Heritage Lectures

Published by The Heritage Foundation

No. 812
Delivered October 22, 2003

November 20, 2003

Preparing Responders to Respond: The Challenges to Emergency Preparedness in the 21st Century

James Jay Carafano, Ph.D.

Thousands of responders per day swarmed over the World Trade Center site in the wake of the September 11 terrorist strikes. A massive and complex undertaking, the response to the attacks in New York only begins to suggest the magnitude and scope of the nation's emergency responder needs.

To deal with future transnational terrorist threats, the United States requires a truly national emergency response system that more fully incorporates federal, state, local, and private-sector capabilities. I would like to outline the scope of the challenge we face and the essential requirements for building a national response system capable of responding to these challenges.

Who Should Be Included in the National Emergency Response System?

There is little common appreciation of all the personnel and services comprising the national response capabilities that could be called on to deal with a terrorist attack. A term in common usage, *first responders*, usually refers to law enforcement, fire, and emergency medical personnel.[1]

These responders, however, are not the only assets that may be required in the aftermath of a strike on the homeland. In contrast, the more appropriate term, *emergency responders*, comprises all personnel within a community that might be needed in the event of a natural or technological (man-made) disaster or terrorist incident.[2]

Talking Points

- To deal with future transnational terrorist threats, the United States requires a truly national emergency response system that more fully incorporates federal, state, local, and private-sector capabilities.
- Emergency preparedness and response includes the preparation, response, and recovery from a terrorist attack, including planning, logistical support, maintenance and diagnostics, training, and management as well as supporting the actual activities at a disaster site and post-recovery after the incident.
- National emergency response is a strategic problem, and at the strategic level, thought should always precede action. Spending money without an overarching systems architecture and a comprehensive acquisition program will be both wasteful and counterproductive.

This paper, in its entirety, can be found at:
www.heritage.org/homelandsecurity/hl812.cfm

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

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

The Homeland Security Act of 2002 defines emergency response providers as including "federal, state, and local public safety, law enforcement, emergency response, emergency medical (including hospital emergency facilities), and related personnel, agencies, and authorities."[3] These responders might include hazardous materials response teams, urban search and rescue assets, community emergency response teams, anti-terrorism units, special weapons and tactics teams, bomb squads, emergency management officials, municipal agencies, and private organizations responsible for transportation, communications, medical services, public health, disaster assistance, public works, and construction.

While the emergency response needs of fire, police, and emergency medical personnel have received considerable attention since the 9/11 terrorist attacks,[4] the requirements of other support groups have frequently been overlooked. For example, public health systems and national urban search are both assets widely regarded as essential to emergency response. Both lack sufficient assets to respond to national emergencies.[5]

The needs of responders in the private sector have received even less attention. For example, in the wake of the 9/11 attacks, the World Trade Center site required about 10,000 skilled support personnel (heavy equipment operators, truck drivers, iron workers, carpenters, and laborers) per day during the initial search and cleanup period.[6] Their operations were essential to the response and entailed significant health and safety risks.[7]

In addition to commercial assets, private nonprofit, nongovernmental groups (NGOs), such as the Red Cross, can also play an important role in emergency response.

Another category of resources frequently overlooked in needs assessments are the response assets required to deal with agricultural emergencies either threatening the U.S. food supply or potentially as source of human infectious disease. Animal diseases, for example, can present a serious risk to humans.

Many diseases can infect multiple hosts. Three-quarters of emerging human pathogens are zoonotic; in other words, they can be readily transmitted back and forth between humans, domesticated animals, and wildlife. Even if animal diseases cannot infect humans, they may have fearful economic impact.[8]

While infectious disease is an ever-present danger in a globalized world, the possibility of terrorists intentionally introducing vectors or contagions to foster the spread of disease introduces an added dimension to the danger. Thus, agricultural response assets could well be an important component of the consequence management system required to meet the threat of terrorist attacks.[9]

Finally, in addition to state and local assets and private-sector assistance, emergency responders

