordinates U.S. maritime security operations in the international waters of the Persian Gulf-Indian Ocean theater, "Pressurizing the maritime environment describes an effect…which deters the terrorists from using the maritime environment.…We do that via integrated operations amongst a coalition force of several nations across the entire region inside and outside the Gulf."[31]

Adapting this kind of interoperability at the local level should strengthen efforts to prevent terrorism. First, a unified effort signals deterrence, and makes it much harder for asymmetric operations to be planned and implemented. Second, the interoperability model requires that personnel and their core capabilities from several different

departments, and even nations, become actual stakeholders in the strategic and tactical objectives that constitute interoperability. Among other benefits, the practice raises morale which, in increasing warrior proficiency through the Navy's mission area qualifiers of speed, agility, precision and persistence, enhances the Navy's ability to deter and prevent acts of terrorism. At a time when communities around the U.S. are implementing the National Incident Management System (NIMS), the Navy's system for achieving interagency operability while maintaining unit independence and readiness stands as a workable model and reference point.

As it has been for the Homeland Defense and Security community, the Navy's doctrinal and operational shift toward preventing acts of asymmetric warfare has been set against the backdrop of a rapidly changing global power dynamic. In addition to the transnational asymmetric threats posed by terrorist organizations, China, in particular, figures prominently in many of the Navy's scenarios, and contemporary observers of sea power have been quick to note this strategic sea change.[32] While *Sea Power 21's* concept of operations emphasizes the importance of an asymmetric response to asymmetric threats, the Navy's traditional role of strategic deterrence against nation-states that seek to employ asymmetric strategies and tactics has not been ignored.

Indeed, the Navy's adoption of the Joint Forces doctrine has in part been aided by China's strategic and tactical reliance on the tenants of asymmetric warfare to determine its shipbuilding priorities. China's recent escalation of its naval capabilities program has largely been inspired by its determination to deter moves by the Taiwanese to seek independence and to tactically counter any military intervention on the part of Taiwan or the United States. When one considers the type of vessels the Chinese People's Liberation Army Navy (PLAN) is presently placing into service, it would appear that a *guerre de course* – a war of trade - is not its primary concern at this time. It is building these specialized vessels with specific operational parameters in mind, namely that of deterring U.S. military support for Taiwan.[33] The United States is not alone in making preparations to counter China's burgeoning emphasis on asymmetric sea combat. Taiwan itself has undertaken a rapid reconfiguration of its military infrastructure, including the acquisition of destroyers, diesel-electric attack submarines, and aircraft, which will reach its apogee within the next decade. Known as the "offshore defense strategy," Taiwan's intention is to develop an effective military deterrent to a Chinese invasion, with particular emphasis on deterring activity in the Taiwan straits.[34]

The U.S. Navy must continue to maintain a strident level of strategic deterrence in order to maintain the present balance of power in eastern Asia. At first glance this might seem more of a tactical imperative, except that in doing so, the Navy is in fact acting in the role of a strategic deterrent to a potential rise in domestic terrorism. A survey of terrorist-related events indicates that as empires and nations undergo periods of economic contraction, incidences of terrorist activity tend to increase. There are several reasons for this relationship, among them the perception that economic decline translates into an inability to adequately project the military and economic power necessary to deter or prevent acts of terrorism. In the years following the First World War, Great Britain saw both its economic and military primacy over the world's affairs markedly reduced. Once this perception became widespread, numerous instances of terrorist activity – particularly on the part of Irish nationalists – occurred. A similar series of events has been witnessed in several of the republics that formerly comprised the Soviet Union. Once the

cohesiveness of the Soviet empire was lost, acts of asymmetric warfare occurred in several republics.

At the present time, with the U.S. maintaining its economic and military primacy, acts of terrorism against its domestic and international interests do occur, but not with the frequency that historical data indicates could be possible were the nation to economically and militarily weaken. For nations and societies, the future is often a pathway that winds through darkness and uncertainty, and the American eagle is not without potential challengers to its economic and military supremacy – including one increasingly acquisitive dragon. By maintaining strategic deterrence through tactical deterrence, the U.S. Navy continues to play a pivotal role in preventing acts of terrorism by protecting the framework by which U.S. economic and military dominance can be sustained.

