

Homeland Security in Real-Time: The Power of the Public and Mobile Technology

Andrew Heighington

ABSTRACT

In the world of homeland security, mobile phones are too often viewed as detonation devices rather than vital communication mechanisms to prevent terrorist attacks from occurring. It takes collective intelligence from federal, state, and local entities, as well as the public, to prevent terrorist attacks. Mobile technology empowers collective intelligence in ways that were never before possible. This essay argues that the nation's crisis communication strategy must be broader and more innovative than commercial broadcast alerts, mobile text messages, and social media sites such as Facebook and Twitter. Federal, state, and local officials, in concert with the public, should adopt a strategy that leverages mobile technology and harnesses the power of mobile applications that allow communication between the government and individuals.

INTRODUCTION

Crises are unpredictable events that demand adaptation and flexibility. During a crisis, many communication experts contend that the public engages in information-seeking behaviors to reduce uncertainty.¹ Research indicates that effective crisis communication with the public requires a clear, relevant, and timely narrative, openness to dialogic communication, and source credibility.² However, as Sung Yung Yang and others note, the content of the message is only half the challenge: "Different forms of communication can bring out a completely different individual interpretation – and in turn, various post-crisis reactions, including... attitudinal and behavioral outcomes."³ Traditional media used for crisis communication typically includes television and radio broadcasts, print, and the Internet. Social media is quickly emerging as another

form of communication that shapes attitudes and behaviors by allowing the public to better seek and share crisis information.

During the 2008 Mumbai terrorist attacks, for example, vital information, such as emergency phone numbers and hospitals needing blood donations, was distributed via Twitter.⁴ Closer to home, Twitter provided valuable situational awareness to the public and military families in the aftermath of the Ft. Hood shooting in 2009.⁵ Research on the September 11th attacks also reveals that individuals actively sought to reduce uncertainty by accessing information through a variety of means.⁶ The American public, increasingly accustomed to the distribution and receipt of information in real-time, will likely engage in similar information seeking behaviors that leverage technology during the next crisis. Consequently, the United States government is taking important steps to prepare for this likelihood. Craig Fugate, administrator of the Federal Emergency Management Agency (FEMA), stated:

As social media becomes more a part of our daily lives, people are turning to it during emergencies as well. We need to utilize these tools, to the best of our abilities, to engage and inform the public, because no matter how much federal, state and local officials do, we will only be successful if the public is brought in as part of the team.⁷

But are current crisis communication tools such as television and radio broadcasts, print, the Internet, and social media effective at leveraging the public during a crisis? Is a more robust platform needed to prevent terrorist attacks from occurring?⁸

This essay argues that television and radio broadcasts, print, the Internet, and social media are not optimally suited to mobilizing the public to prevent a terrorist attack from occurring. The United States government, in partnership with the public, and state and

local entities, should explore ways to better leverage the convergence of the Internet and mobile devices via smart phones to engage the public. Today, more Americans have cellular mobile phone subscriptions than Internet subscriptions and smart phones are quickly becoming the standard cellular phone.⁹ As of December 2010, 63.2 million people in the United States owned smart phones, which is a 60 percent increase since 2009.¹⁰ The increasingly mobile nature of the public through sophisticated smart phones presents a significant opportunity to improve the role of the public in preventing terrorist attacks in the United States.

CURRENT CRISIS COMMUNICATION TOOLS

The U.S. government is reinvigorating the notion that the public can serve as a useful ally during a crisis. In the 2010 *National Security Strategy*, President Obama appropriately recognized that “the ideas, values, energy, creativity, and resilience of our citizens are America’s greatest resource.”¹¹ In pursuit of this goal, the secretary of homeland security launched New York’s Metropolitan Transportation Authority’s “see something, say something” campaign on a national scale to encourage citizens to remain vigilant and report suspicious activity. Similar public awareness campaigns occurred during World War II and the Cold War, but this slogan, written one day after 9/11, is used in a more diverse and ambiguous threat environment. In order for the campaign to be effective, it must issue a clear message on what is suspicious. Although the “see something, say something” campaign comes from a credible source and is an important start to opening dialogic communication with the public, the narrative provides scant details of what the American public should look for that might increase, rather than decrease, uncertainty.

Internet-based social networking tools are also playing an increasingly important role as the U.S. government looks to forge stronger bonds with the public. As of July 2010, twenty-two of twenty-four major federal agencies have official Facebook, Twitter, and YouTube accounts.¹² Many of these agencies, including FEMA, also maintain blogs and mobile websites.¹³ These internet-based

social networking tools, however, require users to pull information from the sites. They have limited capability to leverage the public as force multipliers by distributing actionable information in real-time.

On the mobile front, FEMA is leading the development of an important outreach tool to improve public safety that will employ new and existing communication platforms to rapidly disseminate emergency messages to as many people as possible. This outreach tool – the Integrated Public Alert and Warning System (IPAWS) – will transform the traditional audio-only warnings sent via radio and television. Once implemented, the U.S. government will have the means to send emergency text alerts to cell-phone users within county-sized geographic areas.

