CHAPTER 8

Homeland Security: Strategic, Operational, and Tactical Partnerships

James Chambers

Translating the National Strategy

> *Homeland security is a concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur.*[1]
>
> —The National Strategy for Homeland Security

Since September 11, 2001, many local law enforcement professionals have become somewhat apprehensive about projecting a positive response to the threat of terrorism. Most are anxiously looking to the federal government for direction and the all-important funding of new units and other activities that may become necessary in the national defense effort.[2] In July 2002, the Office of Homeland Security published its *National Strategy for Homeland Security* whose purpose is to "mobilize and organize our Nation to secure the U.S. homeland from terrorist attacks."[3] As President Bush states in his introductory letter, "it is a national strategy, not a federal strategy."[4] Admittedly, "this is an exceedingly complex mission that requires coordinated and focused effort from our entire society—the federal government, state and local governments, the private sector, and the American people,"[5] but one that must be done and done well.

In this effort, the yeoman's share of the responsibility rests on the state and local governments' law enforcement professionals. State and local law enforcement agencies have been, and always will be, the first line of defense in the protection of life and property within their

community.[6] Because of this, it is imperative that leaders in state and local law enforcement operationalize the stated and implied tasks listed in the *National Strategy* and translate those into tactical doctrine and procedures (response plans) for the men and women who "man" the American Front. Once these tasks are identified and plans are developed or revised, leadership must also establish a list of requirements or resources needed to meet those challenges.

Requirements and resources needed to counter our threats will likely include more efficient systems/organizations at the federal and state levels and high cost communications and training programs at the state and local levels, i.e., information sharing, communication interoperability, and first responder training. Seventy-seven percent of the 13,500 law enforcement agencies serving U.S. states, counties, cities, and towns have 24 or fewer sworn officers.[7] For these jurisdictions to successfully meet the challenges they are likely to face in the near- and long-term, they will require financial augmentation from the federal government.

Stated and Implied Tasks at the Operational Level

Operational level tasks link strategy and tactics. The *National Strategy's* objectives are clearly stated tasks, while others may not be stated but implied. In other words, they are implied because they are necessary to do in order to achieve the desired goal. The stated and implied tasks I have gleaned from the *National Strategy*, ones for which I believe law enforcement leaders can organize, train, and equip at the operational and tactical levels are: **Prevent, Respond to,** and **Recover from** terrorist attacks. Each of these tasks carry their own set of implied tasks. One implied task of "prevent" is the existence of an effective intelligence system. An implied task of "respond to" could be the existence of a communications system capable of interoperability with numerous jurisdictions and other emergency services. An implied task of "recover from" could well be the existence of a facility and infrastructure capable of sustaining an Emergency Operations Center (as well as a trained and available staff) for 24-hour operations for 14 days.

From these stated and implied tasks, a response plan can be developed or revised. Many agencies already have plans in place for various contingencies. Some natural disasters or large sporting event plans can easily be modified for response to a mass casualty situation. For

those jurisdictions that are without response plans, they must extract the stated and implied tasks applicable to their area's vulnerabilities and operational/incident management capabilities and create them. From this public safety plan, shortfalls in capabilities and resources can be identified and prioritized. Through the established financial grant process or through future funding programs, federal or state funding should be requested to eliminate vulnerabilities. In some areas, coalition law enforcement/emergency services will likely best serve the public, both operationally and fiscally, especially in the 77 percent of the 13,500 jurisdictions mentioned above.

Actions since 9/11

Since September 11, 2001, there have been many positive changes at all levels of government. President Bush signed into law an act creating the Department of Homeland Security—the largest governmental reorganization since 1947. The Department of Homeland Security Reorganization Plan transferred agencies from standing departments and reassigned them to the Department of Homeland Security; U.S. Customs, Border Patrol, and the Coast Guard to name a few. In January 2003, former Pennsylvania Governor Tom Ridge was confirmed as the first Secretary of Homeland Security.

Agencies within other Departments also made significant internal changes in an attempt to better meet their responsibilities. FBI Director, Robert S. Mueller III, outlined several changes in January 2003's *Police Chief* magazine. Some of those he mentioned include: the creation of the Office of Law Enforcement Coordination; the initiation of a pilot program in Saint Louis, Missouri, called the Joint Terrorism Task Force (JTTF) Information Sharing Initiative; and a new FBI Intelligence Bulletin sent to more than 17,000 law enforcement agencies weekly. The FBI's creation of joint terrorism task forces has proven to be an effective method of addressing the terrorism threat, while providing a means for the pooling of resources and the sharing of information with state and local agencies.[8] Director Mueller stated:

> Twenty-one new Joint Terrorism Task Forces (JTTF) have been started since September 11, 2001, bringing the total to 56. We have stood up a new national JTTF at FBI

> headquarters to complement the work of local task forces. It includes two local police officers as well as representatives from two-dozen federal agencies.[9]

However, the terrorists are capable of moving faster than our bureaucracy. Faster and more frequent changes are needed to prevent future successful attacks. If, in the immediate shadow of the terrorist attacks, the process by which we nominated and confirmed Secretary Ridge took almost a year and a half, how long will other "bold and necessary steps"[10] take as the memory of September 11th fades into history? As a Nation, we have a tendency to focus on the here and now, seldom studying the past and even more rarely planning for the future. Our political system, as a whole, reflects society in this manner.

Use the armed forces antiterrorism funding as a case in point. The ebb and flow of funding has been determined by crisis. After tragedies like Khobar Towers and the U.S.S. *Cole* attacks, money designated for antiterrorism programs flowed in great significance. Once spent and Congressional interest was focused elsewhere, the Department of Defense (DOD) relied on the amount appropriated in the annual budget—typically only a fraction of the money appropriated after a crisis.

Great changes usually begin with great catalysts. I submit the creation of Department of Homeland Security, albeit a wise strategic move, would have never been possible without an attack on our Nation's home front. Knowing how our political system operates, law enforcement/emergency services must continue to lobby for the systems and infrastructure that will achieve Department of Homeland Security's premier strategic objective—to prevent terrorist attacks within the United States—even if we only get an 80 percent solution.

