BEWARE OF ROGUE VOLUNTEERS

Emergency response officials were recently warned to be vigilant of rogue volunteers—the overzealous good Samaritans who flock to disaster sites, then refuse to step aside for professionals.

“When it comes time to let go, they won’t,” said Anne Peterson, US policy studies professor at the University of Washington, who spoke at the World Conference on Disaster Management in Toronto this past June. “You can guarantee that they won’t go away. They consider themselves immune.”

Such was the case at the World Trade Center, where leaders of the thousands-strong volunteer brigades were ordered away by police, but refused, saying, “Hey, I’m a volunteer; you’re not the boss of me. Where were you when the disaster struck?” This indignance is the hallmark of a rogue volunteer, Peterson said.

The genesis of a rogue volunteer is simple, but often overlooked by emergency planners. Initially, at disaster scenes, a lack of formal direction brings out natural leaders among the volunteers. Later, though, the stress of relief work turns these leaders into rogues. They come to see themselves as peers with the police and emergency workers, but they respect the rescue mission more than its proper leaders. This leads them to ignore rules and put others in danger, Peterson said, adding that on 9/11, the failure of police to bring the disaster scene under control quickly was what gave volunteers the opportunity to rise to power and ultimately “go rogue.”

“It may seem strange, but only the most capable people will go rogue,” Peterson said. “They get to the scene first. They size it up and take control, and no one is around to direct their efforts.”

Peterson’s analysis of the city’s response to 9/11 was written in cooperation with Sean Nolan, an official with the New York Office of Emergency Management (OEM), who was on duty that day.

Anecdotal evidence from disaster scenes suggests it takes even the best emergency planners about three days to gain operational control over a disaster scene, from ensuring reliable supply chains to finding adequate staff.

In the meantime, Peterson said, volunteers who show up on short notice tend to get a lot done. In the case of the attack on the World Trade Center, New York’s OEM took 72 hours to establish a control center, by which time three volunteers, who were all managers in their day-to-day jobs, had taken charge of supplies, vehicles, and manpower. “They passed themselves off as full-fledged OEM officials,” she said. “Because they were volunteers, they considered themselves immune from any punitive sanctions.”

In due course, however, their lack of professionalism appeared. One used his cellphone to call OEM officials in the middle of the night, claiming the other two had ganged up on him and would not let him back into the control center. However, when it was clear they had to go, police were so emotional and grateful for their help they could not banish the three volunteers from the site. It took the National Guard to finally send them home.

To offset the threat of the rogue volunteer, Peterson advised officials to plan for volunteer management in a crisis, and perhaps to set up a toll-free number to coordinate their recruitment.

One audience member, who had worked at the World Trade Center site, said police and firefighters also go rogue on occasion, so lack of training might not be a key factor. Another praised the volunteers, saying they got the hard work done while the OEM was struggling to regroup. Another pointed out that natural leaders are essential to volunteerism, and should not be vilified as “rogues.” Instead, they might be tactfully pushed out with ceremonial thank-yous from city officials. (Source: National Post, June 25, 2003.)
Wireless Communications
The Choice for Post-9/11 World

Paul Kolodzy and colleagues of the Stevens Institute of Technology’s Wireless Network Security Center, Hoboken, NJ, think wireless technology is the best solution to the communications knots that plague emergency responders—an issue that came to the fore on 9/11.

With current communications systems, fire and police officials operating on different frequencies and using different terminology run into trouble trying to coordinate actions. Moreover, these frequencies are often congested. Weak and overtaxed radio transmissions were a key reason commanders were unable to track firefighters inside the World Trade Center and warn them the towers were about to collapse.

In spite of 9/11, the situation hasn’t improved much over the last couple of years. “Don’t forget,” says Vincent Stile, policy radio director for Suffolk County, NY, and president of the Association of Public Safety Communications Officials. “We’re government, and government doesn’t move that fast.”

