



FINALIST ESSAYS FROM THE CENTER FOR HOMELAND DEFENSE AND SECURITY'S THIRD ANNUAL ESSAY COMPETITION, 2010

ESSAY QUESTION

How can, or should, the United States make homeland security a more layered, networked, and resilient endeavor involving all citizens?

WINNING ESSAY

[Twitter, Facebook, and Ten Red Balloons: Social Network Problem Solving and Homeland Security](#)

Major Christopher M. Ford, Judge Advocate, U.S. Army

FINALISTS

(listed in alphabetical order by last name)

[Examining the Effective Use of Unaffiliated Volunteers](#)

Mark Bejarano, Graduate Student, American Public University

[Unacceptable Gaps: Community Grassroots Involvement in Homeland Security](#)

Lieutenant Jessica Bylsma, C-130 Pilot, U.S. Coast Guard

[Involving Citizens in Homeland Security - Changing the National Culture of Assumed Safety](#)

Mary Theresa Flynn, Senior Attorney, Federal Emergency Management Agency

[Homeland Bureaucracy - How to Reshape American Homeland Security Policy to Better Engage its Intelligence Professionals through a Layered, Networked and Resilient Attack Upon Terrorism at Home and Abroad](#)

Andrew Hicks, Intelligence Specialist, Department of Defense

ABOUT THE COMPETITION

The Center for Homeland Defense and Security (CHDS) essay contest, now in its third year, is aimed at stimulating original thought on issues in Homeland Security and Homeland Defense. CHDS launched the contest in 2008 to provide people from around the country the opportunity to express their opinions on homeland security issues and to suggest new ideas. This year's winner and four finalists were selected from 145 contest submissions by a committee comprised of CHDS staff, faculty, and alumni. The variety of the essay topics submitted, as well as the backgrounds of the authors, highlights the vast scope of the impact that homeland security policies, programs, and challenges have on our communities and professions. This year's contestants were asked to answer the question, "How can, or should, the United States make homeland security a more layered, networked, and resilient endeavor involving all citizens?"

Congratulations to this year's winners. We hope reading their essays will accomplish the contest objective of stimulating thoughts and ideas and promoting discussion and debate on homeland security and defense issues.

More information about the competition, including the question and guidelines for the current competition and an archive of questions and finalist essays from previous competitions can be found at the following web address:

<http://www.chds.us/?essay/overview>

TWITTER, FACEBOOK, AND TEN RED BALLOONS: SOCIAL NETWORK PROBLEM SOLVING AND HOMELAND SECURITY

Major Christopher M. Ford

Major Christopher M. Ford currently serves as the group judge advocate, 1st Special Forces Group (Airborne), U.S. Army. His work has published in a number of journals, including Military Law Review, Military Review, Parameters, and The Army Lawyer. Major Ford received his Juris Doctor from the University of South Carolina and his bachelor's degree from Furman University. He may be contacted at christopher.ford@soc.mil.

INTRODUCTION

On December 6, 2009, the Defense Advanced Research Projects Agency (DARPA) held a competition designed to, in their words, “explore the role the Internet and social networking plays in the timely communication, wide area team-building and urgent mobilization required to solve broad scope, time-critical problems.”¹ The competition required participating teams/individuals to find “10 8-foot balloons moored at 10 fixed locations in the continental United States.”² Just before the competition opened, the balloons were surreptitiously floated at random locations in nine states, including: California, Tennessee, Florida, Delaware, Texas, Virginia, Arizona, Oregon, and Georgia.³

The winning team, comprised of five students from the Massachusetts Institute of Technology (MIT), found all ten balloons in less than nine hours. Their performance roundly beat the other 4,000 participants in the challenge and shocked DARPA, which had scheduled the competition for two weeks. Incredibly, the team learned of the competition only four days before it started, and in less than two days they had a plan, a website, and more than 5,000 signed up to help them.⁴ They then applied that network to an extraordinarily complex problem spanning the United States. The results were shockingly accurate and swift. The significance and potential application of their system is remarkable. In a period of less than one week, five students constructed a productive, precise, layered, networked enterprise involving thousands of citizens. This essay proposes that the U.S. federal government apply the techniques developed by the MIT team into a nation-wide program designed to address discrete security issues.

THE “NEW” MODELS: SOCIAL NETWORK PROBLEM SOLVING

Naturally, the system developed for the DARPA challenge does not perfectly correlate with all homeland security challenges. For example, the system would do little to physically capture a wanted individual. The system could, however, be used to locate a wanted person. It could also be applied to assist in securing physical sites, borders, cyberspace, and infrastructure. The team leader, Dr. Riley Crane, speculated on a broad range of possible applications:

Can we use this technology we've developed to find missing children or something along those lines where there's an incentive for people to really participate and help out? Often, the police will offer a reward for finding a missing child. Can we restructure that in a way that we tap the vast resources of this network? . . . Or during an emergency, maybe we need to find 10 people in a region who can operate heavy machinery, maybe a building collapsed. ⁵

This approach to problem solving is potentially expansive. Indeed, the tool is so broad and powerful, that it is difficult to pigeonhole individual uses. Suffice to say, the potential application extends to any defined, discrete issue/problem.

At the core of the system is its incentive structure, which was structured to encourage the development of a large network of interested persons. DARPA offered a total of \$40,000 in prize money. The MIT team allocated this evenly between each of the ten balloons, giving each a “value” of \$4,000. They gave \$2,000 to the person who found each balloon. This was hardly unique; most other participating teams offered some sort of reward for finding balloons. What set the MIT team apart is that they then gave a \$1,000 to the person that referred the balloon finder to their website (assuming there was a referral – if there was no referral, the finder received \$2,000 and the other \$2,000 went to charity). Then they gave \$500 to the person who referred the referrer, \$250 to the person that referred them, and so on. This diffuse incentive structure essentially propagated itself over existing social networks: people were incentivized to get as many friends working for the MIT team as possible – almost like a pyramid scheme. The speed with which this propagated itself is remarkable. Each of the five members of the team sent out an e-mail explaining the competition and the incentive structure. Within forty-eight hours, they had 5,000 people signed up to assist them.

Another interesting modern illustration is the Vanish Competition presented in an article in the August, 2009 edition of *Wired Magazine*. ⁶ The competition accompanied an article by Evan Ratliff, which examined instances in which people had attempted to make themselves disappear. The

competition had Ratliff go into hiding for thirty days. During that time, he traveled around the United States in disguise, not making contact with family, friends or editors. He ditched his cell phone, credit cards, and online accounts. He used physical disguises and masked his movement and communications online using various technical tools. ⁷ A \$5,000 prize was awarded to the first person to identify Ratliff, take his picture, and say the word “fluke”.

Almost instantly, thousands of people became actively involved in the hunt. The participants self-organized into dozens of teams, pooling resources to find Ratliff. The teams and individual participants extensively used social networking tools such as Facebook and Twitter to connect and share information. It took twenty-five days for a team to track Ratliff down on a street in New Orleans – more than 2,000 miles from where he started. Throughout his time on the run, Ratliff continuously checked up on the social networking sites to track the trackers. He was eventually caught by team members who were able to identify him online and hack through the measures he had set up to protect his identity. Other team members, physically located in New Orleans, approached him and ended the contest. ⁸

The Vanish competition provides several lessons which affirm the lessons learned from the DARPA challenge. First, thousands of individuals can be incentivized with a fairly small monetary incentive. Though the incentive function was slightly different in the two competitions, both rely on social network mechanisms. In the DARPA challenge, the incentive structure was self-propagating. In the Vanish challenge, the monetary incentive sparked the creation of teams and social networking groups. Once sparked, the teams appear to have developed a strong social cohesion – individuals likely became interested in participating and assisting because they wanted to help the group. For the technically-oriented members of the team, professional pride may have been a strong motivating factor. One member would come up with a clever way to track Ratliff’s movements through FaceBook, and another would respond by improving the tool. This highlights another important lesson learned: not only did teams form naturally, a seemingly efficient division of labor developed as well. In both challenges, existing social networks were used extensively to share information towards the completion of the challenge. Finally, the winning team in the Vanish challenge was able to find Ratliff despite abundant misinformation provided by both other teams and Ratliff himself. The team devised a way to vet information and team members, thereby guaranteeing the accuracy of information received from team members.

CROWD-SOURCING APPLICATIONS

The DARPA and Vanish challenges incorporate many of the mechanisms seen in popular crowd-sourced projects. The term “crowd-sourced” is a generic term applied to describe projects whose design and construction are implemented by a community of people rather than a single corporation. The internet is replete with websites dedicated to crowd-sourcing individual items or services. The concept has been successfully applied to the design and sale of t-shirts (Threadless),⁹ cars (Local Motors),¹⁰ and small consumer products (Quirky).¹¹ It has also been used to write computer programs (Linux)¹² and make loans (Kiva),¹³ and in a host of other applications.