Partnerships for Prevention

> *Every terrorist event, every act of planning and preparation for that event (if conducted inside the United States) occurs in some local law enforcement agency's jurisdiction. No agency is closer to the activities within its community than the law enforcement agency that has the*

> *responsibility and jurisdiction for protecting that community.*[11]
>
> —D. Douglas Bodrero, Senior Executive and Manager,
> State and Local Anti-Terrorism Training,
> Institute for Intergovernmental Research

Each community leader who undertakes the Herculean task of preventing, responding to, and recovering from terrorist attacks in their community knows "the most important focus is on prevention" and for him/her to be successful, it "requires strengthening, to the best of our abilities, our intelligence gathering systems."[12] A report from the National Commission on Terrorism stated in June 2000:

> Good intelligence is the best weapon against international terrorism. Obtaining information about the identity, goals, plans, and vulnerabilities of terrorists is extremely difficult. Yet, no other single policy effort is more important for preventing, preempting, and responding to attacks.[13]

Prevention, in this context, can be broken down further to include interdiction and mitigation. Interdiction, the most desirable form of prevention, is the complete stoppage of a planned terrorist attack at a point between the planning and execution phases. Whether interdiction occurs by employing an unmanned combat aerial vehicle such as the RQ-1 "Predator" against Al Qaeda operatives in Yemen; or by a Cullman County, Alabama, deputy sheriff's patrol conducting a routine traffic stop and finding a trunk load of explosives destined for a terrorist operation, the key is to make interdiction *intentional.* We must have a criminal intelligence system that will provide that capability.

If we fail to interdict terrorist acts, we must succeed in mitigating their effects. Though heavily reliant on a formal intelligence system, mitigation is also reliant on vulnerability assessments conducted by local governments. Something as simple as a well-placed set of concrete barriers at a hospital access point or an intrusion detection system with sensors and cameras at a chemical plant can mitigate a potentially catastrophic attack. Knowing vulnerabilities and the consequences of an attack will also allow plans to be crafted and spending to be prioritized showing the federal or state governments that funding your projects would

be the best use of the taxpayers' money. *Intentional* interdiction and mitigation requires a formal national intelligence system.

Intelligence System Requirements

In December 2001, then International Association of Chiefs of Police (IACP) President Bill Berger testified before the Senate Governmental Affairs Committee on the role of local law enforcement in homeland security. Berger stressed that state and local law enforcement agencies are crucial to success in the war on terrorism.[14] He further stated that there are 700,000 officers who patrol the streets daily with intimate knowledge of their community and implying they all have a part in gathering and using intelligence information to prevent terror in our country. What intelligence gathering agency would turn down the opportunity to have 700,000 intelligence gathering agents? In January 2003, FBI Director Mueller praised the success of local police involvement in gathering intelligence information. "Local officers have passed along tips and reports of suspicious behavior that have ultimately turned up terrorist activities. Recent months have made it clear that defeating terrorists requires a full partnership: local, state, federal, and international law enforcement working hand in hand like never before."[15]

In early 2003, even with all the landmark reorganizations and institutional changes, we have not created a national intelligence system that meets the requirements established by the IACP in the below paragraph:

> Berger stressed that in order to make use of this intelligence-gathering capability, federal, state, and local law enforcement agencies must develop an efficient and comprehensive system for the timely sharing, analysis, and dissemination of important intelligence information. The IACP believes that failure to develop such a system, and to provide guidance to law enforcement agencies in how intelligence data can be gathered, analyzed, shared, and utilized is a threat to public safety and must be addressed.[16]

Joint Regional Information Center

In June 2002, "IACP identified several barriers that currently hinder effective exchange of information between federal, state, and local law enforcement agencies:

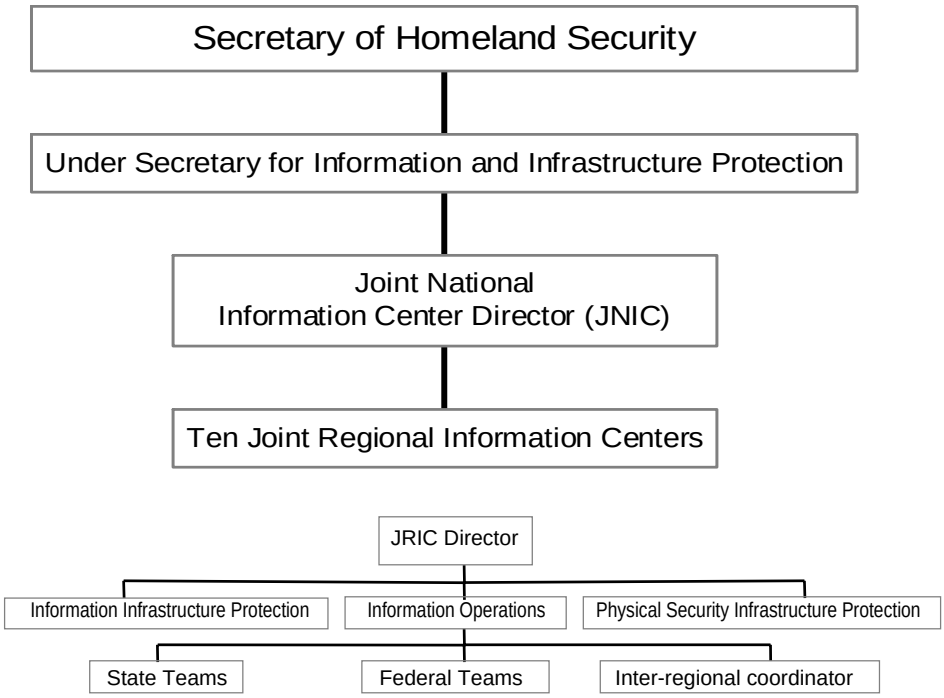
- The absence of a nationally coordinated process for intelligence generation and sharing.
- The structure of the law enforcement and intelligence communities.
- Federal, state, local, and tribal law and policies that prevent intelligence sharing.
- The inaccessibility and/or incompatibility of technologies to support intelligence sharing."[17]

Regardless of the steps that have been taken, some of these barriers still stand in the way of maximum information sharing. To alleviate these, I propose the following organization.