While at the present time the U.S. Navy does have many operational missions, ranging from strategic deterrence and amphibious operations to logistical support and Homeland Security duties, its most important mission continues to be that of strategic and tactical evolution. As the Chief of Naval Operations wrote in his 2005 Guidance, "Transforming ourselves and our great institution for the dangerous decades ahead is our imperative."[35]

---

[1] Vernon Clark, "Sea Power 21: Projecting Decisive Joint Capabilities," *Proceedings*, October 2002. Clark writes: "…we will continue the evolution of U.S. naval power from the blue-water, war-at-sea focus of the 'Maritime Strategy' (1986), through the littoral emphasis of '…From the Sea' (1992) and 'Forward…from the Sea (1994),' to a broadened strategy in which naval forces are fully integrated into global joint operations against regional and transnational dangers."

[2] For an interesting analysis of earlier transformation programs in the U.S. Navy, see Norman Friedman. "Transformation – A Century Ago," *Naval History*, U.S. Naval Institute, 19, No. 2 (April 2005): 32-37.

[3] Alfred Thayer Mahan, *The Influence of Sea Power Upon History*, *1660-1783* (New York: Barnes and Noble Books, 2004), 35. Mahan warns us of the unreliability of large fleets as a guarantee of ultimate victory when he writes, "When the [Napoleonic] empire fell, France had one hundred and three ships-of-the-line and fifty-five frigates." *See also*, Robert D. Kaplan, "How We Would Fight China," *The Atlantic Monthly*, June 2005, 49. Kaplan writes: "Our present Navy is mainly a "blue-water" force, responsible for the peacetime management of vast oceanic spaces…and one that enables much of the world's free trade." *See also*, Tim Weiner, "Arms Fiascoes Lead to Alarm Inside Pentagon," *The New York Times*, June 8, 2005: A1. Weiner's article highlights many of the difficulties the armed forces, including the Navy, have experienced in procuring reliable weapons systems. The article also points out the spiraling cost of weapons systems, a refrain that has been echoed by the Navy's leadership for some time. In a March, 2005 interview with *Naval Forces* magazine, Adm. Clark indicated: "What really concerns me is the ever-increasing cost of the assets that the nation needs for its Navy."

[4] Vernon Clark, "Building a 21st-Century Navy," Interview with Gordon I. Peterson, *Naval Forces Magazine,*1 (2005). Clark remarks: "One of my officers declassified a memorandum about the Navy's acquisition plan for 1967. Allowing for inflation, you get a $129 billion budget that year compared to our budget for fiscal year 2005 which is $119 billion. The 1967 budget bought 620 airplanes and 47 ships. Fiscal year 05 is the best year since I have been here, and we funded eight ships and 113 airplanes."

[5] Ibid.

[6] See Bruce Hoffman, *Inside Terrorism* (New York: Columbia University Press, 1998) for an analysis of the character and behavior of strategy and tactic as applied to counterterrorism thought.

[7] Martha Crenshaw, "How Terrorism Declines." *Terrorism Research and Public Policy*, 80