For instance, at Quirky, individuals submit inventions that they would like to see developed. The members of the Quirky community vote on each project. Aspects of the project are then completed by experts in their respective fields (e.g., a professional graphic artist does the graphic design, a mechanical engineer designs the item’s mechanics, etc.). Inventors receive a percentage of all sales, as do members who worked on a given project. Further, individual members are publically recognized when the product comes to market. The Quirky online store shows a breakdown of which members get how much of the money spent on the item. The incentive structure for participation – at Quirky and other crowd sourcing sites – is both monetary and social.

THE “OLD” MODELS

To fully understand the potential of the new social media models, it’s useful to look at traditional systems that seek to employ broad public support towards a single public goal. Crowd-sourced applications have existed for years. Perhaps the most well-known mechanism is the FBI’s “Most Wanted List.” The list was created in 1950 as a mechanism for enlisting the public’s help in capturing the most dangerous fugitives.¹⁴ Over sixty years, 494 fugitives have been listed.¹⁵ Of those, 463 have been captured – an impressive statistic.¹⁶ However, of those captured, only 152 (or 32 percent) were captured as the result of direct public cooperation.¹⁷ This is hardly a commendable success rate given the fact that the list is perpetually displayed in more than 30,000 post office locations throughout the country, online, and integrated in radio and television campaigns.

One of those campaigns has been to integrate the “Most Wanted List” with another traditional mechanism for applying public participation to solve a public safety problem: the television show *America’s Most Wanted*.¹⁸ The show has resulted in the capture of approximately 1,100 wanted

persons over the course of approximately 1,000 episodes.¹⁹ The show (recently at least) averages six million viewers per episode; given the cost of production and advertising, this is not necessarily the most efficient method of capturing criminals.²⁰

Though popular, *American's Most Wanted* is "old media." People watch the show, but they are not *vested* in the show; a certain percentage of the viewership is simply watching for entertainment. This type of crowd-sourced application is different from the newer applications in that people can passively participate (watch and be entertained without engaging). Perhaps recognizing that the social network structure used in the "new" models of crowd-sourcing are more effective, *America's Most Wanted* has made efforts to establish itself in the social network universe. At the beginning of 2011, their Facebook group has approximately 137,000 members, and the Tweet feed for the show has 3,400 followers.²¹

NATIONAL SECURITY APPLICATION

It could be argued that the social networking model of problem solving is not as efficient as it appears. In both the Vanish and DARPA challenges, there were hundreds of unsuccessful teams. Each unsuccessful team logged countless hours and expended prodigious talent and energy, with no apparent benefit. While it's true that the losing teams gained little personal benefit – they didn't win a prize – the system gained significant benefit from their participation.²² The potential strength of the social networking model of problem solving lies in the sheer volume of participants.

The Balloon Challenge and Vanish Challenge suggest that with little funding, de minimis incentive, and a strong social cohesive element, individuals can create efficient, layered, and accurate organizations that are able to accomplish complex objectives. Applying these systems to homeland security is a natural development.

Critics of the social networking approach would argue the system could be easily corrupted. Individuals targeted by the system could manipulate the system by providing false information. This critique presumes the targeted individuals would be aware that they (or their activities) are being publically hunted. As an initial matter, individuals may never realize they are being sought. They are simply not paying attention, or they don't realize they are part of the enterprise being targeted. Or, just as likely, sought individuals may be reluctant to corrupt the system because they are concerned about digitally revealing their location. Indeed, this is precisely what led to the discovery of author Evan Ratliff.

The MIT team anticipated the issue of system corruption and developed a tool to allow them to quickly cull through tremendous amounts of information and a great deal of misinformation (intentional and unintentional). During the first hours of the competition, many of the 4,000 teams engaged in misinformation campaigns designed to obfuscate and confuse their opponents. The MIT team employed an undisclosed technique which allowed them to identify fact from fiction. Their success evidences the application of an extremely successful tool which was able to manage and verify, or discredit, vast amounts of information. Such an application is critical to the success in the use of social networks in homeland security applications.

The DARPA and Vanish challenges both illustrate the power of the social networks when applied to discrete problems. When properly constructed, tools can harness the power of social networks towards a singular goal. They have the potential to do this with alarming efficiency and speed. Socially networked problem solving is not (for the most part) purely altruistic. There must be some incentive in place to facilitate involvement and action. The incentive may be monetary or social (e.g., earning respect from cyber peers), or a combination of the two. The incentives need not be robust; both DARPA and Vanish demonstrate that complex goals can be accomplished with only the smallest of incentives. The most powerful incentives combine social and monetary elements, and are structured so that they self-propagate.

The U.S. government can, and should, apply the principles underlying these programs to a homeland security paradigm. Most obviously, these models could be used to locate wanted individuals – criminals, witnesses, persons of interest, individuals with particular skills, etc. This functionality, however, barely scratches the proverbial surface of the myriad of homeland security applications, both physical and cyber. For instance, a challenge could be issued to find the security flaws in a given government website. Or, programmers could be issued a challenge to build a website for a particular function.

The modern models created for the challenges can be successfully adapted by the government *if* adapted properly. The models share three commonalities which contribute to their success. First, they are simple programs utilizing existing technologies (e.g., simple web pages, Twitter, Facebook, etc.). Second, the models are structured to answer a single discrete question (e.g., where are the balloons?). Third, the models are fueled by their powerful incentive structures. Indeed, a government program would further benefit from another equally powerful incentive: patriotism.

A simple website, integrated with social networking sites, issuing discrete challenges, and offering small cash rewards – in short, a properly structured program has the potential to solve an array of discrete problems using a vast and powerful enterprise of active, engaged, and networked citizens.

¹ Defense Advanced Research Projects Agency (DARPA), “DARPA Network Challenge,” <https://networkchallenge.darpa.mil/Default.aspx>.

² Ibid.

³ Ibid.

⁴ Lance Whitney, “MIT Floats Ideas in DARPA Ballon Challenge,” *CNET News* (December 8, 2009), http://news.cnet.com/8301-1023_3-10411211-93.html?tag=mncol:title.

⁵ Ibid.

⁶ Evan Ratliff, “Author Evan Ratliff is on the Lam. Locate Him and Win \$5,000,” *Wired Magazine*, August 2009.

⁷ Evan Ratliff, “Writer Evan Ratliff Tried to Vanish: Here’s What Happened,” *Wired Magazine*, November 2009.

⁸ Ibid.

⁹ Threadless, <http://www.threadless.com>.

¹⁰ Local Motors, <http://www.local-motors.com>.

¹¹ Quirky, <http://www.quirky.com>.

¹² Linux, <http://www.linux.org>.

¹³ Kiva, <http://www.kiva.org>.

¹⁴ Federal Bureau of Investigation (FBI), “The FBI’s Ten Most Wanted Fugitives Q&A,” <http://www.fbi.gov/wanted/topten/tenfaq.htm#11>.

¹⁵ Ibid.

¹⁶ Ibid.

¹⁷ Ibid.

¹⁸ Ibid.

¹⁹ America’s Most Wanted, <http://www.amw.com/>.

²⁰ In this regard efficiency is judged as the cost versus benefit, where the “benefit” is the criminals captured, and the “cost” is the volume of persons watching and the production costs. This rudimentary calculation of efficiency does not take into account the fact that America’s Most Wanted exists for a purpose other than to catch criminals. At base, it is a television show which provides an entertainment benefit, generates revenue for the network and advertisers, and employees a significant number of person.

²¹ Twitter, <http://twitter.com/1800crimetv>.

²² It could be argued that even losing teams benefit from an opportunity to hone their professional skills and make professional contacts within their respective industries.

EXAMINING THE EFFECTIVE USE OF UNAFFILIATED VOLUNTEERS

Mark Bejarano

Graduate Student, American Public University

There is something about the nature of mankind such that disasters that endanger life and property bring out both the best and the worst in the beast. However, studies show that the prevalent behavior during such disasters is altruism, and that humans are much more willing to preserve life rather than to ignore or disdain it. This attitude results in a spontaneous desire and effort on the part of able victims, witnesses, or passers-by to do something to aid those in need of help after a disaster strikes. While this attitude speaks well of humanity, the spontaneity often creates conundrums for professionals who are tasked with responding to disasters.

Emergency managers have struggled with the question of how to utilize these ad-hoc helpers. At first, the idea was to get them out of harm's way. However, attitudes and perceptions about volunteers have shifted, and greater efforts are being made to harness volunteers as a resource during the response and recovery phases of a disaster. Part of the struggle lies not only in how to focus that unorganized energy into a useful resource, but also with which agency or organization is tasked with handling that responsibility. Currently, there is no one entity that deals exclusively with spontaneous volunteers. Responsibility for these volunteers is gradually shifting to state and local governmental agencies and non-governmental organizations (NGOs); however, that only increases the need for inter-organizational cooperation when employing these volunteers. The focus of this essay is to examine some of the problems and best practices involved in the utilization of citizens who offer to assist in emergency situations but are not part of any recognized disaster relief entity or agency. These individuals are called unaffiliated volunteers, but are also known as spontaneous, emergent, or convergent volunteers. Throughout this essay, these terms will be used interchangeably.

