Expecting the Unexpected: The Need for a Networked Terrorism and Disaster Response Strategy

W. David Stephenson and Eric Bonabeau

NOTE: This article first appeared in Homeland Security Affairs, Volume III, No. 1 (February 2007), www.hsaj.org.

INTRODUCTION

Hurricane Katrina focused attention on improving the command-and-control management response to natural disasters and terrorist attacks. But what if the command-and-control approach itself is so fundamentally mismatched to dealing with unpredictable, rapidly-changing circumstances (including the incapacitation of command personnel and technology), commonplace in natural disasters or terrorist attacks, that, even if improved, it is still unequal to the task?

The emphasis placed on improving command and control should instead be focused on creating a new, alternative emergency management approach capitalizing on a combination of new communications technology and the science of social networks and "swarm intelligence" that is fundamentally better matched to the circumstances encountered in disasters. The hallmarks of such a strategy would be flexibility, ease of incorporating situational awareness into decision-making, and the ability of anyone available after a catastrophe to create *ad hoc* strategies with available resources.

Katrina's Lessons

All the major analyses of the failures in preparing for and responding to Hurricane Katrina highlighted management failures at all levels of government.[1] Perhaps most succinct was the House Select Committee's report:

> [D]uring and immediately after Hurricane Katrina made landfall, there were lapses in command and control within each level of government, and between the three levels of government.... The lack of effective command and control, and its impact on unity of command, degraded the relief efforts. [2]

The Department of Homeland Security (DHS) was established and the Federal Emergency Management Agency (FEMA) was put under its aegis in part to improve coordination and delivery of services after a natural disaster or terrorist attack. However, the utter chaos after Hurricane Katrina, both in management and delivery of services, demonstrated the flaws in the secretariat's structure and strategy: DHS overall, and FEMA in particular, was inflexible, lacked redundancy, was slow to react to changing conditions, and – when the ordinary chain of command was interrupted – individual components were not able to adapt and become self-directed. In New Orleans, vital supplies and personnel did not arrive until three days after the hurricane made landfall.[3]

While most recommendations in the four major analyses of Katrina focused on how to strengthen traditional command-and-control management, this essay concentrates instead on how to plan for the all-too-likely situations following a disaster or terrorist attack (such as Katrina or the World Trade Center on 9/11) when circumstances arise that could not be visualized in advance, and responders are themselves victims or their ordinary command structure is compromised. In these situations, whoever survives and is available must cobble together *ad hoc* solutions in response to rapidly-evolving situations.

ALTERNATIVE MODEL: NETWARS

A model for an effective alternative to command-and-control in disasters or terrorist attacks is found in a 1996 study for the Defense Department, *The Advent of Netwar.*[4] In it, John Arquilla and David Ronfeldt describe the rise of networked enemies "[who are] organized along networked lines or employ networks for operational control and other communications."[5] They claim the information revolution encourages this shift.

Arquilla and Ronfeldt argue this new type of enemy requires rethinking U.S. defense strategy because it gives small groups who communicate, coordinate, and conduct their campaigns in a networked manner, without a precise central command, an advantage over hierarchical opponents.[6] Logically, fighting a networked enemy requires the U.S. to form networks to fight networks, decentralizing operational decision-making authority.

In recent years the Department of Defense has begun to develop and deploy such strategies under names such as network-centric warfare or "power to the edge" (although the approach is by no means universally accepted).

This essay examines the possibility of extending the networked concept to respond to domestic terror attacks or natural disasters. Since domestic terror cells are likely to employ the same kind of loosely-knit networks as their Middle Eastern counterparts, the "netwar" approach would seem directly relevant when responding to a terrorist attack at home.

At the same time, natural disasters whose effects cannot be predicted accurately from past occurrences, which involve rapidly-changing circumstances, and which exact their greatest toll on the most vulnerable, might be seen as the natural world's analog to terrorist networks, making a flexible, networked strategy also relevant to natural disaster response.

Networked Communication and Science of "Swarm Intelligence" Combine

A combination of two factors – one technological and the other scientific – have emerged during the past twenty years, presenting the potential for a strategy that would not only facilitate flexible disaster and terrorism response, but could actually foster creative, *ad hoc* solutions to unforeseen situations that emerge during a crisis.