[8] Martha Crenshaw, "Innovation: Decision Points in the Trajectory of Terrorism," The Conference on "Trajectories of Terrorist Violence in Europe," March 9-11, 2001, Minda de Gunzburg Center for European Studies, Harvard University, 3.
[9] Frank J. Cillufo and Thomas Tomarchio, "Responding to new terrorist threats," *Orbis*, 42, No. 3 (1998): 440; Nikolas Rose, "The biology of culpability: pathological identity and crime control in a biological culture," *Theoretical Criminology*, 4, No. 1 (2000): 24; Michael Corrado and Michael Davis, "Special section on punishment, quarantine, and preventive detention," *Criminal Justice Ethics*, 15, No.2 (1986): 12.
[10] Office of Homeland Security, *National Strategy for Homeland Security* (Washington, DC: Government Printing Office, 2002), 16.
[11] U.S. Government, *National Strategy for Combating Terrorism* (February 2003), 28.
[12] Ibid
[13] Office of Homeland Security, *National Strategy for Homeland Security*, ix.
[14] Paul K. Davis and Brian Michael Jenkins, *Deterrence & Influence in Counterterrorism* (Santa Monica, CA: RAND, 2002), xiii. Davis and Jenkins write: "Finally, to sustain its [terrorism deterrence] effort for the long term, the United States needs to have and disseminate a persuasive, high-minded strategy, analogous to the Cold War strategy that served the nation so well."
[15] Anne L. Schneider, "Coproduction of Public and Private Safety: An Analysis of Bystander Intervention, 'Protective Neighboring,' and Personal Protection," *The Western Political Quarterly*, 40, No. 4 (December 1987): 617.
[16] Clark, "Sea Power 21." Clark writes: "The importance of Sea Shield to our nation has never been greater, as the proliferation of advanced weapons and asymmetric attack techniques places an increasing premium on the value of deterrence and battlespace dominance."
[17] U.S. Department of Defense. "Navy Announces Results of its Investigation on USS Cole." News Release No. 031-01, January 19, 2001. The release attributes the quote to Chief of Naval Operations, Adm. Clark.
[18] Ibid.
[19] Vernon Clark. "Sea Power 21."
[20] Ibid. Mahan, too, equated naval supremacy with the ability to develop surge capacity: "More important even than the size of the navy is the question of its institutions, favoring a healthful spirit and activity, and providing for rapid development in time of war…"
[21] Clark, "Building a 21st-Century Navy." In 2004, the Navy conducted Summer Pulse '04, an exercise which used seven carrier task forces to successfully test the Sea Basing concept.
[22] Associated Press, "Pentagon seeks new home for warship," www.CNN.com, June 8, 2005.
[23] U.S. Navy, "USS Gonzalez Wards Off Attack on Civilian Mariners in Indian Ocean," USS Gonzalez Public Affairs, Story Number NNS050608-02, June 8, 2005.
[24] U.S. Navy, "Maritime Security Operations: A Critical Component for Security and Stability," U.S. Fifth Fleet Public Affairs, Story Number NNS050608-04, June 8, 2005.
[25] U.S. Navy, "Keel Laid for First Littoral Combat Ship, USS Freedom," Naval Sea Systems Command Public Affairs, Story Number: NNS050603-18, June 3, 2005. According to a US Navy press release, the vessel's new name was chosen to acknowledge, "…the enduring foundation of the nation and honor[s] American communities from coast to coast which bear the name Freedom."
[26] Clark, "Building a 21st-Century Navy."
[27] An illustration of the DD(X) prototype can be found at the US Navy webpage: http://peoships.crane.navy.mil/ddx/ In the DD(X)'s design it is interesting to note the return of the "ram bow," a feature of most major warships following the 1866 Battle of Lissa between the Austrians and the Italians, and in which several ships were sunk by ramming. The concept of using the entire ship as a weapon consequently became a tactical grail until well after WWI. In the case of the DD(X), studies have shown that vessels with longer waterlines have lower friction coefficients and can therefore operate at faster speeds.
[28] Robert D. Kaplan, "How We Would Fight China," *The Atlantic Monthly*, June 2005, 49.
[29] Clark, "Building a 21st-Century Navy." ,
[30] David Longshore, "The Principles of Prevention and the Development of the Prevention Triangle Model for the Evaluation of Terrorism Prevention," (master's thesis, Naval Postgraduate School, March 2005).

[31] U.S. Navy, "Maritime Security Operations: A Critical Component for Security and Stability," U.S. Fifth Fleet Public Affairs, Story Number NNS050608-04, June 8, 2005.
[32] Kaplan, "How We Would Fight China," Kaplan assessment is grim but realistic: "No matter how successfully our military adapts to the rise of China, it is clear that our current dominance in the Pacific will not last."
[33] Richard Halloran, "China Rapidly Expands Military Capability," *Honolulu Advertiser*, February 6, 2005. Halloran writes: "China, which has become the world's third largest shipbuilder, has produced about 100 amphibious ships, and four tank landing ships are under construction. That appears to have obliterated a U.S. Navy joke that, because the Chinese lacked amphibious ships, the only way they could invade Taiwan was by swimming." See also, Edward Cody, "With Taiwan In Mind, China Focuses Military Expansion on Navy," *Washington Post*, March 20, 2004.
[34] www.Stratfor.com, "Taiwan Shifting Defense Priorities Toward Navy," August 19, 2002.
[35] A copy of the CNO's *Guidance for 2005* can be found at www.chinfo.navy.mil/navpalib/cno/clark-guidance2005.pdf.

Homeland Security Affairs

Volume I, *Issue* 1 2005 *Article* 7

Summer 2005

Measuring Prevention

Glen Woodbury*

*Naval Postgraduate School, Center for Homeland Defense and Security, glwoodbu@nps.edu

Measuring Prevention

Glen Woodbury

Abstract

How do we know if prevention is working? Not only is the measurement of prevention activities possible, the methodologies of "how" to measure already exist in numerous processes. Additionally, the definitions of "what" to measure have been both experienced and discussed. This article argues that measuring prevention can be accomplished by examining and evaluating the pieces that make up the whole and demonstrates that not only is prevention measurable, that measurement is well within our reach. Measuring effectiveness is not always done at the level of final outcomes. Often, the processes and systems (or outputs) that lead to preferred outcomes are measured when ultimate outcome measurement is impossible. To increase our understanding of how to combat terrorism, we need to put the argument of immeasurable prevention behind us and accept that prevention can be quantified, at least by evaluating the parts of the whole.