THE NATURE OF SPONTANEOUS VOLUNTEERS

Fritz and Mathewson (1957, in Barsky et al, 2007) define spontaneous volunteers as “personal convergers who have a range of motivations for coming to the area” (p. 496). Among these volunteers are the returnees, who are people who live in the disaster-affected area but have evacuated; the anxious, who are people from outside the community who come to the affected area in order to find information about family members or friends; the curious, who come to the disaster site “mainly to view the destruction” (Barsky et al, p. 496); the exploiters, who are people who attempt to use the disaster for their own personal gain; and the helpers, who are people who come from both inside and outside the local jurisdictions in order to render aid to victims or assist other responders.

Two studies (see O’Brien & Mileti, 1993; Brand, Kerby et al, 2008) have determined several factors that have the strongest positive effect in explaining spontaneous involvement in emergency response: 1) the more devastating the disaster, the more likely people are to help others; 2) younger citizens are more likely to spontaneously volunteer; 3) citizens who possess a higher level of personal preparedness are more likely to aid others, and; 4) citizens who have previously experienced a disaster in their lifetime are more likely to spontaneously volunteer. These tendencies are based on four generalized motivations: 1) a general desire to help others; 2) a specific desire to be in a position to take care of family and neighbors; 3) an increased desire to be productive, and; 4) a strong desire to receive accurate information during an emergency.

Dynes (1994) identifies the changes in social structure that occur in the wake of a disaster, which he describes as situational altruism. He argues: “Thus, [situational altruism] is a situation in which individual altruism needs to be enhanced and the institutions traditionally involved in helping activities need to be supplemented” (p. 2). Dynes further observes, “Since these needs are newly created, the helping activity will not follow strictly previous institutionalized patterns. Traditional roles are expanded. New roles are created. Organizations are formed. New actors, both individual and collective, assume new responsibilities for

providing assistance” (p. 2). These new roles that Dynes describes offer potential advantages to emergency managers, but they are not without cost or consequence.

BENEFITS AND CHALLENGES OF SPONTANEOUS VOLUNTEERS

Wachtendorf and Kendra (2004) list some of the benefits that spontaneous volunteerism brings: “Volunteer convergers may, for example, bring certain abilities that do not exist in sufficient quantities in the established response organizations; they may already be close enough to damaged areas to provide immediate assistance; and they may provide for the flexibility that is needed when organizations confront rapidly-changing conditions” (p. 2). Fernandez, Barbera, and van Dorp (2006) note how volunteers “can be a significant resource of timely manpower, skills, and abilities, while providing valuable insight on a community’s needs.” (p.1). Volunteer Florida (2000) notes how two Florida counties have “demonstrated that it is not only possible but extremely cost-effective to harness this resource, organizing and empowering it to effectively serve communities struck by major disasters” (p. 5).

However, as the literature points out, spontaneous volunteerism creates as many problems as it solves, and poses quite the dilemma for emergency managers. Dynes outlines three distinct problems of situational altruism that he attributes to “over mobilization”. The first problem is that material goods sent by concerned citizens outside of the affected area often arrive too late to be relevant or are not applicable to the needs of the victims. The second problem is that unused donated goods are extremely difficult to organize, distribute, or store, which diverts response manpower. The third problem, according to Dynes, is that where the number of helpers exceeds the number of victims, there is a need to create more victims and to continue to keep victims in that status in order to continue to justify the helping effort, thereby creating victim dependency.

In addition to Dynes’ research, several studies focus on particular aspects of challenges facing organizations that coordinate spontaneous volunteers. Fernandez, Barbera and van Dorp note the challenge organizations face in matching volunteers to needs, as volunteers are often turned away because organizations are unprepared to integrate them into useful activities. Gazley and Brudney (2005) note that the “supply” side of volunteerism (usually expressed as

number of volunteers responding to promotional activities -- President Bush's launching of the USA Freedom Corps would be an example) is heavily emphasized while the "demand" side (whether public or private organizations possess sufficient infrastructure to train, deploy, supervise or retain the increased number of volunteers) remains largely ignored (p. 133). This observation is echoed by the National Voluntary Organizations Active in Disaster coalition, which argues: "The paradox is clear: people's willingness to volunteer versus the system's capacity to utilize them effectively [*italics original*]" (NVOAD, 2008, p. 2).

Another problematic aspect of spontaneous volunteerism lies in the perception of volunteers from professional responders. Wachtendorf and Kendra note how, during the response phase of the destruction of the World Trade Center in 2001, "Many volunteers were without immediately applicable skills, training, or connection to the recognized emergency management apparatus. They wanted to help, too, but it was their lack of identifiable, relevant capabilities, lack of legitimacy or connection to an organization from which they could borrow legitimacy, and probable lack of familiarity with emergency operations which rendered problematic their ties to the response milieu" (p. 9). One way of conveying legitimacy is with proper credentialing, which Wachtendorf and Kendra argues "encompasses a number of tasks, including training, certification, checking into licenses or qualifications, and issuing badges" (Wachtendorf & Kendra, p. 13). Each of these aspects, however, entails manpower and cost to implement.

Despite these challenges, the emergency management community acknowledges that the benefits of volunteerism, even spontaneous volunteerism, outweigh the liabilities and costs associated with their management.

HOW FEDERAL AGENCIES, STATE AGENCIES AND NGOs UTILIZE VOLUNTEERS

The Federal Government prefers not to manage volunteers directly, but would rather direct them towards state agencies or NGOs to receive affiliation and proper training. To that end, the Federal Government focuses on maintaining a vertical relationship with States, tribal governments, and other entities in order to ensure overall management of spontaneous volunteers. For example, the Federal Emergency Management Agency (FEMA), through its

Volunteer and Donations Management Support Annex (VDMSA), delegates the authority to individual states by assuming a supportive role (FEMA, 2008, para. 1). On those occasions where the level of disaster requires greater resources than can be mustered by local authorities, government resources are coordinated through the National Response Plan (NRP), and in turn, by the “overarching structure, doctrines and principles of the National Incident Management System (NIMS), administered by FEMA through the Department of Homeland Security. Both the NIMS and the NRP have been revised since the 2005 Gulf Coast Hurricanes to place more emphasis on collaborative incident management and to recognize the large role played by private sector and voluntary organizations in emergency response” (Gazley & Brudney, 2007, p. 3). Gazley and Brudney (2007) also note that the updated federal response plan, entitled the Federal Response Framework (FRF), reflects the more comprehensive, flexible and inclusive nature of current federal emergency planning

Getha-Taylor and Brudney (2005) note that one key feature of the NRP is its ability “to coordinate the efforts of multiple volunteer organizations, including the various Citizen Corps volunteer programs [such as the Community Emergency Response Team (CERT), the Neighborhood Watch Program (NWP), and National Voluntary Organizations Active in Disaster (NVOAD)]” (p. 5). One perceived problem associated with such groups, as observed by Barsky et al, is liability: “The CERT programme and others like it have created what federal responders refer to as ‘quasi professionals’ ... Citizens with limited knowledge of disaster response and the response capabilities of [Urban Search and Rescue] task forces often respond at the scene because they believe that their CERT training gives them the ability to assist with a response situation. Although such programmes educate the public about ways to assist in a disaster response context, the idea that they can put people on a par with professionals with years of training and experience creates difficulties” (p. 503). However, this notion of liability is not deterring CERT programs from growing in most states. Getha-Taylor and Brudney list, for example, the number of CERT programs by state (see Getha-Taylor & Brudney, Table 2, p. 24) which indicate that, with the exception of the District of Columbia and Arkansas, each state experienced growth in the number of CERT groups operating within that state between 2004 and 2005.

While the relationships between the Federal Government and state agencies and NGOs is best described as vertical, almost pyramid-like in structure, the relationship between the states and the NGOs, and between the NGOs themselves, is much more horizontal, and much more collaborative by necessity. According to Gazley and Brudney (2007), the American Red Cross (ARC), which is the only private organization designated by Congressional Charter to provide relief services, leads all NGOs in funding and scope of authority. However, they are not alone: “An additional 50 or more national organizations, and hundreds more at the state level, comprise a level of response known as VOADs, or Voluntary Organizations Active in Disaster. Still other organizations created to promote volunteerism generally, such as the Corporation for National and Community Service, and the Points of Light Foundation and Volunteer Center National Network, have supplemented the efforts of VOADs by targeting some of their resources at improving volunteer coordination during disasters” (Gazley & Brudney, 2007, p. 2).

The American Red Cross (ARC) (2006) states that one of its primary goals is to “focus on integrating partner groups directly into service delivery, working more inclusively with the diverse community, faith-based groups, civic organizations and other special-interest groups” (p. 3). However, the groups’ internal audit regarding its performance during the 2005 hurricane season, revealed a significant problem: “Beyond the system itself being stretched, the Red Cross discovered that it did not have enough sufficiently trained and experienced volunteers to run the logistics operations” (p. 7). The ARC relies on a model of operation where it can “ramp up its presence in the affected area when disaster strikes” (p. 7). While it may be a flexible model of operation, it has at least one serious drawback: it relies on trained and experienced managers who may have full-time jobs and may not be in a position to commit to an extended amount of time towards disaster activities. The ARC notes, “Because of the enormity and duration of the 2005 hurricanes, the most seasoned operational leaders, both volunteer and paid staff, were stretched beyond their capacity. Key management positions had to be filled with less-experienced volunteers who were overwhelmed at times and insufficiently trained to assume the significant responsibilities assigned (p. 14).