Organization

Create a Joint National Information Center (JNIC) under Department of Homeland Security's Undersecretary for Information Analysis and Infrastructure Protection (see Figure 8.1). Likely housed in Washington, D.C., the JNIC would oversee the backbone of the formalized information system, the Joint Regional Information Centers (JRIC). JRIC's organization would conceptually resemble the organization of the Department of Defense's unified command. A unified command is a command with a broad continuing mission under a single commander and composed of significant assigned components of two or more Military Departments.[18] Most unified commands are responsible for a specific region in the world—United States European Command for instance. JRICs would employ representatives from several federal agencies and be responsible for a specific region of our nation.

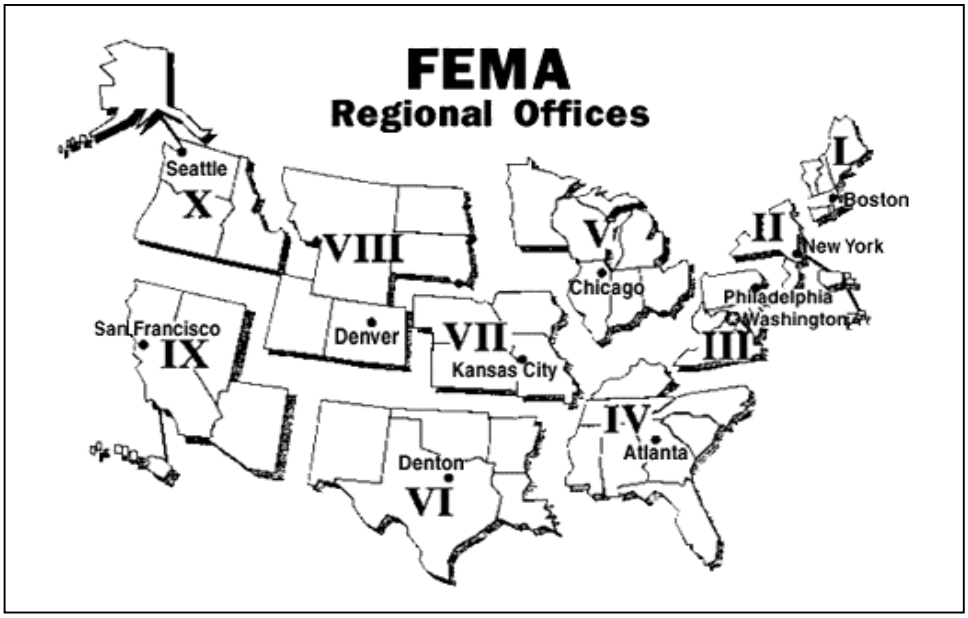
Figure 8.1 Proposed Joint National Information Center Construct



Source: JNIC and JRIC Concepts Proposed by Author

Department of Homeland Security, in creating this information system, should divide its area of operations into regions to make the volumes of information more manageable. Decreasing the input quantity would increase the output quality. The ten regions that the Federal Emergency Management Agency (FEMA) has established works well for my example and would likely work well operationally. *[Editor's note: As the Department of Homeland Security (DHS) incorporates FEMA into its Emergency Preparedness and Response Directorate, FEMA will become synonymous with DHS.]*

Figure 8.2 FEMA Regional Offices



Source: Federal Emergency Management Agency home page, on-line, Internet, available from http://www.fema.gov/regions/.[19]

Each JRIC would be organized to respond to local (city, county, state), national, and international intelligence gathering, analyzing, and dissemination needs. Local needs would be the responsibility of the **state teams** (Figure 8.1). A state team would exist for each state within the region and would consist of trained analysts dedicated to collecting and disseminating information to and from that state as well as other applicable state teams, federal agencies, and the inter-regional coordinator. In Figure 8.2, using Region IV as an example, there would be eight state teams. The size of each state team would vary depending on the workload, i.e., Florida *may* generate more information than Tennessee.

To address the national needs and international connections, other federal agencies such as the Departments of Justice, Energy, Defense, Interior, and the Central Intelligence Agency, to name a few, would assign employees to the JRICs. Workload would also determine which Department's personnel would have to be permanently assigned to the

JRIC or whether it could function like an emergency operations center where members are on call. The raison d'être of the JRIC would demand a permanent assignment of state teams and certain Department of Justice workers.

Operations

The scope of the JRIC should not be limited to terrorism activities only, but should include all criminal activity that may cross state, regional, or international borders. Why? Terrorism is, for the most part, an international organized crime similar in structure to a South American drug cartel or the Russian Mafia. Like all international crime organizations, international terrorism is dependent on what the military call lines of communications (LOC). A LOC is "a route, either land, water, and/or air that connects an operating military force with a base of operations and along which supplies and military forces move."[20] Criminal organizations that "trade" internationally often depend on the same LOCs, i.e., arms and explosive dealers, money launderers, human smugglers, etc. Evidence suggests Middle Eastern terror organizations have already contacted South American cartels.[21] The JRIC's resources should be used to exploit the similarities of international criminals. The cross flow of information would be significant as would the benefits reaped if timely information was disseminated to the proper agencies.

The information sharing cycle is a multidirectional process that could begin at any level and at any agency. As previously mentioned, there are 700,000 police officers employed by local agencies, all of which are experienced in gathering intelligence. Due to the nature of their work, these officers are experts at human intelligence (HUMINT). When a beat officer "works a snitch" for information and builds that informant as a reliable source, that is the purest form of HUMINT. Typically, this information is sent through the existing state system to the agencies currently responsible for intelligence gathering, analysis, and dissemination. In the proposed construct, state agencies would forward the information to their respective state teams in the JRIC. Sending this information forward would not preclude their own analysis and dissemination to local departments. Most states likely have a system in place that would be complemented by the JRIC system. For example, the following is a mission statement from the New Jersey State Police's

Intelligence Bureau. "The mission of the Intelligence Bureau is to diminish and control the capacity of criminal organizations to influence New Jersey's society, economy, and government."[22] This mission statement fits in well with the intent of the JNIC/JRIC concept, including breaking the LOCs of organized crime. Some states may have to modify their current organizations and information flow to meet the JRIC guidelines, but the payback will be well worth it.

