

The State and Local Role in Domestic Defense

by John D. Cohen and John A. Hurson

On the ground and in the skies above Afghanistan, decades of effort to integrate battlefield information systems have paid dividends in the war against terrorism. Army and Marine ground troops, Navy and Air Force pilots, and distant joint command centers now communicate easily via common systems, sharing fresh targeting information in real time, while bombs and missiles launched by pilots from 20,000 feet are then guided by hand-held lasers on the ground with deadly precision.

At the same time, the Sept. 11 terrorist attacks have uncovered the costly lack of integration in our domestic defense efforts. Consider:

- Prior to September 11, a number of the hijackers turned up on the radar screen of local law enforcement or government attention. Some were issued driver's licenses under false identities, two were arrested for drunk driving, another was the subject of a misdemeanor arrest warrant, and yet another was apparently stopped by a state trooper just days prior to the attacks. In each of these cases, their names were entered into state government or local criminal justice-related data systems. Meanwhile, the FBI was seeking to locate at least two of these individuals, and some of their names apparently were also being tracked in other intelligence databases. Unfortunately, because these various information systems are not sufficiently

interlinked and maintained, the chance to potentially disrupt some of the hijackers was lost.

- On September 11, when police and fire departments from Arlington County, Va., Montgomery County, Md., and the District of Columbia responded to the Pentagon terrorist attack, they were unable to communicate with each other using their own radios. Why? Most individual public safety entities operate individual radio systems that utilize different frequencies.

As the examples indicate, the nation's law enforcement and emergency response systems are largely tied to geographical jurisdictions or to specific functions, and as a result do not function cohesively. These and other lessons growing out of the Sept. 11 attacks and their aftermath should guide policymakers as they scramble to bolster the nation's ability to defend against and respond to terrorism.

First, we must redefine our concept of national security. We can no longer afford to think of national security as the sole province of the military, or even the federal government's intelligence, law enforcement, and border control agencies. Keeping America safe from terrorists and responding when they elude our defenses is also the urgent task of state and local law enforcement and response agencies.

Second, our approach to domestic defense must be national and seamless. To this end, we

must improve information sharing with our front line law enforcement officers, either to bring in suspected terrorists or disrupt their plans by catching them in unrelated crimes. Similarly, as the example above also illustrates, we need new communications systems that permit emergency response agencies to coordinate as easily here at home as our troops do abroad. Public health systems need critical information systems to detect outbreaks of bio-terrorism and surge capacity if they succeed.

Third, as weeks turn to months, one thing has become clear: The nation has neither the stamina nor the resources to continue operating indefinitely in an “emergency response” mode. We must find a new way of conducting the business of government that makes domestic defense a top priority in the everyday work of government, not just on emergency footing. If we do so, all law enforcement functions and overall public safety will benefit.¹

Domestic defense is a national priority that must be pursued at every level of government. The federal government must recognize not only its own need to improve the coordination of federal agencies, but also must set clear national priorities to guide action for states and localities. States must ramp up to the task quickly and together, rather than be left to their own pace, political idiosyncrasies, and resources. This coordination should be a top priority for the director of intergovernmental affairs at the Office of Homeland Security. Congress must also provide state and local governments with financial assistance to ensure implementation, using block grants with accountability measures.

Clearly, federal agencies—from the FBI to the border patrol—will play critical roles in our domestic defense. But inevitably, responsibility for future homeland defense efforts will rest primarily upon the states and their localities, given their central role in providing for public safety, civil defense, and

public health.² The first person on the scene of a domestic terrorist incident will be a police officer. Local firefighters and emergency medical technicians will conduct rescue operations and provide medical care at the scene of an attack. Community-based health care and social service entities will provide short-term, continuing care, and social service support to victims and the victims’ families. Local telephone systems including 9-1-1 will become overwhelmed due to a large volume of traffic. Local roadways will become clogged and public utility service may be interrupted.

Though terrorist attacks create confusion and overload response systems, we must resist the temptation to create operational and technology infrastructures that are only mobilized in response to a critical incident or terrorist attack. Instead, we must build on ongoing state and local initiatives such as police partnerships and statewide information sharing and communication capabilities. The goal should be improved service on a day-to-day basis, while recognizing that this infrastructure will serve as the foundation for efforts to prevent and/or respond to critical incidents and terrorist attacks.