AUTHOR BIOGRAPHY: Glen Woodbury is a faculty member and Associate Director of Executive Education Programs for the Naval Postgraduate School's Center for Homeland Defense and Security. His responsibilities include the development of executive education workshops, seminars and training for senior state and local officials. He served as the Director of the Emergency Management Division for the State of Washington from 1998 through 2004 and is a Past President of the National Emergency Management Association. Mr. Woodbury holds a Bachelor of Arts Degree in Engineering Sciences from Lafayette College in Easton, PA (1985) and a Masters of Arts Degree in Security Studies (Homeland Defense and Security) from the Naval Postgraduate School in Monterey, CA (2004).

KEYWORDS: prevention, measurement, effectiveness, combatting terrorism

INTRODUCTION

How do we know if prevention is working? How do we know if all the efforts and resources directed towards stopping the next attack are worthwhile? How do we measure a negative? How do we continue to justify the diversion of public funds from other essential services if our only justification for success will be "nothing happened?" If we could count how many attacks were stopped or deterred, measuring prevention would obviously be a simple task and this article would be superfluous. Unfortunately, inherent in an ability to count what the enemy has decided *not* to do requires an ability to read the minds of our foes or, at the very least, an ability to constantly observe their internal decision cycles. Even if the absence of an attack were not the result of a conscious decision by the terrorist, but rather the result of some unfortunate (from their point of view) circumstance, our ability to quantify the elimination of the threat would require a much deeper intelligence capability than we are able to construct. If we could peer so deeply into the opposition that we could count each of their failures, this same capability would also make the entire homeland security enterprise moot.

The ability to measure the prevention of terrorist attacks is vitally important for a number of reasons. First, there is the accountability issue. The nation, at all levels of government and the private sector, is investing vast amounts of funds and efforts to "prevent the next attack." Not only that, we have reorganized significant portions of the federal government (and some states as well) to protect our citizens, economy, infrastructure and way of life from another horrendous attack upon the homeland. How do we know we are succeeding? What type of examination tells us we have been wise in our investments, or have we been lucky in spite of them? Secondly, we need to effectively guide, and justify, future investments. Without a rational argument and measurement process to explain the benefits of expenditures on prevention activities, we are not only apt to suffer deserved criticism; we also risk sacrificing future investments, political credibility and the public's faith. Third, and most importantly, how can we claim to be effectively protecting the safety and security of the nation without any way of determining whether our path and efforts are, at the least, mostly correct and rational?

This is critical. In the absence of more attacks (and this is a good thing), we are in effect asking the public and appropriators to "trust us" on our near and long term efforts to prevent terrorist attacks. How long will this trust last? Is it already waning? How long can we justify expenditures on this particular public good versus all the others? On the other hand, should another attack occur we will once again dissect every effort we made to prevent it. How will our response to the investigation be viewed if our efforts are based upon unmeasured, unguided and illogically resourced actions to prevent the tragedy in the first place?

Now the good news: not only is the measurement of prevention activities possible, the methodologies of "how" to measure already exist in numerous processes. Additionally, the definitions of "what" to measure have been both experienced and discussed. This article will argue that measuring prevention *can* be accomplished by examining and evaluating the pieces that make up the whole and demonstrate that not only is prevention measurable, that measurement is well within our reach. I will support this argument by discussing and justifying the concept behind process measurement; by briefly examining some current thoughts of what might comprise prevention; and then by proposing and testing one methodological possibility.

PROCESS MEASUREMENT

We are not at the place where we can declare a victory of intelligence. Nor should we be so shortsighted that we are willing to continue a massive investment in preventive action without a means to measure whether it is at all effective. But, to argue against the counting negatives parable, measuring effectiveness is not always done at the level of final outcomes. Often, the processes and systems that *lead* to preferred outcomes are measured when *ultimate* outcome measurement is impossible. Emergency management agencies are not (usually) measured by how many houses are or are not flooded in a storm event; rather, the systems and programs that help prevent flooding are measured against accepted standards of practice[1]. Fire agencies are not generally measured by how many houses are saved or burn; their response times are measured to quantify and compare increased/decreased efficiency versus the inputs they invest. We may not know "how many shipwrecks does a lighthouse prevent?"[2] but we can evaluate the design and decision processes that lead to the specific placement of lighthouses and come to some conclusion as to the soundness of these decisions without knowing whether ships did or did not crash because of them.