The first of these factors is the growing body of scientific understanding of "swarm intelligence" or "emergent behavior." This discipline began with empirical observation of the behavior of social insects such as bees, ants, and termites. Social insects have meager intelligence yet, through collaborative, self-organizing action, create highly-sophisticated structures and collaborative projects. Researchers have created rigorous mathematical formulas to describe the activities of social insects, and are now applying those formulas to human management issues.[7]

The second factor is the development and widespread adoption of networked communications technologies and applications. This includes text messaging and self-organizing, self-healing "mesh" wireless computer networks, which can continue to function when conventional communications infrastructure is damaged and destroyed, and which can be controlled directly by end users without the need for, or control by, central authorities.

Applicability of Swarm Intelligence to Terrorism and Disaster Response

Three characteristics of "swarm intelligence" particularly relevant to emergency management are flexibility, robustness, and self-organization.[8] Most people would agree that all three of those characteristics were missing from the governmental response to Katrina.

The single noteworthy agency exempted from the criticism of governmental response was the U.S. Coast Guard, whose Gulf Coast units did not wait for express authorization to begin search and rescue operations. According to a Government Accountability Office report, "... underpinning these efforts were factors such as the [Coast Guard's] operational principles. These principles promote leadership, accountability, and enable personnel to take responsibility and action, based on relevant authorities and guidance."[9]

Similarly, on 9/11 the only effective response was a classic example of swarm intelligence. A group of total strangers on Flight 93 coalesced (in circumstances when no one would have blamed them for instead dissolving into hysterics) to thwart the hijackers' plan to crash the plane into the Capitol or White House. They exhibited all three characteristics of swarm intelligence in abundance.

Another example is how individuals came together via the Internet to provide a variety of invaluable and reliable information to victims of the tsunami, and, more recently, of Hurricane Katrina. In particular, some of these people took it upon themselves to create the *tsunamihelp* blog and wiki[10]. Later, a core group of those people took the lead in creating the *Katrinahelp* wiki. As one of the *tsunamihelp* volunteers, Dina Mehta, wrote:

> We experienced a near-magical interdependence as we were setting up and establishing this blog. It's not just about the people who were blogging; there [were] a whole lot of volunteers who fed us with links, sent us letters from affected people reaching out for help, others who took on the mantle of editing, sub-groups working on design and template issues, still others quietly contributing by buying up bandwidth and applications and offering up mirror servers, that made the blog more effective. [11]

Mehta accurately describes how individuals participating in a situation that evokes swarm intelligence produce results that are far greater than the sum of their parts. In the case of Katrina, still others spontaneously came together to craft imaginative Google Map mashups (applications combining information from multiple sources) to allow identification of homes in New Orleans[12] and to create unified databases of those needing assistance.[13]

Perhaps the most astonishing examples of swarm intelligence in a recent disaster response situation were the variety of *ad hoc* rescue efforts in New Orleans that Douglas Brinkley described in *The Great Deluge*. Spurred by word of mouth, hundreds of Cajuns spontaneously navigated their small boats to New Orleans in an *ad hoc* citizens' flotilla, the "Cajun Navy," which rescued nearly 4,000 survivors.[14] Reggae singer Michael Knight and his wife Deonne saved approximately 250 people by themselves.[15] Richard Zuschlag, co-founder of Acadian Ambulance Service, used his 200 ambulances, plus medivac helicopters, to evacuate 7,000, while also providing the only reliable emergency communications system.[16]

Networked Personal Communication Devices Foster Swarm Intelligence

These examples demonstrate that swarm intelligence is possible even under the trying circumstances of a terrorist attack or a natural disaster. But does this warrant encouraging swarm intelligence as a formal part of homeland security planning, and, if so, how can it be done?

In part, fostering emergence should be part of the plan because networked personal communications technology has, in effect, already made the choice for us, whether or not officials officially recognize that reality. Just as earlier civilizations used signal fires or semaphores in a disaster, the advances in networked communications, combined with human nature, make it almost inevitable that individuals during a disaster will automatically turn to the increasing array of electronics they use every day to reach out to others for comfort and mutual assistance.

Equally important but less understood by decision makers, and unlike landline phones or the broadcast media, these new communication devices are themselves increasingly networked, and those networks are self-organizing, and self-healing. In many cases (such as mesh networks that were originally developed for the military in battlefield conditions and now are being used by civilians) the networks do not require any kind of external networking. By simply turning on two or more devices equipped with mesh network cards (or free software from the CUWiN project),[17]the network self-organizes.