1. See, for example, Report No. 107–295, *First Responder Terrorism Preparedness Act of 2002*, report to accompany S. 2664, Committee on Environment and Public Works, U.S. Senate, 107th Cong., 2nd Sess., October 2002, p. 5. There is, however, no common definition of first responders. For example, the national homeland security strategy refers to first responders as police, fire, emergency medical providers, public works personnel, and emergency management officials. See *National Strategy for Homeland Security*, The White House, Office of Homeland Security, July 2002, pp. x, 3.
2. Tom LaTourrette, D. J. Peterson, James T. Bartis, Brian A. Jackson, and Ari Houser, *Protecting Emergency Responders, Vol. 2: Community Views of Safety and Health Risks and Personal Protection Needs* (Santa Monica, Cal.: RAND, 2003), p. 7.
3. PL 107–296, Sec. 2(6).
4. See, for example, Brian A. Jackson, D. J. Peterson, James T. Bartis, Tom LaTourrette, Irene Brahmakulam, Ari Houser and Jerry Sollinger, *Protecting Emergency Responders: Lessons Learned from Terrorist Attacks* (Arlington, Va.: RAND Science and Technology Institute, n.d.), proceedings of a conference held on December 9–11, 2001.
5. Council on Foreign Relations, *Emergency Responders: Dangerously Underfunded, Drastically Unprepared: Report of an Independent Task Force Sponsored by the Council on Foreign Relations* (New York: Council on Foreign Relations, 2003), p. 35.
6. *Ibid.*, p. 39.
7. Bruce Lippy and Kerry Murray, "The Nation's Forgotten Responders," National Clearinghouse for Worker Safety and Health Training," December 14, 2002, p. 9.

could include a range of federal capabilities such as Army and Air National Guard and Reserve forces and the Marine Corps Chemical-Biological Incident Response Force as well as a range of federal response teams such as Domestic Emergency Support Teams, Disaster Medical Assistance Teams, Coast Guard National Strike Teams, and Nuclear Incident Response Teams. Their needs and capacity to integrate into the overall national response system also deserve consideration.

While it is believed that about 2.3 million fire, police, and emergency medical personnel might be considered first responders, these numbers do not suggest the full scope of the national response force. Some have estimated that the broader public emergency response community could be as many as 9 million to 10 million.[10] In addition to professional responders and volunteers, there are about 6.5 million skilled construction workers in the United States who could be called up to respond in the wake of a disaster. Indeed, the sheer number of responders dictates the need for a more integrated structure to coordinate and prioritize the activities of multiple response entities.

In addition, the tasks that a national emergency response system would be required to perform are more complex than simply aiding victims at the scene of a disaster. Emergency preparedness and response includes the preparation, response, and recovery from a terrorist attack, including planning, logistical support, maintenance and diagnostics, training, and management as well as supporting the actual activities at a disaster site and post-recovery after the incident.[11]

Understanding the Responder Environment

Another reason responder needs have been "underdetermined" is that they have been based largely on experiences gained from responding to natural and man-made disasters, which may not be an accurate predictor of conditions responders could face in a determined, protracted terrorist campaign.

One distinction between responding to deliberate attacks and responding to natural or technological disasters is that a scene could become an intentional hostile environment for responders. In order to exacerbate physical and psychological casualties, terrorists may deliberately target emergency response capabilities.

For example, terrorists could well use "secondary devices" specifically intended to harm first responders and civilian onlookers. Explosives are commonly used for this purpose,[12] but other weapons might be employed as well. Employing small amounts of various chemical, biological, toxin, or radiological agents in the ancillary strikes against first responders might further confuse a coordinated response.

Follow-on terrorist strikes may not be limited to the initial attack site. To complicate consequence management, attacks might be launched at hospitals, police stations, and emergency operations centers. Many state and city emergency operations centers are particularly vulnerable. Often, they lack physical security protection and redundant communications. Back-up centers and mobile command posts usually do not exist.[13]

8. For example, the costs of responding to an outbreak of foot and mouth disease in Great Britain and the resultant loss of productivity amounted to $11.6 billion. "Dissecting the Challenge of Mad Cow & Foot-and-Mouth Disease," *Agricultural Outlook*, August 2001, p. 4.
9. Identified by FEMA as an area that needs improvement. See Federal Emergency Management Administration, *State Capability Assessment for Readiness*, December 10, 1997, p. 11.
10. See, for example, Joseph J. Collins, *Training America's Emergency Responders: A Report on the Dept. of Justice's Center for Domestic Preparedness and The U.S. Public Health Service's Noble Training Center, Fort McClellan, Anniston, Alabama*, Center for Strategic and International Studies, July 2000, at *www.csis.org/homeland/reports/FirstResponders.html*.
11. *Science and Technology for Army Homeland Security*, Report 1 (Washington, D.C.: National Academies Press, 2003), pp. 93–94.
12. Paul M. Maniscalco and Hank T. Christen, *Understanding Terrorism and Managing the Consequences* (Upper Saddle River, N.J.: Prentice Hall, 2002), p. 228.
13. Committee on Science and Technology for Countering Terrorism, *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism* (Washington, D.C.: National Academy Press, 2002), pp. 8-2, 8-3.