Why can't prevention efforts, especially at the state and local levels, be evaluated in a similar fashion? We can set in place sound and reasoned prevention practices and standards that we can confidently conclude will lead to the prevention of terrorist attacks. These practices and/or approaches can then be measured in pieces or comprehensively to give some sense of a program's effectiveness. For example, if it is accepted that a critical piece of the prevention process is the establishment of a collaborative system that enables and promotes the integration and analysis of data from all sources (from both inside and outside the law enforcement community) – which in turn better guides protection measure decisions – then the existence or nonexistence of this system is a measurement. If it does not exist, one could reasonably postulate that prevention is weaker. If we took all the pieces of one simplified prevention process (threat identification, target evaluation, risk assessment, or response/protection decisions) and detailed the sub-components of the process, we could ideally come up with a systematic approach in which many of the individual pieces of the overall process could be measured. If all, or most, of the pieces are effective, then the whole might be effective. This of course assumes that whatever model process we propose actually portrays a sound and reasoned approach that, when employed, leads to better prevention.

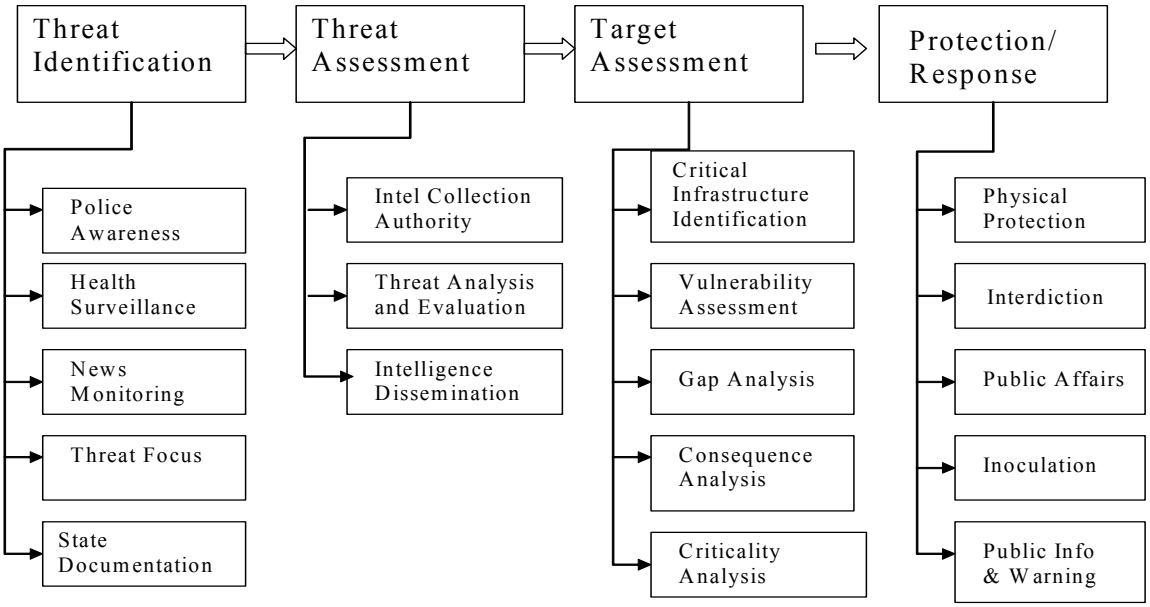
The Department of Homeland Security's Office for Domestic Preparedness proposes a prevention process model in their *Prevention Guidelines for Homeland Security*[3] that could be used to describe both the process to be assessed as well as up to 165 individual tasks and/or outputs. The *National Preparedness Guidance*[4] takes the guidelines' model further and identifies a list of target capabilities that are desired for the entire spectrum of the homeland security effort from prevention to recovery, as well as some common cross-cutting capabilities required in all mission areas.

Specifically, this guidance identifies the prevention and protection target capabilities, or "things we should be able to do well,[5]" as follows:

Prevention Mission Area: Information Collection and Threat Detection, Intelligence Fusion and Analysis, Information Sharing and Collaboration, Terrorism Investigation and Apprehension, and CBRNE Detection;

Protection Mission Area: Risk Analysis, Critical Infrastructure Protection, Food/Agriculture Safety and Defense, Public Health Epidemiological Investigation and Testing, and Citizen Preparedness and Participation.

For discussion purposes, all the processes and elements mentioned above might be incorporated and might be visualized as follows[6]:



There are arguably (and it *will* be argued) many ways to portray all the possible prevention components and tasks in a succinct and simple diagram. The point here is not so much how the final, best model process could best be visually depicted; it is how such a reasonably sound process could be measured by component, task, and/or output.