Text alerts using IPAWS have a maximum displayable message size of ninety characters, which severely limits the narrative the government can provide to the public.¹⁴ Valuable information can be relayed to the public in ninety characters, but these parameters will make it difficult to disseminate enough actionable information to mobilize the public to prevent an imminent attack from occurring. At this time, there is no clear plan to leverage IPAWS to create a *bidirectional* architecture to communicate with the public during a crisis.

Current and future crisis communication mechanisms such as “see something, say something,” social media sites like Twitter and Facebook, and IPAWS are not the best tools for harnessing public capital in a crisis. None of these communication platforms provide a capability that can fully meet the three criterion of effective crisis communication: a clear, relevant, and timely narrative; openness to dialogic communication; and source credibility. Moreover, even though cellular infrastructure cannot be relied upon post-incident, existing mobile communication tools are overwhelmingly tailored towards response. Crisis communication in the face of an imminent terrorist attack requires a more robust communication platform; the operating environment for prevention is far more ambiguous than that for response. Whereas response operations manage the consequences of an incident that has already occurred, prevention operations attempt to

thwart an incident before it occurs despite many unknowns. It will take collective intelligence from federal, state, and local entities, as well as the public, to reveal usable information about the potential perpetrator, the targeted region, and/or the approach vector.

THE WAY FORWARD: TAPPING INTO THE MOBILE REVOLUTION

The United States government, in partnership with state and local entities, should explore the feasibility of developing a mobile application that can more effectively help the public prevent terrorist attacks. The mobile application should include the capability to disseminate images and descriptive information of the threat to a geographically targeted audience; enable individuals to report suspicious activity by pressing a button to automatically call or text authorities; and notify mobile application users through an active, audible, unique ring tone.

There are several benefits to developing a United States government sponsored mobile application with these capabilities. First, a mobile application meets key elements for effective crisis communication: a clear and relevant narrative, openness to dialogic communication, and source credibility. With potentially millions of eyes on the ground that know who or what to look for, the public would become a valuable bottom-up resource that significantly increases our ability to prevent an imminent terrorist attack from occurring and/or to capture a perpetrator. Popular social media outlets like Facebook and Twitter rely on the user to pull information from the site. There is no automatic pushing of information to the user. A crisis communication mobile application fills that void by allowing officials to rapidly push generalized or localized information to the user *and* pull information back from the public. This capability would enable a large segment of the American public to play a productive role in preventing a crisis from occurring or spreading.

Second, mobile applications are inexpensive and easy to develop. The AMBER Alert iPhone application went from an idea to a finished, fully functional product in one

day. This application includes all current, active AMBER alerts with a small photo of the victim. Each alert contains detailed information about the abduction, including physical description, last known whereabouts, and any details or photos of suspects. A "Report Sighting" button allows an individual to report a sighting of a victim or suspects along with the current GPS coordinates to the investigative agency. These reported sightings can then be geographically aggregated so investigators can better assess the credibility of multiple reports.¹⁵

Lastly, the plethora of information sources – including media outlets, blogs, and twitter feeds – creates a “fog of war” that hinders credible and transparent engagement with the public. A government sponsored mobile application provides a mechanism to manage the message by distributing credible and clear information to users. The public would have a precise understanding of who or what to look for and how to report a sighting. Public sightings made through the mobile application then could be visualized on a map or timeline by using free and open source technology such as the Ushahidi Platform. This platform aided the Haiti Earthquake response and the 2010 Washington, D.C. “snowmagedon” clean up. During a terrorist incident, officials could plot public reports on a map, identify geographic clusters to quickly corroborate reports, and dispatch resources accordingly. This inexpensive, prevalent, and intuitive technology creates a dynamic, multidimensional platform that would enable the U.S. government to do more than simply communicate with the public during a crisis. It also provides a valuable mechanism for the public to communicate with the government during a crisis and for the government to filter, validate, and manage a high volume of reports.

A HYPOTHETICAL EXAMPLE: CRISIS COMMUNICATION DURING A BIOLOGICAL ATTACK

Imagining a scenario provides a practical way to understand the utility of mobile applications in preventing a terrorist attack. This hypothetical biological terrorist attack provides a strong starting point.

The BioWatch Program in New York City, using a series of pathogen detectors, provides initial indications of a widespread aerosol release. State, local, and federal officials scramble to confirm the positive finding and identify the pathogen. If it is a biological attack, prophylaxis must be delivered to all individuals in the affected area within forty-eight hours or the consequences will be dire. As a result, state, local, and federal officials preposition assets and prepare for the distribution of medicine from the Strategic National Stockpile managed by the Centers for Disease Control.

A few hours later, the Laboratory Response Network for Bioterrorism confirms that the pathogen is anthrax. The FBI immediately initiates a manhunt for the perpetrators of this attack (and likely other near simultaneous or follow-on attacks). In support of the FBI, the intelligence community reprioritizes intelligence assets to assist with the identification of perpetrators. These agencies identify a suspect and find indicators that a follow-on biological attack is imminent; however, they cannot pinpoint the expected target or locate the suspect. The president uses the Emergency Alert System to disseminate the threat through traditional means such as television and radio. Local officials with text messaging emergency notification capabilities also deploy messages to the public.