Devil's advocates may groan that the federal government has just added another layer to the information/intelligence bureaucracy. They may also argue it would be quicker to just send the information to the affected state. With today's technology, the additional layer should not prevent State A from sending State B information at the same time State A sends it to the JRIC. JRIC would need this information in the regional system because State A may not realize that State G in another region may have corroborating information or even a better defined threat. The inter-regional coordinator's job in the JRIC is to make sure the information flow is completely seamless between all regions.

The success of this type of network was recently seen in the Washington, D.C. sniper case. Information sharing between more than a dozen jurisdictions in 6 states and 1,600 law enforcement officers, aided by the FBI's immense computer database helped solve this shooting spree. There is no doubt in my mind that this partnership was a key factor in getting the snipers off the streets and saving lives.[23] Unfortunately, we solved this crime in the respond mode, not the prevent mode. We cannot afford to be in the respond mode for a weapon of mass destruction (WMD) incident. A formalized system similar to the JRIC would increase our probability of interdiction.

Benefits

There are resounding strategic, operational, and tactical benefits to a consolidated information-sharing system. Currently, there are numerous organizations producing a substantial amount of information. The Regional Information Sharing System (RISS) program is an intelligence-sharing network with a goal of assisting state and local criminal justice agencies.[24] RISS is funded by the U.S. Department of Justice, Bureau of Justice Assistance.[25] The El Paso Intelligence Center (EPIC) is another example of an information-sharing program. EPIC is staffed by 15 federal

agencies. Others, such as the Law Enforcement Intelligence Unit, the state operated Law Enforcement Intelligence Networks, and the High-Intensity Drug Trafficking Area Investigative Support Center also exist and offer information to an already overworked investigator at your medium sized police department.

Consolidating the federally funded agencies gives local agencies a one-stop information shopping capability. With the right focus, trained intelligence analysts at a single JRIC-type center would decrease the quantity and increase the quality of information that flows to the officer on the beat. This would allow the local investigator or patrol officer to spend more time on the street and less time in the communications room. Regionalization of the information-sharing system carries the same benefit. Prior to September 11, intelligence-gathering agencies were overwhelmed with unfocused information. I submit this was a large contributing factor to the terrorists' success. The regional concept divides and conquers the immense amount of material.

The JRIC concept also evens the playing field between the "haves" and "have nots." Some agencies have a robust intelligence system that works well within their community. Some have a robust system that connects to other agencies as well. Other law enforcement agencies also need to benefit from that information, and the JRIC provides that conduit. The "have not" agencies, whether from lack of funding, leadership, or lack of perceived need, have no system in place. Given proper funding, the JRIC would provide national guidance on minimum requirements and effectively meet those needs.

Finally, the JRIC system would allow the FBI's sworn officers to focus on gathering information and acting on disseminated information. I debated internally on which agency, the FBI or Department of Homeland Security, should direct the JNIC system. The Department of Homeland Security has no paradigms to change and no bureaucratic inertia to overcome. The Department of Homeland Security seems best suited to create a new organization. By giving the analysis and the conduit responsibilities to Department of Homeland Security, more FBI agents can be put on the street. Also, the FBI has authority that would best be used in the enforcement arena.

Development of a comprehensive information system, coupled with well trained, dedicated law enforcement professionals will no doubt

increase the probability of interdicting planned terror activities. However, in our free society, security absolutes are very rare. Community leaders must demand a JRIC-like system from the federal government, but they must also plan for that system to occasionally fail. To do otherwise would result in potentially catastrophic consequences.

Planning to Respond and Recover

> *Reducing a community's vulnerability to attack requires, among other things, analyzing a locality to identify likely targets and working to improve security at these locations. Completely protecting every reservoir, parking garage, mass transit terminal, large building, and other likely targets within a jurisdiction is not possible.*[26]
>
> —IACP's Leading from the Front: Law Enforcement's Role in Combating and Preparing for Domestic Terrorism

The terrorist tries to find the softest target to get the most results while expending the fewest resources. The law enforcement agency must assess the risk to particular targets within its jurisdiction and attempt to harden the ones most likely to be attacked.[27] With planning, much of the chaotic activity usually produced by these kinds of events can be avoided.[28] Plan formats are readily available on the Internet. One option is to localize FEMA's Federal Response Plan, (FRP) accessible at http://www.fema.gov/rrr/frp/. This is a very in-depth plan that covers all areas of concern for a critical incident, including necessary support functions, and in part describes "the array of Federal response, recovery, and mitigation resources available to augment State and local efforts to save lives."[29] The FRP is a great starting point to develop a plan for any contingency. *[Editor's note: The Federal Response Plan is currently undergoing a thorough review and update by the Department of Homeland Security and is expected to be released as the National Response Plan in late 2004.]*

Mitigation

Successful prevention of a criminal terrorist act is not limited to intervention. Mitigation tactics, techniques, procedures, and technologies (TTPT) that decrease the terrorists intended effect by reducing loss of lives or structural damage should also be categorized as a successful prevention. Though TTPT need to be jurisdictional-specific to maximize mitigation, sharing with or borrowing from other agencies is highly encouraged. It will lessen efforts and time spent in a vacuum developing your own information. Regardless of jurisdictional similarities, minor adjustments will likely be needed. With that said, I do, however, believe certain steps in the mitigation process are applicable to every community, i.e., conduct assessments, create or revise response and training plans, exercise, and evaluate.

Vulnerability Assessments comprised of Consequence Assessments and Physical Security Assessments should be conducted in each jurisdiction. Methods for conducting Vulnerability Assessments are readily available on the Internet or through contacts in other agencies. The Department of Defense is a prolific assessor. The Defense Threat Reduction Agency (DTRA) conducts one assessment called the Joint Staff Integrated Vulnerability Assessment (JSIVA). The JSIVA is a five-day long installation assessment that examines threat assessment, mitigation techniques, and response capabilities.