DEFINING THE PIECES OF THE PROCESS: OUTCOMES TO OUTPUTS

What are outcomes? Harry P. Hatry defines them, as "events, occurrences or changes in conditions, behavior, or attitudes that indicate progress toward achievement of the mission and objectives of the program. Thus outcomes are linked to the program's (and its agency's) overall mission – *its reason for existing,* [emphasis added]."[7] When considering the establishment of any organized structure for prevention, the immediate step after determining its mission or objective should be the establishment of measurable outcomes that will help focus efforts to advance that mission. The General Accounting Office in April of 2002 testified to the Senate Committee on Government Affairs that two key ingredients were missing from then current strategic efforts towards combating terrorism: the lack of measurable outcomes and the lack of the identification of appropriate roles for state and local governments.[8] This testimony occurred prior to the publication of the *National Strategy for Homeland Security* in June 2002 and its impact

on the authors of the strategy is unknown. Can measurable and achievable prevention outcomes be developed?

From the example process above, it is possible to rephrase the four major elements into four measurable desired outcomes or goals for an organizational effort to prevent terrorist attacks: 1) the increased ability to identify indications of an existing or future threat; 2) the increased ability to evaluate the potential of threats as they are identified; 3) the reduced vulnerability of critical infrastructures and other potential targets; and 4) the increased appropriateness of protection and/or other threat response activities.

Together, these four outcomes describe elements of a risk assessment process that could ultimately provide policy makers and executive decision authorities an objective cost-benefit analysis that will help guide their final actions in response to identified terrorist threats.

Taking it one step further, outputs could also be proposed for measuring each of the desired outcomes. Clearly the list of outputs for the prevention of terrorism could draw from hundreds of potential courses of action. But some of the "highest order" outputs could provide a starting point for organized actions. At this level of detail, it is important to note that what might comprise prevention on an international, foreign policy scale is unlikely to be the same as that for state and local governments or the private sector. For the four prevention outcomes identified above, I propose thirteen individual outputs that might be applied in a domestic stetting:

Outputs for Outcome One, the increased ability to identify indications of an existing or future threat: 1) development of a strategy and commensurate business plans that describe how to assure the collaboration and coordination amongst all entities that participate in the threat identification processes; 2) creation and implementation of a system to collect, screen and store relevant information with investigative value[9]; and 3) development of a training system that provides adequate basic level threat awareness education to all public service entities, the private sector, and the general public as appropriate.

Outputs for Outcome Two, the increased ability to evaluate the potential of threats as they are identified: 1) adoption or development of an appropriate analytical model to assess threat indications; 2) ensured collaboration and integration of assessment and evaluation processes from traditional as well as non-traditional investigative entities, (e.g. health and agricultural agencies); 3) creation and/or assignment of a lead organization to oversee and coordinate a system of threat identification and assessment processes; and 4) through policy, legislative and/or executive action, the identification and development of strategies to overcome barriers to the appropriate sharing of information and intelligence products.

Outputs for Outcome Three, reduced vulnerability of critical infrastructures and other potential targets: 1) assignment or creation of a lead entity to oversee the effort to identify, assess vulnerabilities of, analyze consequences, and recommend protective strategies and priorities of critical infrastructures and potential targets of terrorists; 2) development and oversight of strategies and action plans that maximize the collaboration and coordination of the owners of potential targets and the entity's effort to reduce their vulnerabilities; and 3) provision of a leadership point to assure the coordination between private, local, state, and federal critical infrastructure protection efforts.

Outputs for Outcome Four, increased appropriateness of protection and/or other threat response activities: 1) establishment and oversight of a process that ensures the interconnection of the first three outcomes and results in recommendations for protection decisions and threat response measures; 2) development of a risk management or cost benefit tool that will guide appropriate protection and response action decisions; and 3) development of a methodology that delineates responsibilities for varying degrees of decision-making amongst and between levels of government and the private sector.

These outputs and objectives could be modified, added to, or otherwise changed to better reflect the needs and expectations of individual government or private sector entities. The important and critical assumption is that *should* all of these elements be implemented effectively, it *will* help lead to the prevention of terrorist attacks, and therefore the evaluation of these outputs will provide a viable measurement tool. The emphasis again is measuring a logical and reasonable process that would, by its implementation, lead to better prevention. This approach does not attempt to measure prevention through the accounting of non-attacks which, as stated earlier, is either impossible or at least not quantifiably consistent. One way to analyze the validity of the proposed outcomes and outputs is to ask the negative of each of the elements. In other words, if these four outcomes and thirteen outputs were not in place, could we reasonably assume that the likelihood of a successful terrorist attack is greater? Without these elements in place, the leaders of an organizational effort to prevent terrorism would have no systems or processes by which to identify the threats, to analyze and evaluate probabilities, to prioritize potential targets for protection or to make good risk management decisions about what actions to take in a threat environment. If this were the case, I would measure this particular entity's overall ability to prevent a terrorist attack as extremely low. They would have to instead rely upon luck, or on the decision of the enemy not to attack them for some other rationale unknown to the defending organization.