Agencies have improved their methods of handling regional emergencies, but the team at the Stevens Institute says there are better communications choices for situations where lives are at stake. By weaving several network technologies into one system, the team hopes to give public-safety officials a much-needed tool for coordinating emergency response across jurisdictions.

“We’re trying to link a network of networks,” said Kolodzy, a former wireless expert at the Pentagon and the FCC. “There’s a huge amount of infrastructure out there. Why can’t we somehow exploit existing infrastructure instead of having to build yet another?”

Software-defined radios are an example of a new, more efficient use of existing technologies. Police radios can be programmed to scan open frequencies to avoid interference while doubling as cell phones. “Mesh” or “ad hoc” networking, developed by the military, is another option; these networks involve individual radio devices that serve not only as receivers but also as relay points to pass along information. With this type of network, firefighters deep in large buildings whose signals don’t reach the outside can contact other firefighters nearby, who relay the message onward until it reaches the intended target.

Mesh networks also provide real-time coordinates of their users’ locations—even indoors. This ability is “sort of the Holy Grail for first responders,” said Nader Moayeri, a wireless specialist at the National Institute of Standards and Technology. “There is nothing [out there] like that right now.” Moayeri’s team is working on a wireless system that allows emergency crews to talk to each other, share pictures, and even make phone calls via the Internet.

All the new technologies in the pipeline will take time and money to implement, but the long-term benefits in terms of coordination and saving lives will be well worth the investment, researchers say. (Source: Associated Press, September 12, 2003.)

Power Grid Vulnerable to Viruses, Hackers

After the August blackouts in the Northeast, replacing the nation’s aging power systems with the latest in digital technology became a priority for utility companies. Experts warn, however, that high-tech upgrades make the power grid vulnerable to a new type of threat: computer viruses and hackers that could shut down substations, cities, or even entire states with a few keystrokes.

US, Canadian, and British researchers are already working to identify weaknesses in the digital relay networks, which have been gradually replacing outdated systems throughout North America. “I know enough about where the holes are,” said Eric Byres, cybersecurity researcher for critical infrastructure at the British Columbia Institute of Technology in Vancouver. “My team and I could shut down the grid. Not the whole North American grid, but a state? Sure.”

Experts have been working to safeguard against electronic sabotage since 1998, when test hackers at the US National Security Agency demonstrated how easily they could tamper with power networks. However, the spike in upgrades after the blackouts means experts will have a tough time keeping ahead of potential tampering.

Computer viruses are another new worry. The Blaster worm, which affected 500,000 computers
worldwide in August, may have been a factor in the Northeast blackouts, possibly by blocking communications. According to Joe Weiss, a utility control system expert at Kema Consulting in Cupertino, CA, “It didn’t cause what happened, but it could’ve exacerbated what happened.”

FirstEnergy Corporation, the Ohio utility at the core of the blackout investigation, is conducting research to determine whether computer problems caused by the Blaster worm may have hampered its response to the multiple power failures. The Slammer worm, another internet virus, also took down monitoring computers at FirstEnergy’s idle Davis-Besse nuclear plant, although it caused no outages.

Newer networks running on Microsoft’s operating system are particularly at risk because of its prevalence and its popularity with virus writers. Byres’ team found security vulnerabilities in a crucial computerized control device installed in most Northeast grid substations—a problem the manufacturer has yet to address. “I’ve been trying to get these guys to patch, and they won’t patch it,” he said. “I’ve been on their case for over six months.” Other potential problems involve reprogramming substations’ circuit breakers, diverting power, and overloading neighboring lines.

As with any operation dependent on networked computers, power grid operators will be vulnerable to hackers. “We’re still going to have backdoors no matter how hard we try,” said Gary Seifert, a researcher with the US energy department. “You can’t keep them out, but you hope to slow them down.” (Source: USA Today, September 12, 2003.)