- A terrorist options specialist looks at current threats and threat levels, the threat assessment process, and operations security.
- Two security operations specialists review operational plans, personal protection procedures, and security forces manning, training, and equipment.
- A structural engineer interfaces with base engineers and planners, surveys selected structures, reviews architectural and structural drawings, and performs quantitative analysis of blast effects to establish effective standoff distances.
- An infrastructure engineer focuses on the installation's supporting infrastructure such as water, power, and

communications protection against terrorist incidents. The infrastructure engineer also determines if there are any potential single-node points of failure.

- An operations readiness specialist focuses on the installation's preparedness to respond appropriately to a terrorist attack employing explosives, chemical, biological, nuclear, and radiological weapons. The operations specialist also reviews public affairs, medical, emergency operations center, legal, and communications programs.[30]

Results from JSIVAs are provided to installation leadership for corrective action. Some actions can be corrected through procedural changes, some through physical security installment such as barriers and intrusion detection systems, while others are unable to be addressed due to lack of funding. Vulnerability Assessments allow leadership to identify their vulnerabilities and create a prioritized spending list. Higher headquarters, either through annual budgets or additional Congressional appropriation, will often fund installation projects from their priority list.

Using the same process of assessing the vulnerabilities, identifying monetary shortfalls, and creating a prioritized list, local communities could reap the same fiscal benefit from their state or federal government. An excellent case in point on how preparation yields financial rewards is found in Louisiana.

In December 2002, FEMA granted "nearly $2 million to Louisiana for state and local responders and emergency management to become better prepared to respond to acts of terrorism and other emergencies and disasters."[31] Over the years, Louisiana has suffered from severe natural disasters in the form of hurricanes, floods, and tornadoes. With those come all the logistical challenges associated with a large population in the coastal region. For years, Louisiana has mitigated these effects by planning for warning, evacuation, shelter, and response procedures and funding equipment that supports those procedures. In November 2002, I visited the Louisiana Office of Emergency Preparedness, Emergency Operations Center to see their operation.

Using the Louisiana Emergency Assistance and Disaster Act of 1993, which established standards, requirements, and funding, the leadership in the Louisiana Office of Emergency Preparedness has done a

tremendous job organizing, training, and equipping the state's emergency management system. The Emergency Operations Center is very well arranged and rivals most military command centers I have seen, including the United States Central Command's Combined Air Operations Center at Prince Sultan Air Base in the Kingdom of Saudi Arabia. Their communications system, for instance, connects with 42 towers, making it capable of connectivity with all parishes (counties) in the state.[32] Although mainly used for natural disasters, this Emergency Operations Center is capable of managing any emergency, manmade or natural.

After September 11, 2001, the Louisiana Office of Emergency Preparedness expanded its existing infrastructure and focused on terrorism and WMD. Once they assessed their operation for that additional mission, they revised their response plan, identified deficiencies, and applied for a FEMA grant to fund corrective actions. The effort and money spent in the early years of emergency management did not go unnoticed. Louisiana reaped benefits because of their hard work and dedication to making their communities safer. In the following quote from the FEMA press release, notice the focus in plans at the local level.

> Of the nearly $2 million grant, $1.5 million will be provided for updating state and local plans and procedures to respond to all hazards, with a focus on weapons of mass destruction. The updated plans will help address a common incident command system, mutual aid agreements, equipment and training standards, interoperability protocols, critical infrastructure protection, and continuity of operations for state and local governments. *At least 75 percent of the grant amount is required to go to local governments.* The funds will assist local governments develop comprehensive plans, linked through mutual aid agreements, outlining the specific roles for all first responders (fire service, law enforcement, emergency medical service, public works, etc.) in responding to terrorist incidents and other disasters.[33]

Louisiana took advantage of all the money and effort they placed into their emergency management system. This grant money is currently

available to any community through FEMA. With the stand-up of Department of Homeland Security, coupled with constituents calling for funds to thwart possible terrorist incidents, I am positive future funding for like homeland security projects will be available. To capitalize on these funds, communities should assess their vulnerabilities, create or revise their response plans, identify shortfalls associated with their plans, and prioritize their needed resources.

Consequence and Physical Security Assessments

The Center for Civil Force Protection examines the consequences and physical security. There are four major categories in the Consequences Assessment that need to be addressed: loss of life, loss of revenue, loss of vital infrastructure, and loss of vital resources.[34] Obviously, loss of life would outweigh any consequence and should be given a higher value in calculating where to focus mitigation funding. Schools, hospitals, and large office buildings may fit into this category. The term *may* is used because there are so many other variables in each category. For instance, a large facility such as a school or office building may not be occupied during the hours of darkness. That's a significant factor. The hospital may receive additional weight in the consequence scale because your response plan is dependent on that hospital being available for use as the trauma hub in the case of a mass casualty event. Because of the complex, interwoven network and the multiple variables involved, a Vulnerability Assessment is not a one-person job and also not a job for law enforcement alone. It requires a team with members from all disciplines in the community.

When factoring consequences during a Vulnerability Assessment, place physical security in the plus column. Physical Security Assessments measure each system or facility's detection/assessment, delay, and response capabilities.[35] In the hospital example above, proper physical security measures would reduce the loss of life and/or infrastructure consequences. Physical Security Assessments often lead the assessor to ask a string of questions. Does the chemical plant in town have a security plan? Does corporate security or a private agency administrate it? Is my agency capable of responding to hazardous material incidents or will the corporation take that action? Are the exit routes capable of handling the amount of traffic exiting the cordon while allowing response vehicles access? When answered, questions like these will lead to measures to

mitigate negative effects of terrorist incidents as well as industrial accidents. Capability Assessments, when combined with Physical Security Assessments, begin the lessons learned loop that should be used to revise existing plans and further pinpoint where your money should be spent.