One of the key functions of any NGO, whether it is a large organization like the ARC, or a small religious-based group, is to change the designation of the volunteer from unaffiliated to affiliated. In other words, the large amount of efforts expended by these organizations goes into recruiting volunteers into some sort of affiliation, where their talents and skills can be evaluated, and where training and credentialing can be provided. One of the best models for that service is Volunteer Florida, which provides strong encouragement for devoting staff time towards active volunteer management, as well as a comprehensive set of plans for organizations that wish to coordinate volunteers. Within these plans are details for creating a strong local network for utilizing unaffiliated volunteers, setting up and operating a Disaster Volunteer Reception Center (including floor plans for efficient logistical operation of such a Center), and key documents for reimbursement, risk management, valuation of work performed by volunteers, equipment lists, and forms for registering, referring and documenting volunteer work.

Unfortunately, that key function may not be available in smaller organizations. According to the Urban Institute (2004), "The greatest challenges that charities and congregations face is an inability to dedicate staff resources to and adopt best practices in volunteer management" (p. 2). Their study finds that time spent on volunteer management is generally low and that less than half of the charities and congregations that manage volunteers have adopted sound volunteer management practices. The implication of this is tied to the challenge of legitimacy, in that these smaller organizations claim to present affiliated volunteers, when in reality these volunteers are scarcely more functional than those who converge to a disaster site.

CONCLUSION

There is a growing effort to harness the energy and spirit of spontaneous volunteers and channel it into productive uses. Most, if not all, federal and state agencies that are involved in emergency management recognize the value of these volunteers, and incorporate their utilization in emergency management planning. The federal government tends to delegate the administration of these volunteers to organizations that are lower in the vertical relationship, leaving the task to state agencies and non-governmental organizations. These organizations tend to share a more horizontal, cooperative relationship, and must work together in utilizing

the volunteers. Many of the NGOs increasingly focus their efforts towards coordinating these volunteers.

As it has been shown, challenges to improving the utilization of spontaneous volunteers persist. One of the most significant steps the United States can take to involve citizens in emergency response, in a safe and effective manner, is to create and/or enhance programs at all levels of government that either establish training centers for volunteer coordinators or that fund such centers. By enlarging the number of trained personnel able and willing to coordinate the spontaneous volunteers, many of the other challenges, such as employing them effectively, evaluating their skills, and providing them with legitimacy and proper credentials, will be reduced or eliminated.

REFERENCES

- American Red Cross. (2006). From Challenge to Action: American Red Cross actions to improve and enhance its disaster response and related capabilities for the 2006 hurricane season and beyond. Retrieved January 9, 2009 from http://www.redcross.org/www-files/Documents/pdf/corppubs/file_cont5448_lang0_2006.pdf
- Barsky, L. E., Trainor, J. E., Torres, M. R., & Aguirre, B. E. (2007). Managing volunteers: FEMA's Urban Search and Rescue programme and interactions with unaffiliated responders in disaster response. *Disasters*, 31(4), 495-507.
- Brand, M., Kerby, D., Elledge, B., Burton, T., Coles, D., & Dunn, A. (2008). Public health's response: Citizen's thoughts on volunteering. *Disaster Prevention and Management*, 17(1), 54-61.
- Dynes, R. R. (1994). Situational altruism: toward an explanation of pathologies in disaster assistance. University of Delaware, Disaster Research Center, DRC Preliminary Paper No. 201.
- Federal Emergency Management Agency (FEMA) (2008). Volunteer and donations management support annex. Retrieved December 16, 2009 from <http://www.fema.gov/pdf/emergency/nrf/nrf-support-vol.pdf>.
- Fernandez, L. S., Barbera, J. A. & van Dorp, J. R. (2006). Strategies for managing volunteers during incident response: A systems approach. *Homeland Security Affairs* II, 3, 1-13.
- Gazley, B., & Brudney, J. L. (2005). Volunteer involvement in local government after September 11: The continuing question of capacity. *Public Administration Review*, 65(2), 131-142.
- Gazley, B., & Brudney, J. L. (2007). Collaboration and partnership: Preparing local networks for emergency situations. Paper presented at the Ninth National Public Management Research Conference, October 25-27, 2007, Tucson, Arizona.
- Getha-Taylor, H., & Brudney, J.L. (2005). Volunteers and the Department of Homeland Security: Help or hazard? Retrieved January 26, 2009 from <http://pmranet.org/conferences/USC2005/USC2005papers/pmra.gethataylor.brudney.2005.doc>.
- National Voluntary Organizations Active in Disasters. (2008). Managing spontaneous volunteers in times of disaster: The synergy of structure and good intentions. Retrieved January 11, 2009 from <http://www.nvoad.org/Portals/0/final%202008%20Managing%20Spontaneous%20Volunteers%20LR.pdf>.
- O'Brien, P.W., & Mileti, D. S. (1993). Citizen participation in emergency response. In P.A. Bolton (Ed.), *The Loma Prieta, California, Earthquake of October 17, 1989—Public Response*. Reston, VA: United States Geological Survey.

Urban Institute (2004) Volunteer management capacity in America's charities and congregations: A briefing report. Retrieved January 26, 2009 from http://www.urban.org/UploadedPDF/410963_VolunteerManagement.pdf.

Volunteer Florida (2000). Unaffiliated volunteers in response and recovery. Retrieved January 13, 2009 from <http://www.volunteerflorida.org/emergencymanagement/docs/2008/unaffiliatedvolunteersinresponseandrecovery.pdf>.

Wachtendorf, T., & Kendra, J.M. (2004). Considering convergence, coordination, and social capital in disasters. University of Delaware, Disaster Research Center, DRC Preliminary Paper No. 342a.

UNACCEPTABLE GAPS: COMMUNITY GRASSROOTS INVOLVEMENT IN HOMELAND SECURITY

Lieutenant Jessica Bylsma
C-130 Pilot, U.S. Coast Guard

A famous quote from a naval battle in the War of 1812 stated, "We have met the enemy and they are ours..." (Dudley, 1992). Today America has ventured far from being able to defend itself through military force alone. Two oceans can no longer isolate the United States from threats from abroad, as it first learned in Pearl Harbor and more recently learned on September 11, 2001. Since then, much research has been completed about the required "layering" of defenses due to globalization's effect on ease of travel, technology access and information sharing. However, the security system's lowest level—and possibly the most effective—has been neglected. Grassroots community involvement, not just community outreach, must be elevated from its status as the weakest link in the homeland security chain.

A CALL TO ACTION

At the heart of each citizen is a fundamental conviction that calls out for action in the face of injustice. Terrorism and human suffering are the greatest of injustices and affect victims indiscriminately. In the aftermath of Hurricane Katrina, people throughout the country were volunteering, donating, and calling for the government to act. More recently, this action was seen in the January 2010 earthquake in Haiti and subsequent surge of support from citizens and government agencies. Most strikingly, even during the height of the greatest recession since the Great Depression, 2008 charitable donations totaled over \$307 billion (Bond, 2009). But well-intentioned volunteers and charitable donations, however large, are still limited in scope. For actions to reduce injustices like terrorist attacks and natural disasters, the community, businesses and the government must be involved.

The role of government is to accomplish tasks where the market fails, tasks such as firefighting, roads and national security. Government agencies at the local, state and federal level are ultimately responsible for leading America in disaster preparedness, but they also require the

assistance of voluntary agencies and non-governmental organizations. These agencies are depended upon to train volunteers to be ready to respond to disasters and are relied upon to assist those citizens affected by a disaster when an event occurs (FEMA, 2008). What is unclear is how citizens fit inside this framework. Although FEMA's National Response Framework is the guidance document for coordinated disasters preparedness, it is unclear on a plan to involve citizens in the disaster preparedness chain.

The current means for citizen involvement in national preparedness are organizations which are predominantly composed of volunteers such as the American Red Cross and the FEMA-sponsored Citizen Corps. These volunteers have made every effort to work with national, state and local agencies and everyday citizens of communities. However, the effect of these groups working alone is limited. Studies show that in 2009 only 56% of Americans had stocked disaster preparedness supplies and only 44% of households had an emergency plan detailing where to go and what to do in the event of a disaster. These results translate into a *decrease* of emergency plan preparedness by 14% since 2003, one year after Citizen Corps was originally formed (Citizen Corps, 2009). The Citizen Corps, the Red Cross, or similar community outreach organizations face even greater funding and workforce limitations than do businesses and the government. These agencies are predominantly dependent on a volunteer workforce that is much more difficult to rely upon than paid employees and their actions are also limited in scope by the extent of the private donations they receive. Since there is currently no other means for educating citizens to become more proactive, there is a gap in the current disaster preparedness model. Considering the need to reach the entire population of the United States, volunteer organizations cannot be expected to cover this gap in capability alone: they will fail.