For example, the New York City Emergency Operations Center was on the 23rd floor of 7 World Trade Center. When the building was destroyed during the 9/11 attacks, the city had no adequate secondary command and control capability available. It took three days to reconstitute all the functions and capabilities lost by the destruction of the emergency operations center.[14] In the future, terrorists might deliberately attack emergency operations centers to replicate such outcomes.

In addition, attacks on emergency responders might not be limited to physical strikes. Terrorists could also deliberately target command and control capabilities.

Some attacks may focus on computer information systems. For example, in 1992, the London Ambulance Service installed a faulty computer dispatch service. Delays resulting from dispatching snafus resulted allegedly in the deaths of 20–30 patients. An intentional disruption of computer dispatching services during a crisis might result in even far greater chaos and disruption. Meanwhile the Internet, as was the case after the 9/11 attacks, could be employed to spread rumors and disinformation or be the target of denial-of-service attacks.[15] In fact, this should be expected as a matter of course.

The increasing likelihood of cyber strikes following physical attacks appears to be becoming an established trend.[16] Additionally, as after the September 11 strikes,[17] an attack would likely generate unprecedented local levels of user demand, severely stressing servers and some Web sites, such as popular news portals, and restricting emergency responder access to critical Web-based resources.

Alternatively, electronic jamming might be used to interrupt emergency frequencies; defeat detection, early warning, and monitoring systems; or attack critical infrastructure. Any form of electromagnetic radiation from satellite television transmissions to wireless networks and satellite-based global positioning system (GPS) signals is a potential target for attack.

GPS, for example, uses very low-power signals, which makes it particularly vulnerable to jamming. GPS is also susceptible to spoofing and broadcast signals with deliberately misleading information. In fact, the vulnerability of the GPS L1 civil signal is a serious problem. GPS is heavily relied upon by the commercial sector. Loss of GPS is a threat to civil transportation, which uses its signals for navigation as well as communications, data processing, and Internet services that rely on the GPS timing signal.[18]

14. James Kendra and Tricia Wachtendorf, "Elements of Resilience in the World Trade Center Attack," University of Delaware, Disaster Research Center, n.d., pp. 6–9, at *www.udel.edu/DRC*. See also Jackson *et al.*, *Protecting Emergency Responders: Lessons Learned from Terrorist Attacks*. Significant controversy remains over the cause of the breakdown in communications during rescue efforts in the north tower of the World Trade Center after the September 11 attacks. Some held that the repeater installed in the building, a device specifically designed to boost the radio transmissions of first responders inside the structure, failed. Others claim that human error may account for communication breakdowns. Nevertheless, as a result of interrupted signals, some emergency workers were not evacuated before the building's collapse. See *Increasing the Fire Department of New York's Preparedness* (New York: McKinsey and Company, 2002), p. 7, at *www.nyc.gov/html/fdny/html/mck_report/toc.html*, and Jim Dwyer and Kevin Flynn, "9/11 Tape Raises Added Questions on Radio Failures," *The New York Times*, November 9, 2002, p. A1.
15. National Infrastructure Protection Center, "Cyber Protests Related to the War on Terrorism: The Current Threat," November 2001, at *www.nipc.gov/publications/nipcpub/cyberprotests1101.pdf*. This report concluded that post-9/11 illicit computer activity was not particularly damaging.
16. "Cyber Attacks During the War on Terrorism: A Predictive Analysis," Institute for Security and Technology Studies, September 22, 2001, p. 1.
17. *The Internet Under Crisis Conditions: Learning from September 11* (Washington, D.C.: National Academies Press, 2002), p. 2.
18. *Vulnerability Assessment of the Transportation Infrastructure Relying on Global Positioning System Final Report*, John A. Volpe National Transportation Systems Center, August 2001, p. ES5. The findings of this report contrasted with an earlier study, conducted by Johns Hopkins University, which concluded that the application of anti-jamming technologies could reduce the risk of deliberate jamming as a potential threat to civil aviation. This study, however, relied heavily on simulations and did not examine potential dangers to a wide range of critical infrastructure. See T. M. Corrigan *et al.*, *GPS Risk Assessment Study: The Final Report*, Johns Hopkins University Applied Physics Laboratory, January 1999, p. 1-1.

Jamming might be employed after a bombing to incapacitate radios and cell phones in a local area, complicating efforts by emergency responders and exacerbating fear in the civilian population. In addition, other more exotic means may be used to disrupt communications using wire, cable, and fiber-optic lines.[19]

To further stress responder capabilities, terrorists may conduct simultaneous or near-simultaneous attacks. Such attacks might be designed not only to increase psychological casualties, but also to complicate the challenge of providing support to several incidents at the same time. Finally, terrorists may employ nuclear, chemical, or biological weapons that might inflict casualties on a massive scale, which could quickly overwhelm the capacity of responders.