(It is noteworthy that the One Laptop Per Child project, which aims to distribute millions of laptops costing $100 each to impoverished schoolchildren worldwide, believes the ability to create instant networks is so important that it includes a built-in mesh capability in each computer.[18] Equally important, if one or more nodes are disabled, the network can still function; it simply routes around the interruption.)

Even cell phones still functioned during both 9/11 in Manhattan and in New Orleans during Katrina, for those who knew how to use them correctly under the circumstances. Although voice mails would not go through, packet- and IP-based SMS text messages did, because they use minimal bandwidth and can route around obstacles.[19]

Authorities may have little choice in factoring these communication devices into emergency communication strategies because so many are controlled by end users who will use them in a disaster. Used inappropriately and without guidance, these devices could consume all available bandwidth and crash networks. By contrast, if officials provide guidance before a disaster on how to use networked communications appropriately, those communication devices could be an important expansion of the new phenomenon of “sousveillance” (i.e., the opposite of surveillance). Sousveillance is frequently associated with using camera phones or video cameras to document official malfeasance.[20] In disasters or after terrorist attacks, it could also refer to individuals using those devices not only to spread information among survivors, but actually to provide information about damage, those in need of assistance, etc. that could be incorporated into the situational awareness network. If disaster processes were revamped on the basis of systems dynamics to include built-in feedback loops, this information could be fed into the system for rapid correction.

It is one thing for individuals to have communication devices they can use for mutual benefit during a crisis. Having a large number of individuals – in close physical or virtual proximity – merely coexisting does not assure swarm intelligence. For swarm intelligence to emerge, they must interact.

Wikis and Other Web 2.0 Collaborative Tools

A second related technological development could foster this necessary interaction. These are so-called collaborative software programs, particularly wikis, which are designed specifically to allow participation by a wide range of people on a self-organizing basis. These are frequently referred to as Web 2.0 applications, for which the Web itself is the platform (a critical consideration in a crisis, since the Web does not reside on a single computer that might be unavailable) and which tend to foster collaboration and "harvest collective intelligence."[21]

As has been widely reported,[22] almost any wiki, at any point in time, will contain erroneous information. However, so do the FEMA and DHS websites. The difference is that other users can and will quickly correct these errors – much more rapidly than would happen with an official website. As a result, to this day, the *Katrinahelp* wiki remains the single most comprehensive and authoritative source of information for survivors. Similarly, a recent study demonstrated that the all-volunteer written *Wikipedia* is as, if not more, accurate than the peer-reviewed *Encyclopedia Britannica*.[23] A recent report by the highly-respected Center for Strategic and International Studies, "Wikis, Webs, and Networks: Creating Connections for Conflict-Prone Settings," recommending that governments and NGOs consider using wikis and other social networking applications to deal with what they term "collapsed and fragile states" globally, concluded that "... in many cases, the daily benefits of open information systems [such as wikis] outweigh the potential threats."[24]

Katrinahelp is also a prime example of swarm intelligence. Working in isolation from each other the contributors could never have created its rich content; it was precisely the give-and-take of the collaborative editing process that *made Katrinahelp* so informative.

BASIC STRUCTURE OF A NETWORKED DISASTER AND TERRORISM RESPONSE

We cannot detail the structure of such a networked homeland security system in a paper of this length. However, the basic structure of such a system includes:

- An opt-in system that would allow willing members of the public to become part of the network, both providing and receiving information while preserving non-participants' privacy.
- Legal and technological barriers to capricious use of the system to avoid having it used as a tool for discrimination or petty harassment.
- Coordination of all the components through new "presence" applications that allow creation of instant networks and sharing of real-time, location-based information.[25]
- An effort to involve a variety of commercial applications that are familiar to the general public (so there will be no learning curve if they are used in a crisis, unlike dedicated governmental emergency communications systems that are unfamiliar to the public and must be learned in the midst of a crisis),

particularly ones that serve to create online and physical social networks, thereby fostering “swarm intelligence.”

Portland Connect and Protect Program Shows Network Approach Works

One system already in operation will illustrate how networked communications devices, combined with the applications private-sector entrepreneurs create and refine constantly to exploit these devices’ power (especially applications providing location-based, real-time information that would be critical in a disaster), foster swarm intelligence in emergencies.