AN INFORMED COMMUNITY

When individuals are prepared, they are less likely to burden the emergency responders and disaster volunteers with problems that could have been avoided. For example, Citizen Corps volunteers can be trained to know how to shut off gas mains in their neighborhood after an earthquake, saving response personnel time during the crucial first 72 hours of a disaster. However, these same responders may become overburdened by people overwhelming communications lines and crowding the scene of a disaster because they do not know where

their loved ones are due to improper pre-disaster planning. Prepared businesses (aided by prepared employees) are also better able to react to reduce the effects of a crisis. Businesses with an up-to-date emergency plan are able to recover more rapidly and contribute to the needs of a community in its recovery efforts (Erickson, 2006).

Finally, a government with a prepared community is better able to deal with a crisis and can help to prevent terrorist attacks in the first place. It was everyday citizens who noticed but did not report the suspicious activities of the 9/11 terrorists during the planning phase of the attack while they lived freely (and sometimes conspicuously) among their local community. It was also everyday citizens who saved even more lives during 9/11 by sacrificing their own on American Airlines Flight 93. They were willing to do this because they were aware of the true threat of those terrorists, unlike the neighbor who did not understand the true threat of some foreigners living together who played flight simulator games throughout the day (De Becker, 2002). With the proper knowledge of how to detect suspicious activity and react to a disaster, citizens can serve as the lowest level of a fully integrated homeland security strategy. In addition, since the goal of terrorists is to shock a community and show a government's weakness to its people, a collective resilience to disasters will make the United States homeland a much less attractive and effective target of terrorism.

THE COMMUNITY MODEL

Some vital preparedness tools for individuals include emergency plans, communications plans, preparedness kits, and an awareness of their surroundings. Emergency plans help families think through possible situations and agree upon common meeting areas or escape routes when a disaster happens. Communications plans can be as easy as the entire family being aware of an out of area point of contact that each family member can call to verify that everyone is safe. A major post-disaster risk is that people, especially parents at work while children are at school, will be exposed to further harm by leaving a safe haven to locate their loved ones. Responders typically have difficulty reaching those affected by a disaster because of damaged infrastructure. Individual preparedness kits that can be catered to local threats so that communities can meet their short-term needs while waiting for help. Citizens also need to have an awareness of their surroundings viewed through both a natural disaster and man-

made disaster perspective. Awareness of possible natural threats for an area can help people think through their personal risk for being affected and how they will react. Knowledge about what constitutes suspicious behavior and discussions about how to report these threats can also lead to the prevention of future terrorist attacks. An understanding of the true risks and how to react to chemical, biological, and nuclear threats can also reduce the initial panic that may otherwise surround a suspected use of a device (De Becker, 2002).

A resilient community is a place where individual members, businesses, and local agencies are prepared for disasters. Outreach organizations play a strong part in connecting these lower-level actors. However, they need help from the government at all levels to be the most effective. The Department of Homeland Security has taken the step to designate September as “National Preparedness Month.” As it now stands, this is more of an interagency, state, local and federal governmental coordination effort. What is missing is the concentrated effort to integrate citizens at a grassroots level into preparedness.

While National Preparedness Month works well for interagency coordination, what American citizens need is a focused one day event that, like Earth Day, channels their attention to one specific topic for 24 hours. No better day could be planned for this focus than on September 11th. As it stands, Patriot Day rightly serves as a remembrance of the sacrifices made by people on the tragic day almost nine years ago. But augmenting the remembrance with a call to action better serves the memory of those lost on that day.

The call to action serves several purposes. Among businesses, the single day can be the reminder needed to dust off business emergency plans and brief senior management on where the company and its workforce stand regarding preparedness. Another reason is psychological. A major effect on an individual after disaster strikes is a feeling of helplessness. The American Red Cross teaches volunteers working with those affected by disasters to refer to them as clients, not victims. Calling people victims only reinforces their feelings of helplessness. The Red Cross further encourages clients at shelters to participate in everyday chores and assist fellow clients in daily tasks such as tidying up their living spaces and clearing tables after meals. This behavior allows members to begin the process of psychological healing by giving them control and purpose. Similarly, expanding Patriot Day to become a day of memory *and*

preparedness will alter the psychology of the United States from the mentality of victim to the mentality of action. Finally, many local and state agencies have had trouble coordinating preparedness events within their communities (Deitz, 2010). Designating one specific day, especially one with so much meaning, can cut through excuses and delays. While a one month timeline for preparedness is sufficient for interagency actions, businesses and community members would be better served with a concentrated effort on a day that is so meaningful to every US citizen. On that day, each participant has the chance to honor those who made the ultimate sacrifice and make good on their pledge that they will do their part to ensure it never happens again.

NATIONAL PREPAREDNESS DAY

A possible contributor to the lack of preparedness at the community level is the difficulty in obtaining participation from its citizens. Yet, having a family talk about what to do in an emergency should not be approached as a chore. There are many ways to openly or subtly encourage citizens to participate in a national preparedness day. With creative involvement of all members, the opportunities to gain the participation needed are only limited by the creativity of those involved.

No matter how activities for this one day event are carried out, the most important approach must be targeted at people having fun. A charity group in the United Kingdom championed this concept when it changed its regular fundraisers from appealing to guilt to appealing to fun. Instead of hosting telethons, this group sold red noses for the equivalent price of two candy bars and hosted an evening of comedy acts performed by famous comedians who donated their services. Because of their approach, they obtained donations from all income levels and all demographics (Moriarty, 2006). Similarly, a nation preparedness effort would not need to be based on a theme of need. It could be approached as an opportunity for fun.

For example, schools have strong influence on preparedness. Studies show that of the many resources used to obtain information related to the H1N1 virus, schools were mentioned as a source of flu information by 23% of respondents (Citizen Corps, 2009). During September 11th, teachers could incorporate preparedness activities into their curriculum, especially elementary schools. These could include coloring contests, essay contests, or visits from characters who are

linked to a preparedness theme. Just like Sparky the Fire Dog, the National Fire Protection Association's character that teaches kids to "stop, drop and roll" when on fire, a character could be created that makes it fun for children to learn about plans for emergencies or suspicious activities. Another option is for children to take a short preparedness quiz, such as how they would leave their house and what number they would call for informing their family that they were safe. Children who answered well would get a star or some small certificate, and children who did not score well will more likely be motivated to go home and ask parents about this information. Furthermore, since these activities are carried out by schools in the community, the threat information can be catered to local risks, so that Florida children are not being quizzed on frostbite and Wisconsin students are not quizzed on hurricane preparedness.

From a "whole community" standpoint, a one-day event allows for a concentrated effort for small towns and cities to host an event. Small towns could host parades in their streets or fairs in their parks with a disaster preparedness and Patriot Day theme. Parades could host local groups involved with emergency response and planning including firefighters, police, the National Guard, the Red Cross and other community outreach groups. People will have the chance to interact with the groups that are involved in their local emergency response efforts. They have the chance to learn more about what the groups can and cannot do. For example, one of the challenges for the Red Cross is that many citizens do not know the entire breadth of services that are offered and do not seek assistance for smaller disasters such as a single house fire or flood. A town fair with a preparedness theme would allow people to learn more about what services are offered. This is especially true if local agencies host demonstrations of their capabilities. For example, local FBI offices or local police involved in terrorism awareness could have demonstrations of what suspicious behavior is. When everyday citizens interact with these police and FBI agents and hears from them how to handle such a situation, they will be less hesitant to act when the real situation occurs, especially if their required action is to call the agents they have already interacted with. Another benefit of a concentrated effort by local groups involved in preparedness is that members of these groups can learn what other resources are available. During a fair or parade, these groups have a chance to interact with each other at an informal level to understand overlap or gaps in preparedness coverage at the local level. It also will help to build the relationships needed to effectively coordinate during a crisis. As one attendee of a preparedness lecture stated, "Ground zero is not the best place to

start exchanging business cards.” Fairs and parades, when approached from a preparedness angle, unite a community in a concentrated effort to prevent a future attack like 9/11.

Like Earth Day, a one day event can channel the desires and attention of people who are otherwise deeply involved in busy daily routines. During a one day event, everyday citizens will be able to learn how they can help prevent or lessen the extent of another disaster in the future just by taking some simple preparedness measures. Smart media coverage of the event would lead to an even greater awareness of preparedness activities since the media is currently a major source of disaster information for the general public.

CONCLUSION

A one day preparedness event provides the means for everyday people to participate in preventing a future attack like that on September 11, 2001. The event need not be a chore or only a somber remembrance of the victims of attack. With a little creativity, the event can honor those who lost their lives on that day by enabling citizens to do their part to prevent a future attack.