In addition to the threat of additional or massive attacks, responders will have to deal with the demanding conditions and requirements that will be resident in responding to any terrorist strike. One major command and control challenge that responders will likely face is the problem of convergence.

Convergence is a phenomenon that occurs when people, goods, and services are spontaneously mobilized and sent into a disaster-stricken area.[20] Although convergence may have beneficial effects, like rushing resources to the scene of a crisis, it can also lead to congestion, create confusion, hinder the delivery of aid, compromise security, and waste scarce resources.

This proved to be a major concern during the response to the September 11 attack on the World Trade Center. When the first tower was struck, firemen, policemen, and emergency medical technicians from all over the metropolitan area streamed to the site, leaving other parts of the city vulnerable and, after the towers collapsed, creating tremendous problems in accounting for emergency personnel.[21] Additionally, in the days following the tragedy, many organizations deployed assets to New York City only to find they were unnecessary.[22]

In contrast to the problem of convergence, virtually every large-scale exercise or response experiences problems in agency notification, mobilization, information management, communication systems, and administrative and logistical support. Organizations have particular difficulty in optimizing flexibility and the capacity to decentralize operations and conduct rapid problem solving, often a key requirement for responding effectively to major disasters.[23]

Emergency response operations are also frequently plagued by a lack of information sharing and confusion over responsibilities among policymakers, law enforcement, emergency managers,

19. One potential tactic might employ a power generator capable of emitting an electromagnetic pulse that could permanently incapacitate computers and other electrical systems. Russian experiments investigating the potential of such generators concluded that electromagnetic pulses in the range of 10–100 kilovolts, linked to a power supply and grounding circuits in a five-story building, would be capable of damaging computers and incapacitating security systems. Yury V. Parfyonov, "Electromagnetic Terrorism," in *High-Impact Terrorism: Proceedings of a Russian–American Workshop* (Washington, D.C.: National Academy Press, 2002), p. 85. Little is published about the likelihood of turning such devices into practical weapons, but the potential suggests greater thought should be given to investigating possible threats and that perhaps more attention should be paid to the security of grounding systems and power cables, particularly for computer, power generation and transmission, and telecommunications assets related to critical infrastructure.

20. For a discussion of convergence, see Julie L. Demuth, *Countering Terrorism: Lessons Learned from Natural and Technological Disasters* (Washington, D.C.: National Academy of Sciences, 2002), p. 7. See also Jackson *et al.*, *Protecting Emergency Responders: Lessons Learned from Terrorist Attacks*, p. xiii.

21. The problem of organizations, units, and individuals "self-dispatching" themselves without the knowledge or permission of the on-scene incident commander was also a problem at the site of the attack on the Pentagon. Arlington County, *After Action Report*, p. 12.

22. For example, the U.S. Joint Forces Command's JTF-Civil Support deployed a liaison team to New York City approximately three days after the 9/11 attacks. The city requested few DoD resources, and the task force soon withdrew and handed coordination for the civil support mission over to a DoD regional Defense Coordinating Officer. New York's WMD-Civil Support Team also deployed to the city days after the event and did not play a significant role. See "JTF-CS Response to Terrorist Attacks on 11 September 2001," Joint Center for Lessons Learned *Quarterly Bulletin*, December 2001, pp. 11–12.

first responders, public health workers, physicians, nonprofit organizations, and federal agencies. The necessity for speed can exacerbate the coordination challenge.

Effectively negating threats in many cases requires a rapid response capability, and operating on compressed timelines leaves little room for miscues in coordination.[24] One significant requirement, for example, is quickly emplacing an incident response structure that can detect and assess threats and mobilize appropriate resources. In particular, for a chemical or biological attack, actions taken in the first hours to identify, contain, and treat victims may significantly reduce the scope of casualties.

Also complicating an emergency response is that many first responders such as uniformed police are ill-organized and equipped to rapidly address terrorist attacks that might require assets or equipment not normally employed during a tour of duty. Police, for example, lack capacity to carry a lot of additional emergency response equipment in the trunk of patrol cars. Officers on foot, bicycle, or equine patrol have even less capacity. Undercover agents and antiterrorism squads trying to blend into their surroundings and trying to appear inconspicuous have problems with carrying additional equipment as well.[25]

Some jurisdictions address the problem of lack of available equipment by caching protective gear at strategic locations. The pace of response is then driven by their capacity to identify threats and dispatch equipment to the scene.