Swan Island Networks, the non-profit Regional Alliances for Infrastructure and Network Security (RAINS), and the City of Portland transformed the city’s 911 system to make it truly interactive.[26] The system analyzes and synthesizes incoming warnings, then redistributes them not only to EMTs and police, but also to hospitals, schools and other institutions, as well as to willing members of the general public.

While not part of the original design, participants now communicate with each other as well with central authorities. For example, parole officers send alerts to the school, and hotel managers pass along storm threats (often more rapidly than the official warnings).

> Connect & Protect is now a large conglomeration of overlapping alerts stretching across nine Oregon counties. Each stream of warnings is controlled by the agency that issues it. Fairly strict security features attempt to limit abuse of the warnings – certain categories of calls, such as reports of sexual crimes, are not transmitted publicly, the alerts can’t easily be copied or pasted, anonymity is forbidden.[27]

A *Wired* magazine article about the Connect and Protect program concluded with a paragraph summarizing this essay’s contention as well. A comprehensive terrorism and natural disaster response strategy must include a fall-back approach in the likely situation that circumstances are unprecedented and/or first responders are overwhelmed:

> If national safety – the ability to respond to hurricanes, terrorist attacks, earthquakes – depends on the execution of explicit plans, on soldierly obedience, and on showy security drills, then a decentralized security scheme is useless. But if it depends on improvised reactions to unknown threats, that’s a different story. A deeply textured, unmapped system is hard to bring down. A system that encourages improvisation is quick to recover. Ubiquitous networks of warning may constitute our own asymmetrical advantage, and, like the terrorist networks that occasionally carry out spectacular attacks, their power remains obscure until they're called into action.[28]

As Portland’s Connect and Protect demonstrates, a networked homeland security strategy is feasible today, using existing technology and requiring much less time to create and deploy than some of the costly, dedicated emergency communications systems government is creating. Equally important, by facilitating those three qualities of swarm intelligence needed in a crisis (flexibility, robustness, and self-organization), such a strategy could transform the general public from hopeless victims, waiting for aid that may never come, into self-reliant components of the overall response, able to craft *ad hoc* strategies to respond to fast-changing circumstances.

CONCLUSION

So why is a networked homeland security strategy not under consideration? While executives can relate easily to the flexibility and robustness aspects of swarm intelligence, they may find it harder to deal with the concept of self-organization, probably because that carries with it a loss of their ability to exercise top-down command-and-control.

However, as mentioned earlier, a technological imperative is at work. Due to the potential of networked personal communications devices to function in a crisis, independent of (or despite) a central authority, officials really do not have a choice in embracing a networked disaster and terrorism response strategy. Government has already effectively lost control of the flow of information during emergencies. The public now has the power at their fingertips to network in a disaster – and human nature dictates that they will use it.

Polls have shown that, since Katrina, the public has lost faith in government's ability to protect them.[29] Those same polls show that individuals are taking more steps to prepare to help themselves in a disaster.[30] Government can capitalize on the technology and science of networks and treat the public as full partners in prevention and response, creating the conditions that would directly foster swarm intelligence, or the people may simply take matters into their own hands and circumvent the government during natural disasters and terrorist attacks.

W. David Stephenson is principal, Stephenson Strategies (Medfield, MA). A former corporate crisis and Internet consultant, he specializes in homeland security strategies to empower the general public. He writes a blog on homeland security and is a frequent speaker at conferences.

Eric Bonabeau is chief executive officer and chief scientific officer of Icosystem, (Cambridge, MA) which uses the tools of complexity science and advanced computational techniques to provide software simulation tools for exploring business issues and strategies. He is one of the world's leading experts in complex systems and distributed adaptive problem solving, and spent several years as a research fellow at the Santa Fe Institute. Bonabeau is co-editor-in-chief of the Advances in Complex Systems, *and co-author of* Intelligence Collective, Swarm Intelligence, and Self-Organization in Biological Systems.

[1] The major reports analyzing problems in responding to Katrina include: U.S. House of Representatives, Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina, *A Failure of Initiative: The Final Report of the Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina* (U.S. House of Representatives, 2006); Senate Committee on Homeland Security and Government Affairs, *Hurricane Katrina: a Nation Still Unprepared*, (U.S. Senate, 2006); Frances F. Townsend, *The Federal Response to Hurricane Katrina: Lessons Learned* (White House, 2006); Office of Inspector General, Department of Homeland Security, *A Performance Review of FEMA's Disaster Management Activities in Response to Hurricane Katrina*" (Department of Homeland Security, 2006).