State and local governments should develop a comprehensive strategy to address these and other important issues related to the prevention of, and response to, critical incidents. This strategy should include an assessment of potential targets for attack (buildings, water works, power plants, and so on) and a detailed response plan that includes how federal, state, local, and private entities will work together to prevent and/or respond to critical incidents. This strategy should include both immediate and long-term action plans, identify key components of the response system, and establish key systems that are needed to support the response to such critical incidents.

To this end, this paper recommends a variety of actions, including these four concrete steps:

- Launch “integrated justice” information systems to link the information from various arms of the criminal justice system about the people who commit crime and the places where crime occurs. Efforts underway in 38 states and the District of Columbia must be accelerated and made universal.
- Integrate emergency response communications systems so first responders from different agencies and jurisdictions can talk to each other as easily as the troops in Afghanistan. The state of Maryland has launched a pilot project to patch disparate radio systems into an integrated network that offers a model for the way forward.
- Establish a coordinated surveillance, identification, containment, and response system designed to minimize the effects of a biological and/or chemical attack. The Lightweight Epidemiology Advanced Detection & Emergency Response System (LEADERS) deployed by some hospitals and state medical offices in New York and Phoenix during this year's World Series is a good first step that can be expanded to improve detection capabilities.
- Make it easier for the public to call for help or information without jamming 9-1-1 lines with a clearly identifiable phone number such as the 2-1-1 system being deployed in some locales.

Connect the Dots with the Data

As indicated above, agencies were unable to draw a larger pattern out of disparate bits of information, contained in separate databases, about the activities of terrorists involved in the

Sept. 11 attack. We will never know whether better data sharing would have helped thwart the attacks. But we do know that terrorists often use traditional crimes such as drug trafficking, money laundering, bank robbery, and illegal weapons trafficking to offset the costs and further support their political/terrorist objectives. In fact, the first indication that a terrorist cell is operating within the United States may be behavior discovered during an investigation by local police following the report of suspicious circumstances or some type of criminal event.

Whether the focus is on drug trafficking or an act of bio-terrorism, rapidly collecting and disseminating good information about the people who commit crime and the places where crime occurs is the key. Yet most police, parole officers, and courts are operating with 20-year-old information technology. Even though high-speed digital technology is currently available, many police officers still wait unacceptable periods of time to receive basic information about a vehicle or person they stop. Days or weeks can pass before criminal warrants find their way into state databases, leaving dangerous criminals on the street and police unaware they are wanted. Judges sentence offenders without seeing their criminal history records. Investigators in one jurisdiction may be unaware that information exists in a neighboring jurisdiction regarding an individual under investigation.³

There is some progress afoot. As stated above, efforts are underway in 38 states and the District of Columbia to create “integrated justice” information systems to permit the rapid flow of information between the different components of the criminal justice system (police, courts, corrections). This data allows law enforcement to identify suspicious trends and effectively target those involved in criminal activity. These same systems are an essential component of any statewide efforts to prevent and/or respond to future critical incidents and terrorist threats.

Accelerating these efforts to deploy integrated justice systems must be a national priority. But information sharing cannot stop at the state level. Law enforcement and security authorities across the country must be able to access each other's data in real time. Just as search engines on the Web allow instantaneous access to vast sources of information with the click of a mouse, we must create a system in which secure facilities (such as airports) can access the terrorist "watch list" in the National Crime Information Center (NCIC), keeping in mind privacy and the need to protect intelligence sources and methods. Also, public safety information and communication systems should be interlinked with those of other critical government systems (such as those that support transportation, social services, and public utility-related activities).

Wire the Responders

During any critical incident, it is essential that first responders be able to communicate with each other in real-time via radio. Unfortunately, most individual public safety entities operate individual radio systems that utilize different frequencies.

The inability of Washington-area emergency response teams to communicate at the Pentagon is just one example. Generally, when police officers chase a criminal up a freeway, they cannot directly speak to officers from other departments. If a prisoner escapes from a state prison, corrections officers are unable to use their radios to talk to officers from local police departments.