Even when personal protective equipment is available, first responders find they have significant limitations. Clothing, gloves, and masks are bulky, heavy, and demanding on physical labor. Most protective gear is too uncomfortable for extended wear. Routine activities such as communicating, pushing buttons, and observing surroundings cannot be easily accomplished in protective gear.[26]

Finally, it is often extremely difficult to extend the situational awareness that must be extant in the emergency response system to the frontline responders. For example, fire personnel need to know hydrant and standpipe locations, as well as utility and building designs and hazardous material inventories. Often, critical information is stored in locations or formats (e.g., paper records) that prevent them from being readily on hand.

Taken together, these challenges will present enormous obstacles to responders that may well have to deal with multiple catastrophic attacks requiring the integrating of multiple assets across multiple regions and multiple layers of government. To effectively address such threats, the United States will require a much more robust and integrated national response system.

Requirements for a National Emergency Response System

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

Network-centric operations generate increased operational effectiveness by networking sensors, decision makers, and emergency responders to achieve shared awareness, increased speed of command, higher tempo of operations, greater efficiency, increased security and safety, reduced vulnerability to potential hostile action, and a degree of self-synchronization. In essence, this means linking knowl-

23. For a discussion on the importance of decentralized execution and flexibility, see Kathleen J. Tierney, "Disaster Preparedness and Response: Research Findings and Guidance from the Social Science Literature," University of Delaware, Disaster Research Center, n.d., pp. 13–14, at *www.udel.edu/DRC*.

24. For example, an analysis that modeled the economic consequences of a biological attack found that the speed of the response was the single most important variable in reducing casualties. Arnold F. Kaufmann *et al.*, "The Economic Impact of Bioterrorist Attack: Are Prevention and Postattack Intervention Programs Justifiable?" *Emerging Infectious Diseases*, April–June 1997, at *www.cdc.gov/ncidod/eid/vol3no2/kaufman.htm*.

25. LaTourrette *et al.*, *Protecting Emergency Responders, Vol. 2: Community Views of Safety and Health Risks and Personal Protection Needs*, p. 53.

26. Jackson *et al.*, *Protecting Emergency Responders: Lessons Learned from Terrorist Attacks*, pp. xii, 8.

edgeable entities in the response to emergencies from the local to the national level.

Such a system might produce significant efficiencies in terms of sharing skills, knowledge, and scarce high-value assets, building capacity and redundancy in the national emergency response system, as well as gaining the synergy of providing a common operating picture to all responders and being able to readily share information. Network-centric systems might be especially valuable for responding to large-scale or multiple weapons of mass destruction attacks, where responders will have to surge capacity quickly, adapt to difficult and chaotic conditions, and respond to unforeseen requirements.[27]

In particular, three aspects of a system-of-systems approach could be essential to improving national emergency response capabilities.

- One is "just in time" logistics, the ability to ensure that support arrives at the scene precisely when it is needed rather than having resources stockpiled or requiring responders to carry equipment with then all the time.
- The second is "situational awareness." Emergency responders may rely on early warning to minimize exposure to risks and decrease requirements for personal protective equipment and other support assets.
- Third, enhanced situational awareness will provide for better command and control, addressing issues such as managing convergence and coordinating operations managed by multiple agencies and levels of government.

Putting First Things First

While building a national system-of-systems emergency response system is critical to the long-term security of the nation, erecting this robust capability will take time and serious effort. The first step cannot be to simply go out spend a lot more money. National emergency response is a strategic problem, and at the strategic level, thought should always precede action. Spending money without an overarching systems architecture and a comprehensive acquisition program will be both wasteful and counterproductive.

Spending on homeland security has already doubled since the September 11 attacks. For now, stabilizing funding at current levels appears prudent. While enormous security challenges remain, allowing the many agencies involved some time to absorb these large increases makes sense.

Once a firm foundation for the nation's homeland security architecture is established, increased funding may be needed in future years. There is little room for complacency in the face of global terrorism in the 21st century.

—James J. Carafano, Ph.D., is Senior Research Fellow for National Security and Homeland Security in the Kathryn and Shelby Cullom Davis Institute for International Studies at The Heritage Foundation. These remarks were prepared for a panel on "The State of Homeland Security Two Years After the Debacle," conducted by the Criminal Justice and Fire Science Programs, Montgomery County Community College, Blue Bell, Pennsylvania, on October 22, 2003.

27. For the scope of assets that might be required in a weapons of mass destruction incident, see Eric V. Larson and John E. Peters, *Preparing the U.S. Army for Homeland Security: Concepts, Issues, and Options* (Washington, D.C.: RAND, 2001), pp. 60–61, at *www.rand.org/publications/MR/MR1251*.