WORKS CITED

- Bond, S. (2009, June 10). US charitable giving estimated to be \$307.65 billion in 2008. Giving USA Foundation. Retrieved January 30, 2010 from <http://philanthropy.com/article/Charitable-Donations-Fell-by/63106/>
- Citizen Corps. 2009, August. Personal Preparedness in America: Findings from the 2009 Citizen Corps National Survey. Retrieved January 27, 2010 from http://www.citizencorps.gov/pdf/2009_Citizen_Corps_National_Survey_Findings.pdf
- De Becker, G. (2002). *Fear less: Real truth about risk, safety, and security in a time of terrorism*. New York, NY: Little, Brown and Company.
- Dudley, W. (1992). *The Naval War of 1812: A Documentary History*. Vol.2. Washington, D.C.: Naval Historical Center: p. 553. Retrieved June 2, 2010 from <http://www.history.navy.mil/trivia/trivia02.htm>
- Erickson, P. (2006). *Emergency response planning for corporate and municipal managers* [2nd ed]. Boston, MA: Butterworth-Heinemann.
- Federal Emergency Management Agency. (2008, January). The National Response Framework. FEMA. Retrieved June 2, 2010 from <http://www.fema.gov/pdf/emergency/nrf/nrf-core.pdf>
- Dietz, J. (personal communication, January 28, 2010). Purdue Homeland Security Institute.
- Moriarty, C. (2006, May 29). Red nose day: A very silly idea that changed one charity's destiny. *ABIX*. Retrieved June 2, 2010 from <http://www.highbeam.com/doc/1G1-146361521.html>

INVOLVING CITIZENS IN HOMELAND SECURITY – CHANGING THE NATIONAL CULTURE OF ASSUMED SAFETY

Mary Theresa Flynn

Senior Attorney, Federal Emergency Management Agency

The United States must endeavor to involve all citizens in the enterprise of homeland security, in terms of identification of risks, acknowledgement that incidents will occur, and appropriate incident response. To do so, the United States must encourage citizens to embrace homeland security as part of their responsibilities as citizens and as a function of America's national wellbeing. This will require a change in America's national culture of assumed safety.

Homeland security includes preparation for, and response to, terrorist activity and natural disasters. But regardless of our success in identifying and containing terrorist threats, we will never fully "contain" nature. That realization makes natural disasters easier to predict: we know that they will always occur, and they occur for scientifically predictable reasons. Because natural disasters are more consistently predictable than terrorist activity, they present a useful laboratory for testing the ability to change a national culture. Towards that end, this essay explores an existing program within the Department of Homeland Security, *i.e.* the National Flood Insurance Program's flood hazard mapping program, as an investigative model for analyzing and expanding citizen understanding of, preparation for, and response to, either a terrorist attack or a natural disaster. We can later apply the resulting lessons learned to instigate a change in American culture regarding the broader range of homeland security concerns, including terrorist incidents.

THE NATURAL DISASTER "LABORATORY"

We know that natural disasters will happen. And through agencies such as the Federal Emergency Management Agency, the United States Geological Service, and the National Oceanic and Atmospheric Administration, we know with specificity where they will happen. We can also predict – to a significant degree – when and to what extent, most natural disasters will occur and what impact they are likely to have. Indeed, this information is already mapped and is resident within federal government repositories that are accessible to the public via the internet. However, one must know where to look, and more importantly, *have the motivation to look there.*

Oddly, the predictability of the likelihood, exact location, and magnitude of natural disasters, and the ready availability of information as to how they will affect individual citizens, comes as a surprise to many people. This innocence is precisely what the United States needs to change if it is to engage citizens in the heightened sensitivity, preparation, and mitigation, which are required to secure the homeland against disasters of any ilk. This change is essential to make homeland security a more layered, networked, and resilient endeavor involving all citizens.

Accordingly, in order to develop the most effective way of broadly engaging citizens' interest in homeland security, the United States should explore the most effective ways to get information to the public of when and to what extent natural disasters will occur *in the area where they live*. Moreover, this information must be put in a context that is meaningful to them. Until they accept and understand the very real risks they currently bear, convincing them to prepare for, and mitigate against, those current risks – much less terrorist risks yet to develop – is a futile exercise. Without this information, the risk of a significant natural disaster actually happening *to them* is simply not real.

Yet, it is not just *significant* natural disasters that can *and will* cause the United States to suffer preventable damage and delay in future incident responses. A flood of only two feet may only be a significant weather event, and not a disaster in and of itself. Yet its timing may impede a community's ability to respond to a contemporaneous terrorist attack or a mass casualty event, by orders of magnitude. ¹ Even a "minor" flood of two feet will render evacuation routes impassable. Combine that minor flood with a terrorist attack and there will be a vast number of citizens backed up at a now-impenetrable exit point. Ambulances will be stymied in their attempts to reach the injured.

Under a different scenario, if a similar "minor" flood blocked routes to the local hospital, a plane crash, train wreck, or other mass casualty event would prevent doctors, nurses, and other essential personnel from reporting to the hospital as needed. Yet, understanding that risk, and planning for it will obviate many of these surprises, and perhaps save many lives.

Among the questions that need to be asked are:

- Do citizens know what roads will be impassible in the event of a flood?
- Do hospital personnel know what routes will be impassible in the event they must report to work due to a mass casualty event?

- Do emergency medical technicians know what routes will be blocked as they respond to emergencies and then attempt to get to the nearest medical facility?
- As flood waters rise, do local police, public works, and emergency personnel know which areas of their communities to evacuate first, depending upon which rescue routes will become impassible first?

THE NATIONAL FLOOD INSURANCE PROGRAM'S FLOOD HAZARD MAPS

The purpose of the National Flood Insurance Program ("NFIP") is threefold; it intends to discourage development in a floodplain; it intends to shift the burden of constant disaster relief to those who live in the floodwaters' path, through an insurance system of risk-sharing related to the degree of risk one chooses to incur; and most importantly for the purposes of this discussion, it is designed to map the geographical boundaries and predicted depth of a flood event that has a one-percent chance of occurring in any given year. The resulting flood hazard maps inform the community as a whole of the danger of flood risk to hospitals, police stations, evacuation routes, and other infrastructure. From these maps the community knows if or what portion of a hospital complex will flood, and the height to which the flood waters will rise. The maps depict which roads will flood and to what depth they will flood. Similarly, each citizen is also informed if or what portion of their home will flood, and the height to which the flood waters will rise – *if they look at the flood hazard map.*

This critical information is already in the hands of the more than 20,000 communities in the United States that participate in the NFIP. Importantly, this flood hazard data is available digitally to many of these communities, and soon will be available digitally to all of them. Thus, this information can be readily integrated into a community's Geographical Information System ("GIS") as a flood hazard overlay. It can then be selected to display as needed as an overlay on a community's 911-Emergency Services Locator Map, the community's real estate tax maps, zoning maps, or all of the above. Yet that integration into the tools of emergency services personnel and other community officials is not enough to invest individual citizens with an appreciation of the ongoing risk to them. Without appreciation of that risk, citizen behavior will not change, and the culture of assumed safety will continue.

LAYERED VERSUS NETWORKED

The United States' approach to homeland security appropriately involves state and local governments in all aspects of homeland security. It has to. The federal government does not have the resources nor, importantly, the local knowledge (*e.g.* the best evacuation routes) essential to disaster planning and response. Moreover, in many instances the United States does not have the legal authority to promulgate or administer regulations essential to natural disaster protection and mitigation.

For example, the federal government is constitutionally prohibited from adopting or enforcing zoning laws, building codes, and other types of land-use ordinances. The Tenth Amendment of the Constitution reserves to the states, all power and authority not specifically and explicitly granted to the federal government elsewhere in the Constitution.² In turn, with the exception of the *adoption* of a uniform statewide building code and many criminal and traffic laws, the states generally devolve most police powers to local governments. That is why building codes, criminal laws, and traffic laws are usually state statutes enforced by local government police and building officials. Zoning ordinances, which are more location specific, are usually both adopted and enforced by the local government.

That is also why the National Flood Insurance Program must require participating communities to adopt local flood mitigation ordinances³ as a condition of participating in the NFIP. The federal government cannot adopt, nor can it enforce, zoning ordinances which require citizens to locate new construction out of the mapped floodway, nor can it impose building code requirements compelling the elevation of a structure's first floor to or above the predicted base flood level in the mapped flood hazard area. By contrast, the state or local government can. For these and many other reasons, the United States must – and should – continue to cooperate with, support, and rely upon its state and local partners.

But sometimes, reliance on these layers of state and local government to get necessary information out to citizens works to the federal government's disadvantage. Here, the NFIP flood hazard mapping program is instructive. The NFIP gives its flood hazard maps to its participating communities. Yet, other than requiring that a single copy of the flood hazard maps remain on file at the community's headquarters, the NFIP does not require the distribution of the flood hazard information to the citizens. It does not even require that the flood hazard data be integrated into a community's 911-Emergency Services Locator Map. Instead, the NFIP relies on the community to

decide whether, and the extent to which, it makes that information readily available to its schools, hospitals, public works department, police, emergency services, or to its citizenry.

To their credit, many participating communities integrate that flood hazard mapping data into their GIS database as a matter of course and common sense. In other instances, the NFIP must entice a community to assimilate the flood hazard mapping data into their GIS database, or alternatively, place a copy of the flood hazard maps in the local public library. The carrot offered to these communities is a complex system of awarded points for engaging in enumerated flood mitigation activities above and beyond the minimum floodplain standards required as a condition of participation in the NFIP. Under this system, called the Community Rating System, the communities must apply the rules contained in an inscrutable 700-page manual to convert the points to discounts on flood insurance premiums for their citizens. ⁴ Thus, many communities fail to incorporate flood hazard data in a publically available database.