Exercises and Evaluations

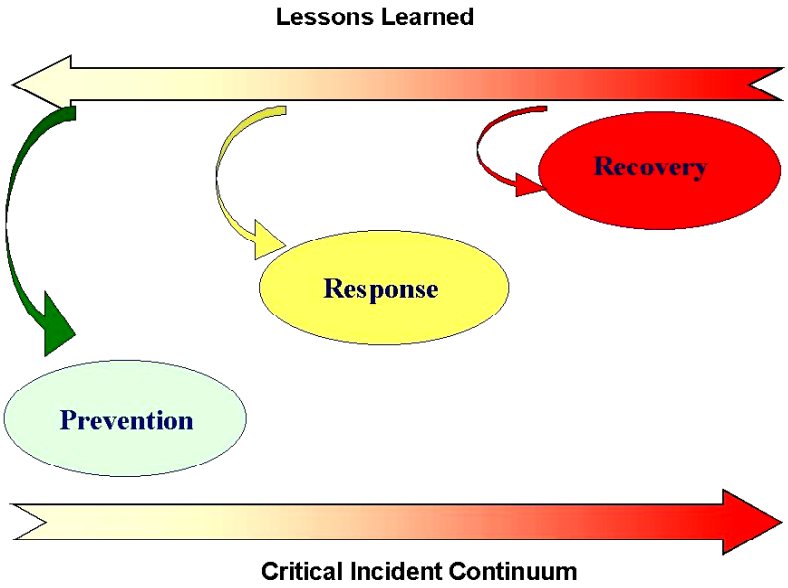
Over the last 25 years, emergency management training, as well as component-specific training, (law enforcement, fire, and medical) has kept stride with the needs of the community. State, federal, or private industry has always had visionary leadership to forecast future training needs. For most agencies, the shortfall has not been availability, but funding to support their training programs. Community leaders must fund or seek funding to continue these vital training programs. Well-trained responders are more confident and competent. Should an incident occur, the investment in training would pay huge dividends in lives saved.

An area that may not be as familiar to jurisdictions is exercising and evaluating their existing systems. Exercising and evaluating are as much a part of Vulnerability Assessments as studying consequences and physical security. Communities should conduct multidisciplinary exercises to identify vulnerabilities. Each community must determine which agencies need to be involved. In the previous example, the Louisiana Office of Emergency Preparedness Emergency Operations Center has a workspace for a representative from the hotel and restaurant industry. Their presence and connectivity with local hotels along the hurricane evacuation route provides valuable information to decision-makers. If your jurisdiction has the same concern, they must be included in the exercise. The entire system's efficiency is multidisciplinary dependent. Those communities that have conducted pre-incident exercises based on well-developed community response plans and have actually faced critical incidents have discovered that planning and exercising substantially improves their personnel's performance. Exercises work out relationships and problems before an incident occurs.[36] Exercise results also add information to your lessons learned loop.

When conducting these exercises, community leaders should consider inviting experts from other jurisdictions to observe and evaluate their plans and execution of their plan. The ideas, viewed from the outside, may identify additional vulnerabilities overlooked by the host. It's highly

likely these vulnerabilities may be overcome by simple procedural changes. Leaders who engage in this bold approach may be risking ego bruising as others will probably be critical of systems different from their own. Communities who ask others to evaluate their operation should remember that the criticism is intended to provide a different approach to an issue that can be dismissed or adopted by the community leadership. Evaluation, whether self-conducted or assisted by an outside agency, is a continual process. As depicted in the Critical Incident Continuum in Figure 8.3, it provides valuable information for every task.

Figure 8.3 Critical Incident Continuum



Source: Author's Model

Funding the Fight

Chief Ed Flynn of the Arlington County, Virginia, Police Department said, "While billions of dollars will, and should, be spent on federal-level preparedness and response to terrorism, one fact remains clear: the first responders to these acts will be beat cops—and they will need the

leadership of their chiefs to do the job right."[37] Training and equipping the beat cop to do the job for which they have been assigned is a leadership responsibility. For most local departments, training and equipping for terrorist prevention, response, and recovery requires funds over and above what most local departments are allocated annually. Federal assistance is vital to protect the lives and infrastructures. Two of the responsibilities of the Department of Homeland Security Director of the Office for Domestic Preparedness include:

- Coordinate preparedness efforts at the Federal level, and work with all state, local tribal, parish, and private sector emergency response providers on all matters pertaining to combating terrorism, including training, exercises, and equipment support, and
- Direct and supervise terrorism preparedness grant programs of the Federal Government (other than those programs administered by the Department of Health and Human Services) for all emergency response providers.[38]

The Department of Homeland Security has a tremendous opportunity to create a funding system that will insure funds and grants reach those who protect America's Front, and provide good stewardship of those allocated funds. Rather than creating their own system for this funding, the Department of Homeland Security should look at the funding system of the Department of Defense. When money is allocated from the Defense Budget to the Services, it is assigned a Program Element Code that identifies a specific mission. For instance, the Program Element Code for air base defense is 27588. Money allocated under that Program Element Code is for the sole purpose of air base defense programs and equipment. The system does allow money to transfer to other missions, but significant justification is required. Homeland Security Program Element Codes could include such programs as First Responder Training; Communications Systems; Hazardous Material; Biological, Agricultural, Chemical Abatement; Counterterrorim Task Force (SWAT), and many more.

The following is an example of how the system could function in the Department of Homeland Security. Pascagoula, Mississippi, after assessing their industrial complex and revising their response plan, may

need three additional Hazardous Material response vehicles to mitigate the damage an attack or accident could cause. Federal money is allocated for those vehicles under a Hazardous Material Program Element Code with the understanding that the money can only be spent on those vehicles. Meanwhile, the five jurisdictions within Jackson County, Mississippi decide to form a coalition and pool their resources to create a Hazardous Material response team. As a coalition, they only need one more vehicle to mitigate damage at the industrial complex, but they find their communications interoperability is insufficient for that coalition to operate. They request part of the original allocation to be transferred to the Communications Program Element Code. They justify their request by showing multiple benefits that serve emergency management in a much broader sense than just the industrial complex; i.e., the communications system is located in a coalition Emergency Operations Center and can be used for any manmade or natural disaster. The Department of Homeland Security would likely approve the request to change the color of money because it is more efficient and helps multiple jurisdictions with one allocation.