Efforts to address such deficiencies have been energized following the events of September 11. For example, Maryland recently announced efforts to establish a statewide network that will link the independent wireless voice and data systems currently used by federal, state, county, local and private entities with a new patching

technology. The state intends to link its efforts with those currently planned by both the Washington Metropolitan Area Council of Governments (COG) and the Capitol Area Wireless Interoperability Project (CAPWIN). The goal is to eventually create a regional "patching network" linking public safety, transportation, and other appropriate agencies in Maryland, the District, and Virginia. This initial phase will focus on facilitating communication between smaller municipal public safety entities (police, fire, EMS) with appropriate county and state entities.

As a first step, the state will deploy seven cross-band radio connector devices at various locations throughout the state. Each of these devices will then be linked, providing contiguous coverage for an area that includes most of the state. Once installed, the independent radio systems currently in use by the various public safety systems operating within this area will be able to communicate with each other. Deployment of this system will begin in November, and it is anticipated that the design, installation, and training will take approximately nine months.

As part of this demonstration project, the state will deploy approximately 100 handheld computers containing wireless modems to allow individual users to access the Maryland Interagency Law Enforcement System (MILES) and the National Crime Information Computer (NCIC); send messages to other personnel (both inside and outside an individual's agency); access information contained in other key databases (such as those containing information related to commercial vehicles); and record information regarding suspicious persons, vehicles, and circumstances.

Bolster Defenses Against Biological and Chemical Terrorist Attacks

The recent deaths caused by anthrax exposure illustrate that the threat of bio-terrorism is no

longer limited to action movies or books—it is real, it is here, and the nation needs to be prepared for future attacks. While the different types of infectious and chemical agents that could be effectively used in an attack on domestic U.S. targets is limited, the effects of such an attack are potentially devastating. The best defense is a strong public health system that uses technology to identify emerging disease and environmental threats.

In all likelihood, the first indication of a domestic bio and/or chemical incident will be subtle and difficult to identify. First, primary care physicians, emergency medical personnel, and staff at local hospital emergency rooms located within and close to the exposed area will begin seeing an increased number of people seeking treatment for flu-like symptoms or other medical issues. Over a several-day period, emergency room doctors—working in publicly and privately funded hospitals—will record and report, most often using a paper-based system, patient-related information that eventually will generate concern that people have been exposed to biological and/or chemical weapons. State authorities will work with the Center for Disease Control to determine the exact agent utilized, to support treatment activities. Once determined, the Department of Health and Human Services and appropriate state agencies will initiate response procedures that include providing doctors treatment protocols, and even dispatching physicians and pharmaceutical drugs.

Currently, if any jurisdiction within the United States were the target of biological or chemical attacks, the response would include one or more of the following entities and resources: fire and rescue responders who have received little or no training; hospitals, clinics, and other health care providers whose staff have little or no formal training in medical management of chemical and/or biological attack, and that are poorly coordinated, lacking medical management and

decontamination protocols, adequate bed capacity, and advanced life support systems; or public health surveillance systems that rely upon protocols and business processes that may be too slow to effectively identify and address a biological and/or chemical weapons attack. The list could go on, including a hodgepodge of federal agencies that operate in a poorly coordinated system that may not meet immediate needs for effective crisis management.

But the point, as made by a recent report by the U.S. General Accounting Office (GAO) about hospitals, is that inadequate training and planning for bio-terrorism is a major problem. As the GAO noted with hospitals, they often lack basic tools, such as communications, information, and Internet technologies that allow them to communicate rapidly and effectively with field units, health departments, and laboratories. Often times it is difficult to get hospitals and medical personnel to participate in local training, planning, and exercises to improve preparedness. The GAO also reports that there is little or no excess capacity in the health care system in most communities for accepting and treating mass casualty patients.