A MEASUREMENT EXAMPLE

There are numerous applications and methodologies for converting desired outcomes and outputs to measurement language. Examples of measurement methodologies include everything from an exhaustive process involving the assignment of values or weights to each element and its detailed tasks, to a simpler exercise in which one might use stop light colors for each element; (e.g. "red" means no effort or system in place to achieve the output or outcome, "yellow" indicates some efforts are underway or partially completed, and "green" designates completion or sustained efforts in effect). Finding the "how" to measure is the easy part. There are any number of models to use and hundreds of expert consultants, contractors and academics ready to engage in methods for measurement. Defining the "what" to measure is where we are challenged.

For a brief illustrative example that applies one method for "how" to measure the "what" I am proposing, I have used outcome number Two: Increased ability to evaluate the potential of threats as they are identified**.** Applying a simple numerical weighting system to the outputs, each has been graded according to the following scale and criteria.

0 = No effort or system underway nor recognition of the need

1 = Recognition of the need but no effort or resources to accomplish the output

2 = Initial efforts and resources underway to achieve the output

3 = Moderate progress towards accomplishing the output

4 = Sustained efforts underway and output near to fulfillment

5 = Output achieved and resources devoted to sustain the effort

For this example, I have assigned a numerical assessment to each of the outputs and provided a fictional, but plausible, narrative of that evaluation.

Measurement of Outcome Two
(Increased ability to evaluate the potential of threats as they are identified)

Measurement of 2-1

Adoption or development of an appropriate analytical model to assess threat indications.

Score = 2

Through the intended, financed and planned, yet to be implemented, establishment of a state fusion center, it is expected that an analytical model will be utilized based upon national best practices or customized design.

Measurement of 2-2

Ensured collaboration and integration of assessment and evaluation processes from traditional as well as non-traditional investigative entities, (e.g. health and agricultural agencies.)

Score = 2.5

While the formal fusion center and system is yet to be established, all law enforcement agencies and non-law enforcement entities have recognized the requirement to participate in the sharing and dissemination of information and intelligence. Staff have been identified and protocols have been established to transfer threat and vulnerability related data and to participate in evaluation of such data in a collaborative fashion.

Measurement of 2-3

Creation and/or assignment of a lead organization to oversee and coordinate a system of threat identification and assessment processes.

Score = 4

The state patrol's intelligence division has been assigned lead responsibility for the achievement of this objective. It has been resourced by both state and federal funds and its efforts are monitored and accountable to the Governor, the state patrol chief and the homeland security director. Long term strategic planning and budgeting efforts have been completed and approved, in concept, by the state legislature.

Measurement of 2-4

Through policy, legislative and/or executive action, identification and development of strategies to overcome barriers to the appropriate sharing of information and intelligence products.

Score = 2.5

While much discussion and some action has overcome and/or satisfied some privacy act and civil liberty issues, much work remains to be done; specifically, in the issue area of the sharing and protection of data shared between the public and private sectors.

Out of a possible "score" of 20 for objective Two, this fictional entity measures 11 (the total of the four scored outputs). So one might say that this entity's "increased ability to evaluate threats as they are identified" is not yet realized but is progressing. Therefore, in combination with the other three prevention objectives, the executives could reasonably assess their overall prevention efforts, at least at a strategic level. While as much subjectivity as possible can be taken out of this process through firmer scoring criteria, the question of whether this objective or its outputs are important to overall prevention will most likely be a subjective decision by the senior officials responsible. But this simple evaluation can at least paint a picture of the level of progress in this element from which further resource, executive guidance, or prioritization can be accomplished. The score may be acceptable at this point in time and the executive directive is to continue as planned. Or the assessment may be judged to be woefully inadequate and the timeframe for the establishment of a fusion center is accelerated.

As stated before, there are many variations and available tools to measure objectives and outputs. Additionally, what is deemed important to be measured could deviate or adjust from the proposed tool presented here and the outputs could be expanded and examined at a greater level of detail. The key question again is if, by measuring the pieces of a logical approach that can be reasonably expected to lead to better prevention, can overall prevention itself be measured and evaluated? If (as this article suggests) the answer is yes, then not only can investments and efforts be more logically and justifiably applied, the public good is better served by measured and guided efforts that actually lead to the intended result.