In communities where the flood hazard data is available in the GIS database, a citizen must purposefully go to the community's website to search for the flood hazard data that applies to his or her property. But citizens that go looking for flood hazard data likely already appreciate the enduring risk they bear, and may already be of a mind that that hazard will likely require some action on their part, or awareness of the implications to them and their community. It is the citizens to whom it would never occur to look for such data that are of concern here.

PUT THE INFORMATION WHERE THE PEOPLE WILL FIND IT – PUT IT WHERE THEY ALREADY GO

This section is the corollary to the old saw: "Put the sidewalks where people walk, instead of where you think they ought to walk." Parents, whose primary interest may be their children's schooling, will likely visit that school's website, even if they would never consider looking at zoning or real estate tax maps where a community may have placed flood hazard information. Flood data depicting which access roads will likely be flooded should and can be resident on the school's website. This information would be especially useful should a school lockdown occur for an unrelated event.

Hospitals, if they don't already, should have a GIS database to evaluate access by ambulances and personnel during a mass casualty event. Flood hazard data should be resident there so all hospital personnel are exposed to the notion that floods will affect their working lives. Indeed, it should be

part of every hospital's emergency plan. Even the community's bicycle trail map should contain flood hazard data – not because of any dire interruption to an afternoon's bike ride – but rather because it places this information where the biking aficionado will see it. Until all of these people have that “*Gee, this is real, a flood or other disaster could happen to me*” moment, homeland security will never be a fully layered, networked endeavor involving all citizens.

The key here is educating citizens as to flood hazards when they will not naturally seek that education on their own. The incidental exposure to flood risk data via websites where people's interests naturally take them, is a laboratory opportunity to perhaps engender, and then evaluate, a cultural shift. While there is no direct correlation to predictable, mapped natural hazards versus unanticipated, (and surely not mapped) terrorist attacks, lessons learned about the potential for a cultural shift from flood risk education can be evaluated and applied as appropriate to more broad-based goals.

WHAT THE UNITED STATES SHOULD DO NEXT

The NFIP needs to cut out the middleman. Instead of allowing a participating community to choose whether it will integrate NFIP flood hazard data into its GIS database, the NFIP should amend its minimum standards for participation to require all communities with a GIS database to integrate the NFIP flood hazard layer. Inasmuch as all new and every revised flood hazard map are produced and dispersed digitally to the community over the internet, this requirement would not cause a hardship.

Both the NFIP and the United States Fire Administration (“USFA”) are part of the Federal Emergency Management Agency. Both have disaster prevention as a major mission objective. The NFIP and the USFA should work together to integrate flood hazard maps as an overlay to every 911-Emergency Locator Map possible. The data should be disseminated freely. Opportunities for cooperation with other federal agencies to disseminate this data, and evaluate this model, should be explored, but this will require the disintegration of the “silo” mentality in many federal government programs.

Finally, the successful involvement of all citizens in a layered, networked, and resilient homeland security endeavor will require a multi-disciplinary approach to achieve that goal.

¹ One need only recall the difficulties from the severe snowstorm experienced by first responders after the crash of Air Florida Flight 90 into the Potomac River on January 13, 1982. A Metrorail train crashed in an underground tunnel at the same time. Federal workers were leaving work early due to the severe snowstorm and roads and bridges were jammed with commuters, blocking access for ambulances to both tragedies.

²See, *Tenth Amendment to the United States Constitution*. The text of the Tenth Amendment reads: "The powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved to the States respectively, or to the people." The Tenth Amendment is known as the "Reserve Powers Clause" or alternatively the "Police Powers Clause" because the maintenance of a local police force, zoning authority, building codes, and other land-use authority are collectively known as the "police powers."

³ Local flood mitigation ordinances of NFIP participating communities must meet or exceed minimum standards set out at 44 C.F.R. Part 60, § 60.1, *et sec.*

⁴ See, Federal Emergency Management Agency, *National Flood Insurance Program Community Rating System Coordinator's Manual*, FIA-15/2007.

HOMELAND BUREAUCRACY - HOW TO RESHAPE AMERICAN HOMELAND SECURITY POLICY TO BETTER ENGAGE ITS INTELLIGENCE PROFESSIONALS THROUGH A LAYERED, NETWORKED AND RESILIENT ATTACK UPON TERRORISM AT HOME AND ABROAD

Andrew Hicks

Intelligence Specialist, Department of Defense

INTRODUCTION

The 2006 National Security Strategy of the United States proclaims, “A government has no higher obligation than to protect the lives and livelihoods of its citizens. The hard core of the terrorists cannot be deterred or reformed; they must be tracked down, killed, or captured. They must be cut off from the network of individuals and institutions on which they depend for support. That network must in turn be deterred, disrupted, and disabled by using a broad range of tools” (The White House, 2006 p. 12). The National Security Strategy (NSS) of the United States intends to provide a strategic guidance; it essentially provides the broad goals to be attempted, rather than *specific* guidance on *how* to achieve those goals. The National Strategy for Homeland Security also identifies the threat of terrorism, specifically violent Islamic extremism and lists select measures designed to enhance homeland security effectiveness (U.S. Department of Homeland Security, 2007 p. 9.). The question remains, what specific tools have American Intelligence Agents been provided to better protect our country from terrorist attacks? Essentially, have the flaws, which were so painfully obvious in the aftermath of 9/11 and most recently presented by the radical Islamic attack at Fort Hood and the attempted Christmas day suicide bombing of Northwest Airlines flight 253, been resolved? If flaws still exist, what changes must be made to U.S. Homeland Security policies to more effectively thwart terrorist attack against Americans at home and abroad?

POLITICAL TURMOIL AND AN EMERGING FRAMEWORK

Today, the American Intelligence Community plays by complex and sometimes contradictory rules. Overall guidance to the intelligence community is provided by Executive Order 12333, *United States Intelligence Activities*, most recently updated in 2008. In order to fully understand EO 12333, it is necessary briefly trace the document back to the context of its creation. EO 12333 was first written in by then President Ronald Reagan as a response to significant intelligence regulations and legislation of the previous administrations. The political mood in American became turbulent in the 1970s as the public witnessed the escalation of the unpopular conflict in Vietnam, multiple accusations of spying against federal intelligence agencies, including Army Intelligence, the Federal Bureau of Investigation (FBI) and the Central Intelligence Agency (CIA) The infamous political scandal known as *watergate* also contributed to the climate of mistrust by many American voters. Key politicians felt compelled to reign in the intelligence community's power and hold leaders accountable for what many considered grave privacy invasions against Americans. The accusations and scandal eventually forced President Nixon out of office, enacted sweeping legislation to include the Foreign Intelligence Surveillance Act (FISA), the privacy act of 1974 and permanent congressional oversight on intelligence activities. Army Intelligence, the FBI and the CIA made sweeping changes which drastically altered their intelligence collection activities (National Commission on Terrorist Attacks upon the United States, 2004 p. 88-91).

A NEW ERA

Ushered into office on the promise of honesty and openness, Jimmy Carter promised a new direction for American intelligence and foreign policy. Unfortunately, serious diplomatic failures, including the Iranian Islamic Revolution and the subsequent taking of hostages at the American embassy in Tehran began to swing the political pendulum back toward a stronger foreign policy. President Ronald Reagan was elected in 1980 and in 1981 provided new and specific guidance to the intelligence community which had suffered devastating setbacks in the tumultuous 1970's. Reagan signed Executive Order 12333, which appears to have been his administration's way of reengaging the intelligence community in the defense of America and its interests. EO 12333 caused the Federal Bureau of Investigation (FBI), Central Intelligence

Agency (CIA) and the Department of Defense (DoD) to write new regulations in accordance to the presidential guidance, many of which have changed little since then. The most significant of which directed the FBI to have primary responsibility for intelligence and terrorism within the United States. EO 12333 directed the CIA to retain primary responsibility for intelligence and terrorism outside the U.S. The DoD, which included military intelligence services of the Army, Navy, Marines and Air Force, enacted internal regulations and attempted to independently work within the executive constraints (Office of the President, 2008). Since the DoD necessarily operates both overseas and stateside, the rules and subsequent interpretation became complex. The overarching principle that may have been clear to the Intelligence Community in the 1980s was that presidential direction and congressional oversight, which was often contradictory, had changed the paradigm. It is at this stage that the growing presence of lawyers, needed for their interpretation of presidential and congressional intent, became a controlling element in the community, without which agencies and their Agents hesitated to act for fear of prosecution.