States should conduct a thorough assessment of response systems to determine whether they are adequate to manage the significant threat to the public. Additionally, each individual state should take steps to improve its health care system so that it is prepared for future mass casualty incidents, such as bio-terrorist attacks. State governments should establish a coordinated surveillance, identification, containment, and response system designed to minimize the effects of a biological and/or chemical attack. This should include a comprehensive, response plan across local, state, and federal agencies that includes:

- establishing a local state command center;

- obtaining adequate detection equipment and enhance state capability for laboratory identification of pathogens;
- integrating secure communication systems among statewide detection units, labs, first responders, health care facilities, and government agencies;
- developing statewide disease surveillance information systems;
- accelerating specialized training of health care providers, first responders, and other personnel;
- coordinating protection of local first responders and facilities;
- ensuring access to stockpiled medications and vaccines;
- constructing decontamination facilities at all hospitals within the state;
- increasing surge/bed capacity and alternative/mobile medical facilities for all hospitals; and
- coordinating all local biochemical response with current federal and military systems.

One example of an information system that could support efforts to detect acts of bioterrorism is LEADERS. The Web-based system is being built to allow hospitals and medical authorities to subscribe without having to buy any additional hardware or software. Through LEADERS, medical personnel will have the ability to track symptom outbreaks as they are reported by hospitals in real time. They will also be able to map geographic regions where outbreaks are occurring and determine response capabilities of various medical facilities. Early components of the LEADERS

system were deployed in hospitals and state medical offices in New York and Phoenix during this year's World Series, when the threat of anthrax attacks had put security officials on a heightened state of alert. The system also was used in New York shortly after the Sept. 11 terrorist attacks and within 24 hours had linked more than 250 hospitals to real-time symptom tracking. States may want to expand upon the original LEADERS capability and include (1) additional reporting sources (EMS, 9-1-1, primary care physicians), (2) passive reporting capabilities (information automatically transmitted by reporting parties' systems) and (3) capabilities that support infection detection within individual health care facilities.

Connecting Citizens with 2-1-1 and 3-1-1

State, county, and local governments need to make it easier for the public to call for help. Not surprisingly, on September 11 the public sought emergency and non-emergency assistance via telephone. In areas where there was a clearly identifiable phone number where the caller could obtain information and referral support for social service, health care, and other non-emergency topics, the public utilized that number. In cases where an alternative number was not clearly identifiable, the public tended to call 9-1-1.

One successful example of a non-emergency system in use on and after the events of September 11th was in Connecticut. In 1999, the state deployed a statewide 2-1-1 telephone system for information and referral services on health and human services. 2-1-1 is an easy-to-remember, toll-free, statewide number providing points of contact designed to assist people in clarifying their needs for services and to direct them appropriately. With the 2-1-1 system in place (integrated with 9-1-1 and other critical systems), on September 11 the state was able to adequately respond to requests such as families looking for victims, mental health services, blood bank needs, etc. Likewise, Mayor Anthony Williams and the

District of Columbia were able to decrease the overwhelming number of 9-1-1 calls received in Washington, D.C., on September 11 by off-loading non-emergency calls onto the Metropolitan Police Department's existing 3-1-1 Police Non-Emergency Telephone System. In the wake of the terrorist attacks, the District government publicized the use of 3-1-1 with the assistance of area media outlets, allowing 9-1-1 emergency calls to be prioritized while still responding to requests for information, referral, and other non-emergency inquiries."

Such systems and the data they accumulate provide invaluable foundational resources for local governments and the non-profit and private sectors to better and more cooperatively prevent and respond to crisis situations and everyday events.

Conclusion

The nation is rightfully focused on domestic defense and providing our public health, public safety, military, and intelligence communities with the tools, the authority, and

the resources necessary to detect, prevent, and respond to all forms of terrorist crime and violence. But protecting our homeland from terrorists—need not and must not—be done at the expense of our core civil liberties and constitutional protections. Proactive, information-driven, law enforcement efforts—supported by rapid, effective sharing and collection of information—eliminates the need to utilize ineffective, random, and reactive enforcement strategies. Furthermore, the best preparation for future acts of terror can be found in the same techniques and technologies that can be used to better protect our neighborhoods from drug traffickers, robbers, and burglars, and to keep our communities healthier. Our goal should be to deploy information and communication technology and operational strategies that support efforts to provide effective delivery of service by government agencies each day, recognizing that this infrastructure will serve as the foundation for efforts to prevent and/or respond to future critical incidents and terrorist attacks.