CONCLUSION

As proposed in the introduction, this concept of measurement by process effectiveness is not ground-breaking. The public health community proposed this approach for their evaluation of efforts to combat bio-terrorism and other catastrophic threats[10]. Their effort was comprised of two major objectives. One, to measure the ability of the public health community to respond to all events – not just bio-terrorism – by measuring its preparedness for other threats such as West Nile Virus, SARS and an influenza season; and two, to measure such preparedness by evaluating the pieces (e.g. an epidemiological surveillance capacity,) of the overall processes which, when working in concert, are designed to achieve an effective prevention and response capability.

There are also other potentials for measurement, not discussed in this article, involving the measurement of other consequences of those systems primarily designed for counter-terrorism. For example, if the systems and actions to better share law enforcement threat data to identify potential terrorists also serve to increase the ability to identify and capture non-terrorist criminals, then the increase/decrease of common criminals identified could indicate measurement of the overall system as well. While the examples presented above are over-simplified, they demonstrate the enormous potential and opportunities to measure prevention without having to rely on "what did *not* happen."

This article is written in the middle of the year 2005, a time when the congress, state and local governments, and their executing agencies are all focusing on the homeland security funding questions of "how much?" and "how will we know when it is enough?" For some mission areas, measurement will be easy. Consequently, the policy debates over what capability gaps to "buy," will be less esoteric. The gap between not enough communications gear and almost enough will be much simpler to quantify than the one between the unknown amount of prevention we possess and the near to perfect results we demand, but cannot define. But if we do nothing else, we need to put the argument of un-measurable prevention behind us and accept that it *can* be quantified, at least by proxy and/or by evaluating the parts of the whole. Oddly, considering the purpose of this article, the near-term challenge we face is not the establishment and acceptance of a system that depicts prevention in measurable outcomes and outputs. The real challenge will be to avoid the temptation to only resource those missions we already understand versus those of vastly more importance that we are just learning to build.

---

[1] For example, the emergency management community has established standards for a state and local emergency management system that can be evaluated through a program called the *Emergency Management Accreditation Program.* More information is available at www.emaponline.org. Additionally, some discipline-specific programmatic standards are proposed for disaster management through the *National Fire Protection Association (NFPA)* in their NFPA 1600 document: http://www.nfpa.org/assets/files/PDF/NFPA1600.pdf.

[2] While this metaphor is found in other references, e.g. death penalty arguments, I first heard it expressed in the context of terrorism prevention from Dr. William Pelfry during class instruction at the Center for Homeland Defense and Security, Naval Postgraduate School, Monterey, CA.

[3] Office for Domestic Preparedness, U.S. Department of Homeland Security, *Prevention Guidelines for Homeland Security. The Office for Domestic Preparedness Guidelines for Homeland Security June 2003: Prevention and Deterrence* (Washington D.C., June 2003).

[4] U.S. Department of Homeland Security; Office of State and Local Government Preparedness. *National Preparedness Guidance; Homeland Security Presidential Directive 8: National Preparedness.* Washington D.C., April 27, 2005.

[5] The *National Preparedness Guidance* uses the term "how prepared do we need to be?" which is just as useful a question in the process of setting the bar for desired capability. The Department of Homeland Security intends to define the desirable levels of capabilities for all the elements of the Target Capabilities List, including the ones listed here, in late 2005, which states will be required to review as part of their FY2006 grant applications.

[6] This diagram was drafted during a workshop of subject matter experts at the Naval Postgraduate School, Center for Homeland Defense and Security on January 28-29, 2004. The principle author is Bruce Lawlor, first Chief of Staff for the U.S. Department of Homeland Security. I modified it slightly from its original draft version.

[7] Harry P. Hatry, "What Type of Performance Information Should be Tracked?," in *Quicker, Better, Cheaper? Managing Performance in American Government*, ed. Dall W. Forsythe (New York: Rockefeller Institute Press, 2001), 21.
[8] David M. Walker, Comptroller of the United States. In testimony to the Committee on Government Affairs, U.S. Senate. *Homeland Security: Responsibility and Accountability in Achieving National Goals.* U.S. General Accounting Office. Expected release on April 22, 2002. http://www.gao.gov/new.items/d02627t.pdf, 7 [Accessed February 19, 2004].
[9] *Guidelines for Homeland Security June 2003: Prevention and Deterrence,* 19.
[10] Division of Public Health, Department of Human Resources, State of Georgia; and the Center for Public Health Preparedness and Research, Rollins School of Public Health, Emory University. *Indicators of Preparedness for Public Health Emergencies*, DRAFT, April 19, 2004. Copy provided by Dr. Kathleen Toomey, former Director of Public Health for the State of Georgia.