NEW FIRE CHECKLIST DEVELOPED TO MEET CURRENT CMS GUIDELINES

All ambulatory care centers certified by Medicare are required to use a new fire safety checklist to meet the 2000 Life Safety Code. The Accreditation Association for Ambulatory Health Care (AAAHC) has been granted authority by the Centers for Medicare & Medicaid Services (CMS) to survey facilities on behalf of CMS to ensure that the physical environment is up to code.

The Life Safety Code was adopted by the CMS in March 2000. All ambulatory surgical centers are required to meet the code to qualify for reimbursement. The AAAHC adopted the code as part of its own standards shortly thereafter, and created a modified on-site survey for distribution to facilities seeking CMS certification.

The checklist provides a way to review the CMS safety requirements, though it is not all-inclusive, says Stephen Kaufman, RN, director of accreditation services for the AAAHC. However, he adds, it serves as a good guide for both the facility and the surveyor. “All currently accredited, Medicare-certified [ambulatory surgical centers] that are in the AAAHC’s deemed status program have received a copy of the checklist and information about how to proceed.”

Facilities fill out the AAAHC checklist prior to undergoing the CMS survey. The checklist runs through 189 life safety items under the following categories:

- General requirements
- Exiting requirements
- Electrical requirements
- Medical gas and vacuum system requirements
- Fire protection requirements
- Building services requirements
- Operational requirements

Any healthcare facility interested in purchasing the checklist can find it online at the AAAHC’s Web site at www.aaahc.org/products/products.shtml. (Source: healthsafetyinfo.com, October 15, 2003.)

MASSACHUSETTS OFFICIALS RETHINK DISASTER PLANS

For years, residents were taught to respond to a catastrophe such as a natural disaster or nuclear attack by convening in designated shelters in their community. For those who grew up during the Cold War era, evacuation routes and bomb shelters were the way to safety.
But today, EM professionals in the region are preaching a different gospel, worried that people could put themselves at far greater risk by leaving their surroundings in the event of an emergency. With the threat of terrorism now on the minds of even small fire and police departments, the current theory holds that the best response to such an event is for people to take shelter in their own homes.

“The reason for that is evacuation isn’t always the best way to stay safe,” said Joe Cavanaugh, public information officer for the Lincoln, MA, Fire Department. “For example, if there was a chemical spill, you may actually end up driving through a plume of chemicals, so oftentimes it’s safer to keep people where they are—staying indoors, closing windows, turning off fans and ventilation systems.”

While certain situations—such as a gas leak, flooding, or an incoming hurricane—would call for evacuation, more often local authorities will recommend staying put in the event of a nearby emergency. The phrase for this approach, officials say, is “sheltering in place.”

Every community in the state of Massachusetts has an emergency plan that includes provisions for both evacuations and for sheltering in place, said Peter Judge, spokesman for the Massachusetts Emergency Management Agency. But Judge said there would be a greater awareness among residents that taking shelter in one’s surroundings at the time is the preferred response. “I think everyone in emergency management agrees now that we need to do a better job defining what ‘sheltering in place’ means,” he said.

Advances in technology have made the sheltering-in-place approach more feasible. One major advancement is a system, developed by an Indianapolis, IN, firm called Reverse 911, which allows authorities in the community to quickly dial all the homes of residents to deliver recorded instructions during an emergency. Several communities in Massachusetts have Reverse 911 systems. The city of Marlborough, MA, purchased the $27,000 system a year ago, and is able to map out a specific area of town or to narrow it down by street. A computer tracks whether the message was received by a person or was recorded by machine.

“With the cutbacks throughout the departments, we’re able to do more on the computer and telephone,” said Donald E. Cusson, emergency manager for the city. “We don’t have the bodies to go knocking on all the doors,” he said.

Cusson said, however, that there is some concern that unlisted numbers—and those that have registered for the state’s do-not-call list—may unknowingly be blocking the Reverse 911 system. Cusson recommends those individuals contact their public safety departments.