Appendix

What follows is an eight-point action plan, based on one developed by Maryland Lt. Gov. Kathleen Kennedy Townsend, for state, county, and local governments to consider when providing for the domestic defense of their communities.

- Action 1:** Appoint a person to coordinate all planning and implementation efforts.
- Action 2:** Develop a comprehensive plan that identifies potential threats, articulates a coordinated strategy to confront those threats, and identifies budgetary and other funding requirements.
- Action 3:** Use technology to promote information sharing by linking the independent wireless and data systems currently in use by federal, state, county, local, and private entities.
- Action 4:** Establish information and referral services for health care and social service programs that allow government and non-government personnel to obtain referrals by either calling a single phone number or using the Internet. This capability will make it

easier for people in need to obtain appropriate care. It will also divert non-emergency traffic from 9-1-1 systems.

Action 5: Conduct a review of the 9-1-1 infrastructure to determine whether it is adequate in light of current and anticipated demand. This review should specifically examine issues related to the proliferation of cellular telephones, staffing, and system capacity.

Action 6: Take steps to mobilize local communities to work with authorities to prevent future acts of domestic terrorism. Community residents and public safety agencies are dealing with a new environment of alerts and threats. Each must walk a fine line to ensure heightened awareness without causing unnecessary alarm. State and local governments should identify appropriate trainings to enhance the relationship between citizens and public safety agencies in these new circumstances.

Action 7: Establish a public health information network that will assist in the identification and response to both naturally occurring disease outbreaks and biological and/or chemical weapon attacks. The network should be an Internet-based, secure information system that links emergency, urgent-care, and other appropriate health care-related entities and facilities so that states are prepared to:

- recognize an outbreak of an emerging disease;
- circulate information to physicians, nurses, county and local emergency medical systems, and other appropriate health-care providers;
- support individual efforts to make a rapid assessment of likely diagnosis; and
- make decisions as to the appropriate allocation of scarce resources, such as antibiotics, antivirals, and vaccines.

Action 8: Establish appropriate specialized training programs for health care providers, first responders, and other public safety personnel.

John D. Cohen is president and CEO of PSComm, LLC, and director of the Progressive Policy Institute's Community Crime Fighting Project. He also serves as a special advisor on critical infrastructure to Maryland's Governor's Cabinet Council for Crime and Juvenile Justice.

John Adams Hurson is a member of the Maryland House of Delegates, where he serves as chairman of the Environmental Matters Committee.

For further information about PPI publications, please call the publications department at 202-547-0001, write: Progressive Policy Institute, 600 Pennsylvania Ave., S.E., Suite 400, Washington, DC 20003, or visit PPI's site on the World Wide Web at: <http://www.ppionline.org/>.

¹ As time has passed since the attacks the Nation's efforts in Afghanistan contrasted with domestic efforts that were often perceived as disjointed and unorganized. A number of state and county health officials have criticized the response to the recent anthrax cases by the Center for Disease Control and the Department of Health and Human Services. Some local law enforcement officials claim that federal authorities are failing to share information and are asking them to engage in tasks that were illegal under state law. Finally, the Administration has issued a number of "alerts" warning of undefined attacks to occur at unknown times.

² While state, county and local efforts have focused on law enforcement, fire/EMS, health care, and social service that serve as the front line of the efforts to protect our communities, in Washington, the Bush Administration has focused primarily on expanding the detention and surveillance authorities of federal agencies igniting a debate between the Administration and civil libertarians. The Administration has created military tribunals to try non-citizen suspects of terrorism. Currently, more than 1,000 Arab-Americans and native Middle Easterners have been detained by authorities as part of the national terrorist investigation raising questions of Habeas Corpus. Wiretap authorities have been expanded and federal officials have indicated that conversations between prisoners and their lawyers may be monitored. As a result, many civil rights organizations and some in Congress have begun to express concern over of the Bush Administration's focus regarding protection of the homeland and its citizens.

³ The governors of both California and Florida have called for the creation of statewide databases to support anti-terrorism law enforcement efforts.