[2] U.S. House of Representatives, *A Failure of Initiative*, 186.

[3] Douglas Brinkley, *The Great Deluge* (New York: Morrow, 2006), 245-51, 635.

[4] John Arquilla and David Ronfeldt, *The Advent of Netwar* (Santa Monica: Rand, 1996).

[5] Ibid., 1.

[6] Ibid., 82.

[7] Derek Story, "Swarm intelligence: an interview with Eric Bonabeau," *P2P.com*, 2003, http://www.openp2p.com/pub/a/p2p/2003/02/21/bonabeau.html. "With self-organization, the behavior of the group is often unpredictable, emerging from the collective interactions of all of the individuals. The simple rules by which individuals interact can generate complex group behavior. Indeed, the emergence of such collective behavior out of simple rules is one the great lessons of swarm intelligence. "

[8] Eric Bonabeau and Christopher Meyer, "Swarm Intelligence: a whole new way to think about Business," *Harvard Business Review* (May 2001): 108.

[9] Government Accountability Office, "Coast Guard: Observations on the Preparation, Response, and Recovery Missions Related to Hurricane Katrina," GAO-06-903, (2006), http://www.gao.gov/new.items/d06903.pdf.

[10] *Katrinablog*, http://www.katrinablog.org/; *Katrinahelp* wiki, http://katrinahelp.info/wiki/index.php/MainPage.

[11] Dina Meta, "Social Tools - Ripples to Waves of the Future," *Global Knowledge Review* (2005), http://www.gurteen.com/gurteen/gurteen.nsf/id/gkr2005-05.

[12] David M. Ewalt, "Google is Everywhere," *Forbes.com*, September 2, 2005, http://www.forbes.com/technology/2005/09/02/hurricane-google-map-rescue-cx_de_0902google.html.

[13] W. David Stephenson, "Katrina Data Project & Public Web Stations: smart mobs in action," W. David Stephenson blogs on homeland security et al., September 27, 2005, http://stephensonstrategies.com/2005/09/27.html.

[14] Brinkley, *The Great Deluge*, 381.

[15] Ibid., 306.

[16] Ibid., 458.

[17] W. David Stephenson, "CUWiN already visualized low-cost mesh net for emergency use," *W. David Stephenson Blogs on Homeland Security et al.*, http://stephensonstrategies.com/2005/08/31.html#a450.

[18] One Laptop Per Child, http://www.laptop.org/faq.en_US.html.

[19] Jennifer McAdams, "SMS does SOS," *Federal Computer Week*, April 3, 2006, http://www.fcw.com/article92790-04-03-06-Print.

[20] Wearcam.org, "Secrecy, not privacy, may be the true cause of terrorism," http://wearcam.org/sousveillance.htm.

[21]Tim O'Reilly, "What is Web 2.0," *O'Reilly.com*, September 30, 2005, http://www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html.

[22] Jim Giles, "Internet Encyclopedias Go Head to Head," *Nature.com*, December 14, 2005, http://www.nature.com/news/2005/051212/full/438900a.html.

[23]Stacy Schiff, "Know It All," *The New Yorker*, Aug. 31, 2006, http://www.newyorker.com/fact/content/articles/060731fa_fact.

[24] Rebecca Linder, "Wikis, Webs, and Networks: Creating Connections for Conflict-Prone Settings" (Washington: Council for Strategic and International Studies, 2006), http://www.csis.org/component/option,com_csis_pubs/task,view/id,3542/type,1/.

[25] W. David Stephenson, “Roaming Presence: hot presence application for emergency use,” *W. David Stephenson Blogs on Homeland Security et al.*, http://www.stephensonstrategies.com/2005/10/24.html#a576.

[26] Gary Wolf, “Reinventing 911,” *Wired*, December 2005, http://www.wired.com/wired/archive/13.12/warning.html.

[27] Ibid.

[28] Ibid.

[29]ABC News, “Poll: Confidence in Anti-terror response Drops,” October 9, 2005, http://abcnews.go.com/Politics/PollVault/story?id=1189755&page=1.

[30]Ibid.