The basis for my proposal stems from information received in the United States Air Force Counterproliferation Center's Homeland Security Seminar. A representative from a Federal agency discussed his experience in dealing with local governments. He said most local governments expressed their lack of confidence in their state agencies' ability to pass along the Federal money to them. In order for the funding system within the larger Homeland Security system to be effective, local agencies must trust their state-level brethren. Also, because of the enormity of the undertaking, the Department of Homeland Security needs state governments to administer their money. The division of labor helps with the span of control. State agencies must be trusted by both the Federal and local governments to properly administer homeland security dollars. A Defense Department-like program with accounting trails and Government Accounting Office audits would insure proper appropriation and would instill trust in all parties.

Emergency Management Coalitions

Coalition warfare is commonplace in the history of warfare itself. Various reasons exist as to why these coalitions formed. Today, coalition warfare exists mainly for diplomatic or political reasons. Emergency

Management Coalitions should exist for the same reasons they have existed in historical warfare, however, one of the main reasons is fiscal efficiency. As previously mentioned, 77 percent of the law enforcement agencies have 24 or less sworn officers. They operate on a shoestring budget. Joining forces and the creation of co-dependent jurisdictions would provide better use of the limited homeland security dollars.

Many states are now divided into districts. For instance, Georgia has eight, while Mississippi has three. Cities and counties within districts should consider forming emergency management or law enforcement coalitions. For example, take four adjoining counties. Each, depending on their vulnerability assessment, may require certain services to mitigate their vulnerabilities in case of a critical incident. In this example, the four counties may have the common needs: first responder training, interoperable communications, hazardous materials response, and Counterterrorism Task Force.

Each county would take one of the four needs as their responsibility. Let's say County A takes the responsibility for first responder training. That county, through their emergency management or public safety director, would request funds to send a member from each discipline (police, fire, emergency management services, etc.) to a first responder instructor training class. Once they were trained, they would train all members of all agencies within their coalition. State and Federal funds would be spent on just one county but they would get four counties worth of training in return. This example applies to all aspects of the Respond to and Recover from tasks. Additionally, the example is also not just limited to the coalition in the example; memorandums of understanding could easily be reached with adjoining coalitions, including ones in adjoining states. The possibilities, with the right leadership, are endless.

Conclusion

> *We face an adaptive enemy. Empowered by modern technology and emboldened by success, terrorists seek to dictate the timing of their actions while avoiding our strengths and exploiting our vulnerabilities.*[39]
>
> —National Strategy for Combating Terrorism

In concluding my discussion on strategic, operational, and tactical partnerships, I weigh my points and ideas against the goals and objectives of the *National Strategy for Combating Terrorism*. Although the complete integration of all goals and objectives are vital for successful homeland security, I will concentrate on the fourth goal—Defend U.S. Citizens and Interests at Home and Abroad—and its objectives:

- Implement the *National Strategy for Homeland Security.*
- Attain domain awareness.
- Enhance measures to ensure the integrity, reliability, and availability of critical physical and information-based infrastructure at home and abroad.
- Integrate measures to protect U.S. citizens abroad.
- Ensure an integrated incident management capability.[40]

The *National Strategy for Homeland Security* is the approved roadmap by which we as a nation will protect our American way of life. The stated tasks are clear and the implied tasks as they pertain to each community are easily extracted. Federal agencies responsible for Homeland Security must create new systems or modify existing systems to produce maximum effects while minimally taxing (fiscal and otherwise) the American people and our infrastructure. Systems that provide real-time, accurate threat information to the agency or agencies that have the greatest potential for incident prevention and that properly fund local governments so they can alleviate or mitigate their vulnerabilities are two examples. Vulnerabilities are identified and prioritized through assessments. They can be conducted locally, by other agencies, or by a contractor, but must be accomplished.

State and local governments, using the *National Strategy for Homeland Security* as the basis for their operational and tactical plans, coupled with threat information and known vulnerabilities, can further develop detailed plans, prioritized requirements lists and request Federal funding assistance for resources beyond their financial capability. All financial requests should be linked to the goals and objectives of the *National Strategy for Homeland Security*. The International Association of Chiefs of Police President, Chief Joseph Samuels, Jr., has brought

national attention to funding priorities and advocates for Federal assistance to states and local governments. "It is critical that our members have the tools and resources needed to meet public expectations of us for safety and security. Securing Federal financial assistance and resources for state and local law enforcement will be one of the three priorities."[41]

Information and funding systems like those proposed in this text are vital in attaining integrated domain awareness. "Domain awareness is dependent upon having access to detailed knowledge of our adversaries distilled through the fusion of intelligence, information, and data across all agencies."[42] The Joint Regional Information Center provides domain awareness plus. The Joint Regional Information Center construct is designed as an information conduit, not terrorist related information only. International and interstate criminal lines of communication are like high occupancy vehicle lanes for all to use. To field an information system that fails to include all like information would be like removing a step from a math formula and still expecting the correct answer.

To better explain how an incomplete system is a formula for failure, I will use a historical case in point—the Law Enforcement Assistance Administration funding in the 1960s. This program was designed "to provide state and local law enforcement agencies with modern tools to fight crime but was disestablished in 1982 amid criticism that it had frittered away billions of dollars while crime rates rose."[43] On the surface it looks as if the idea and funds behind the idea were flawed, but consider the following information.

The criminal justice system is much more than just law enforcement. The criminal justice system consists of education, enforcement, the courts, and corrections. The Law Enforcement Assistance Administration only provided funds for law enforcement. As law enforcement efficiency improved, it created backlogs in the courts and overcrowding in the prisons—a funnel effect.

As court dockets filled, lesser crimes were often handled through plea-bargaining, with the criminal getting a lesser punishment. Likewise, the state prisons and county jails suffered from overcrowding. This drove United States courts to establish guidelines for prisons and jails and levy fines for noncompliance. Since states and counties could not afford the penalty for violating federal court mandates, work release programs were created instead of raising taxes to build more prisons. In many cases,

prisoners were released before serving half of their sentence and relocated into halfway houses and worked in the community. Crime rose, in this case, because of law enforcement's effectiveness—funding a component vice the entire criminal justice system.

Finally, ensuring an integrated incident management capability, considering the variety of jurisdictions within the United States, may be the most costly of the objectives. "An effective, integrated response requires incident management planning, enhanced interoperability, and coordination, based on and supported by rapid and effective decision-making."[44]

Federal guidance will be necessary to ensure integration. The Department of Homeland Security will need to establish minimum requirements for each jurisdiction type. For instance, a municipality with a population from 50,000 – 100,000 people must have the capability to communicate with all emergency management agencies within their county and bordering counties.