COMPOUNDING THE MISTAKES

In response to EO 12333 and subsequent DoD directives, the United States Army created Army Regulation 381-10, U.S. Army Intelligence Activities, which intricately detailed the circumstances upon which the U.S. Army could collect information on U.S. persons (Department of the Army, 2007). The Army went on to detail exactly how its intelligence agents would pursue national security crimes in Army Regulation 381-12, Subversion and Espionage Directed Against the U.S. Army (SAEDA) (Department of the Army, 1993). A myriad of other regulations, including Army Regulation 381-20, The U.S. Army Counterintelligence Program, would further define and restrict DoD components from intelligence collection (Department of the Army, 1993). Internal regulations and policies built systematic layers of bureaucracy, which drastically reduced the speed and function of intelligence Agents on the ground. In such an accusatory climate, it is easy to understand why some agencies were guilty of *stovepiping* or failing to share information with other agencies. Since intelligence and its efficacy relies upon speed, oversight and its bureaucracy in the 1970s served to relegate the efficiency of the American Intelligence community.

LAW ENFORCEMENT VERSUS INTELLIGENCE

Antiquated federal laws also factored into the formula which ultimately resulted in the American intelligence community's reduced efficiency. The *posse comitatus* act, although written to deny local law enforcement the ability to requisition troops for their service, was often misinterpreted to restrict DoD intelligence Agents from pursuing crimes deemed to be within the responsibility of *law enforcement* (Trebilcock, 2000). Since terrorism is neither uniquely a law enforcement crime nor an intelligence crime, but rather both; the artificial and nonsensical divide between law enforcement and the intelligence community served to systemically weaken the entire American intelligence community. The 9/11 Commission Report noted how significant difficulties of sharing law enforcement and intelligence information within the FBI were problematic to the disruption of the 9/11 attack (National Commission on Terrorist Attacks upon the United States, 2004 p. 78-79). The FBI, the most empowered domestic intelligence and law enforcement agency directed to act within the United States proved unable to communicate effectively even within its own organization. The Department of Defense, with its rigid military chain of command, has also been plagued with communication problems. Mathew Bogdanos explained in Joint Force Quarterly how the doctrine within the DoD did not properly facilitate *joint* forces cooperation which is a direct impediment to the Global War on Terror (2005). With such an examples, it is very easy to understand how the multitude of agencies across the intelligence community find it problematic, if not impossible, to push through the barrier between law enforcement and intelligence to effectively share timely information and coordinate complex counterterrorism and intelligence investigations.

STATUS, LOCATION AND TURF WARS

In addition to the created divide between Law enforcement and Intelligence, whether a subject is considered a U.S. person or not has developed into another stumbling block for the intelligence community. Out of deference to laws enacted in the 1970s, the intelligence community has adopted different rules and additional layers of bureaucracy ostensibly designed to safeguard the privacy rights of the American people. Agencies operate differently based on whether the subject of an investigation is a U.S. person and whether or not the subject

is inside the United States. In effect, an investigation is drastically slowed by the first tentative steps to discover the status and location of a subject. At this point, several agencies may have investigative jurisdiction of some nature and the details of which are often complex, contradictory and the source of conflict between agencies. If the subject is considered a U.S. person and located inside the United States, this is, essentially, the worst case scenario for an intelligence investigation. The kid gloves are firmly in place when it comes to investigative action an Intelligence Agent may take and the requisite bureaucratic approvals for each investigation act are countless and cumbersome *if* approved. Some agencies may have no authority to conduct an investigation whatsoever depending on the combination of status and location. In truth, neither the location nor the status of a terrorism or intelligence subject should be a factor in what tools are at the disposal of an American Intelligence Agent. Regardless of the employing agency, an intelligence Agent must rely upon their training and expertise to determine which investigation actions and tools are necessary on a case-by-case basis. Only a homeland security policy specifically designed to fail would place restrictions upon its Intelligence Agents and their ability to pursue investigations. It is the professional integrity, training and expertise of American Intelligence Agents which will safeguard the privacy of innocent U.S. persons, not arbitrary government intervention. The current restrictive policy is akin to a customer asking a mechanic to fix his car, but the customer will pick and choose what tools are available, in what circumstances they will be used, and approval for additional tools *may* be approved upon request. Such a policy only succeeds in producing much slower, inefficient and inferior results. There is a level of trust that must be established between the American people and their intelligence Agents, without trust, government intervention will only continue to succeed in degrading the effectiveness of our homeland security.

A LAYERED HOMELAND SECURITY STRATEGY

To create a *layered* Homeland Security strategy it is necessary to have multiple intelligence agencies actively seeking the same priorities. This concept capitalizes on three necessary concepts for an effective Homeland Security, redundancy, efficiency and competition. The U.S. government must redefine and not simply in name only, terrorism as the primary responsibility and investigative priority for DoD, FBI and CIA intelligence Agents. Agencies

directed by the President through an updated EO 12333 and coordinated by the Director of National Intelligence, must act to streamline their internal bureaucratic controls to empower Intelligence Agents on the ground to take swift action to pursue all terrorism information and investigations to their final conclusions. Remove the understood primacy of the FBI as lead agency in the United States and instruct Agents of the DoD, CIA and FBI to pursue all terrorism investigations to conclusion, whether stateside or abroad.

There is no logic to defend a policy which presumes U.S. persons privacy rights are more effectively protected by dividing jurisdiction between intelligence agencies. If this logic were practically implemented into local law enforcement, a county Sheriff's deputy would be unable to arrest a murderer within the city limits, but would have to coordinate and communicate with local police first. This is, obviously, not the case. Local law enforcement officers have overlapping jurisdictions and will act to arrest criminals outside geographic jurisdictions if the need or opportunity arises. As was the case with several of the 9/11 suspects American Intelligence Agents were tracking some of the future hijackers movements, but were forced to concede jurisdiction as the suspects travelled into the United States. The reverse is also the case and primacy of the CIA overseas must also be removed. Such complicated hand-offs between intelligence Agencies are unnecessary, inefficient and often, as was the case with 9/11 plot suspects which were under surveillance overseas but were lost in transit to the U.S., results in failure (Commission on Terrorist Attacks upon the United States, 2004 p. 181-182).

IMPLEMENTATION

Once an intelligence Agent from the DoD, FBI or CIA identifies the subject of a terrorism/intelligence investigation, that Agent and his or her supporting agency must be afforded the approval and necessary support to conduct the investigation to conclusion. The subject would be identified and placed into intelligence databases. The accessibility of case information, necessary for de-confliction among intelligence agencies, would be greatly enhanced by a central database. However, as it is now, without a central database, agencies would be forced to communicate more and work together in many cases because each agency would be overlapping in mission and jurisdiction in a layered attack.

Enhanced use of current mechanisms such as the joint terrorism task forces would greatly aid the process of de-confliction, while continuing to promote a layered security strategy and healthy competition among intelligence agencies. Such a strategy would allow Agents on the ground to decide how and when they would request assistance from Agents outside their own agency, thus eliminating bureaucratic requirements yet allowing for practical coordination. Agencies, no longer tasked with sole responsibility for a jurisdiction, would likely be more willing to assist other agencies with investigations since it would no longer be necessary to reserve resources to protect their home turf or jurisdiction. With systemic restrictions cleared, Agents must be granted the necessary internal procedures, search warrants and investigative tools through the Federal Intelligence Surveillance Act (FISA) Court.

CONCLUSION

A revision of Executive Order 12333 is necessary to eliminate key restrictions which have, over time, systematically degraded the efficiency of the American Intelligence community. Specifically, it is necessary to unite the DoD, FBI and CIA with the *same* priorities and jurisdictions. The DoD, CIA and FBI must make terrorism their first priority and through their Agents, aggressively pursue terrorist and intelligence investigations to their conclusion. DoD, CIA and FBI Intelligence Agents must be fully supported on the highest levels of government with all the necessary investigative tools at their disposal regardless of a subject's status or location. The DoD, CIA and FBI Intelligence Agents must operate with equal authority and overlapping jurisdictions to create a legitimate source of competition. Agencies simultaneously attacking terrorism and intelligence investigation create a more *networked, resilient* system because it builds in redundancy, a *layered* approach and no single points of failure.

REFERENCES

- Bogdanos, Matthew F. (2005, March, issue 37). Joint Interagency Cooperation: The First Step. *Joint Force Quarterly: A Professional Military Journal*.
- Department of the Army (1993). *Army Regulation 381-12: Subversion and Espionage Directed Against the U.S. Army (SAEDA)*. Washington, DC: U.S. Government Printing Office.
- Department of the Army (1993). *Army Regulation 381-20: U.S. Army Counterintelligence Program*. Washington, DC: U.S. Government Printing Office.
- Department of the Army (2007). *Army Regulation 381-10: U.S. Army Intelligence Activities*. Washington, DC: U.S. Government Printing Office.
- National Commission on Terrorist Attacks Upon the United States. (2004). *The 9/11 Commission Report*. Washington, DC: U.S. Government Printing Office.
- Office of the President of the United States (2008). *Executive Order 12333: United States Intelligence Activities*. Washington, DC: U.S. Government Printing Office.
- The White House (2006). *The National Security Strategy of the United States of America*. Washington, DC: U.S. Government Printing Office
- Trebilcock, Craig T. (2000, October). The Myth of Posse Comitatus. *Homeland Security Institute: Journal of Homeland Security*
- U.S. Department of Homeland Security (DHS), *National Strategy for Homeland Security* (2007), http://www.dhs.gov/xlibrary/assets/nat_strat_homelandsecurity_2007.pdf