From this Federal guidance, local communities will establish their operations requirements. Using the above example, the required capability could mean a new central communication system or just reprogramming the existing equipment. Cost will vary with each jurisdiction. Resourceful governments will establish coalitions as mentioned in this text. Some less populated regions may have no other recourse but to bear the sole brunt of the required minimum standard. A funding system, as mentioned previously, where money is categorized and checks and balances exist to ensure the money allocated is spent properly, not only facilitates this objective, but builds confidence at every level of government from Congress to the constituency.

Although each citizen should do their part to prevent terrorism, those of us who have chosen public service as our profession carry a tremendous responsibility—organizing, training, and equipping the men and women who man the American Front. Together with these men and women, "we must take the battle to the enemy, disrupt his plans and confront the worst threats before they emerge. In the world we have entered, the only path to safety is the path of action. And this nation will act."[45]

In the wake of the September 11, 2001, attacks, there was no hesitation to *react*. As the ripples from that sensational event fade into a vast ocean of competing priorities, we must be able to articulate our strategic, operational, and tactical goals and objectives necessary to

prevent or mitigate future loss of life. We must act to prevent and mitigate because we cannot afford the consequences of waiting only to reaction.

Notes

1. Office of Homeland Security, The *National Strategy for Homeland Security*, July 2002, 2.

2. Philip M. McVey, "An Effective Homeland Defense Partnership," *Police Chief*, April 2002, 174.

3. Homeland Security, *National Strategy*, 1.

4. Ibid., n.p.

5. Ibid., 1.

6. D. Douglas Bodrero, "Law Enforcement's New Challenge to Investigate, Interdict, and Prevent Terrorism," *Police Chief*, February 2002, 43.

7. International Association of Chiefs of Police, *Criminal Intelligence Sharing: A National Plan for Intelligence-led Policing at the Local, State, and Federal Levels*, (Alexandria, VA: August 2002), 10.

8. Bodrero, 48.

9. Robert S. Mueller, III, "From the Director: Teamwork is Our Future," *Police Chief*, January 2003, 8.

10. Homeland Security, *National Strategy*, n.p.

11. D. Douglas Bodrero, "Law Enforcement's New Challenge to Investigate, Interdict, and Prevent Terrorism," *Police Chief*, February 2002, 43.

12. W. Ronald Olin, "Why Traditional Law Enforcement Methods Cannot Win the War on Terrorism," *Police Chief*, November 2002, 30.

13. National Commission on Terrorism, *Countering the Changing Threat of International Terrorism*, (Washington, DC: June 2002).

14. Gene Voegtlin, "IACP Testifies on Local Law Enforcement Role in Homeland Defense," *Police Chief*, February 2002, 8.

15. Robert S. Mueller, III, "From the Director: Teamwork is Our Future," *Police*

Chief, January 2003, 8.

16. Voegtlin, 8.

17. Gene Voegtlin and Jennifer Horne, "IACP President Testifies on Department of Homeland Security, " *Police Chief*, August 2002, 8.

18. Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 12 April 2001, 446.

19. Federal Emergency Management Agency home page, on-line, Internet, available from http://www.fema.gov/regions/.

20. Joint Pub 1-02, 245.

21. Name withheld due to academic freedom policy, Air War College, Montgomery, Ala., 10 January 2003.

22. New Jersey State Police Homepage, n.p., on-line, Internet, November 2002, available from http://www.njsp.org/about/itelb.html.

23. Mueller, 9.

24. Bodrero, 45.

25. International Association of Chiefs of Police, *Criminal Intelligence Sharing: A National Plan for Intelligence-led Policing at the Local, State and Federal Levels*, (Alexandria, VA: August 2002), 8.

26. International Association of Chiefs of Police, *Leading from the Front: Law Enforcement's Role in Combating and Preparing for Domestic Terrorism*, 10.

27. Philip McVey, "An Effective Homeland Defense Partnership," *Police Chief*, April 2002, 176.

28. International Association of Chiefs of Police, *Leading from the Front: Law Enforcement's Role in Combating and Preparing for Domestic Terrorism*, 10.

29. Federal Emergency Management Agency, "Federal Response Plan," n.p., on-line, Internet, December 2002, available from http://www.fema.gov/rrr/frp/frpintro.shtm#purpose.

30. Defense Threat Reduction Agency, "Joint Staff Integrated Vulnerability Assessments Fact Sheet," July 2002, n.p., on-line, Internet, November 2002, available from http://dtra.mil/news/fact/nw_jsiva.html.

31. FEMA. On-line, internet, available from http://www.fema.gov/regions/vi/2002/r6_03_12_01la.shtm.

32. Visit November 2002, Brief, Baton Rouge, LA.

33. FEMA. On-line, Internet, available from http://www.fema.gov/regions/vi/2002/r6_03_12_01la.shtm.

34. Center for Civil Force Protection, "Community Vulnerability Assessment Methodology," Presented by Nick Nicholson, PhD. Sandia National Laboratories, National Institutes of Justice, Slide 19. On-line. Internet, November 2002. Available from http://www.nlectc.org/ccfp.

35. Ibid., Slide 21.

36. IACP, Leading, 10.

37. Ibid.

38. Department of Homeland Security, Reorganization Plan, November 25, 2002, paragraph 2,B, 3,c. On-line, Internet, January 2003, available from http://www.dhs.gov/dhspublic/.

39. *National Strategy for Combating Terrorism*, 24.

40. Ibid. 25-27.

41. Joseph Samuels, Jr., "President's Message: The Challenge Before Us," *Police Chief*, November 2002, 6.

42. *National Strategy*, 25.

43. William L. Schwabe, *Improving Crime-Fighting Technology in Law Enforcement*, 2001, n.p., On-line, Internet, November 2002, available from http://www.fathom.com/story122018.

44. *National Strategy*, 27.

45. George W. Bush, June 2002, quoted in the *National Strategy for Combating Terrorism*, 11.