Twelve hours into the incident, communication via the Emergency Alert System and local means have yielded few results. Misguided calls inundate local law enforcement agencies, wasting time and resources. The federal government decides to use a mobile application to disseminate information, including a photo, of the suspect. Those with the mobile application on their phone now know exactly who to look for and, recognizing the seriousness of the situation, forward the picture to

their families and friends. Local law enforcement receives a plethora of tips, but the mobile application, by geographically aggregating all reports, allows investigators to assess the credibility of multiple reports and efficiently deploy assets.

Eight different people report seeing the individual in a white van at a Washington, DC gas station. Law enforcement scrambles resources to the scene and uses the gas station's security cameras to obtain the license plate of the van. Federal officials, working closely with state and local officials, then disseminate a second, targeted message to those in the metro DC area with the mobile application. The message includes the license plate number in addition to the photo of the individual. A tourist outside the U.S. Capitol sees the van parked across the street and immediately reports the sighting through her mobile phone. Shortly thereafter, law enforcement officials receive additional tips via the mobile application. All of these reports are automatically plotted in Google Maps and law enforcement officials quickly recognize that the follow-on tips provide strong evidence that the initial report was credible. All resources are immediately dispatched to the incident scene. The perpetrator is apprehended and the second attack is prevented.

It may be just a matter of time until a scenario such as this occurs. The proposed mobile application will not necessarily prevent all terrorist attacks. It could, however, give the nation its best chance to prevent an imminent terrorist attack from occurring by rapidly marshaling the public in a cost-effective and timely manner.

THE PRIVACY CHALLENGE

Pursuing this initiative will entail overcoming a significant, but not insurmountable, privacy issue. Individuals will likely express concerns about having a government sponsored

application on their mobile device. In order to address these challenges, the federal government should construct the mobile application program along the following guidelines. First, it must be a free service for all users. Second, individuals who do not want to participate may opt out at any time. Third, the mobile application must adhere to the most stringent privacy controls available and will not collect personal data. Fourth, the government must only transmit messages via the mobile application during an emergency. The mobile application should not bombard individuals with daily or even monthly messages from the government. Lastly, an outreach campaign should include a frank discussion with the American public regarding the vital role of individuals in preventing terrorist attacks and the benefits of participating in the mobile application program.

CONCLUSION

In the world of homeland security, mobile phones are too often viewed as detonation devices rather than crucial communication mechanisms. In order to significantly tilt the odds against the terrorists and in favor of the “good guys,” the nation’s crisis communication strategy must be broader and more innovative than commercial broadcast alerts, mobile text messages, and social media sites such as Facebook and Twitter. Federal, state, and local officials, in concert with the public, should adopt a strategy that leverages mobile technology and harnesses the power of mobile applications. There is no silver bullet solution to preventing terrorist attacks, but mobile applications provide a more robust mechanism to tap into millions of eyes on the ground during a crisis and the tool the public needs to “see something, say something.” It is a new form of the old neighborhood watch concept, providing expanded situational awareness to the public during a crisis and better intelligence leads to prevent and apprehend the “bad guys.”

About the Author

Andrew Heighington serves as the special assistant to the assistant secretary of defense for Homeland Defense and America’s Security Affairs. In this role, Mr. Heighington assists the assistant secretary on several cross-cutting portfolios related to homeland defense and homeland security planning, national preparedness, and counterterrorism. Heighington graduated summa cum laude from the University of Richmond and is a member of Phi Beta Kappa. He is currently pursuing his master’s degree in Security Policy Studies at George Washington’s Elliott School of International Affairs. He may be contacted at Andrew.Heighington@osd.mil.

The opinions expressed here are the views of the author and do not necessarily reflect the views or opinions of the United States government or of the Department of Defense.

-
- ¹ Charles R. Berger and Richard J. Calabrese, "Some Explorations in Initial Interaction and Beyond: Toward a Developmental Theory of Interpersonal Communication," *Human Communication Research* (Fall 1975): 99-112.
- ² Sung Yung Yang, Minjeong Kang, and Philip Johnson, "Effects of Narratives, Openness to Dialogic Communication, and Credibility on Engagement in Crisis Communication through Organizational Blogs," *Communication Research* 37 (2010): 475.
- ³ *Ibid.*, 474.
- ⁴ Brian Stelter and Noam Cohen, "Citizen Journalists Provided Glimpses of Mumbai Attacks," *New York Times*, November 29, 2008, <http://www.nytimes.com/2008/11/30/world/asia/3otwitter.html>.
- ⁵ Chris Kanalley, "Fort Hood Shooting Shows How Twitter, Lists Can be Used for Breaking News," *Poynter*, November 6, 2009, <http://www.poynter.org/how-tos/digital-strategies/e-media-tidbits/99282/fort-hood-shooting-shows-how-twitter-lists-can-be-used-for-breaking-news/#>.
- ⁶ Michael P. Boyle and others, "Information Seeking and Emotional Reactions to the September 11 Terrorist Attacks," *Journalism and Mass Communication Quarterly* 81, no. 1 (Spring 2004): 155-167.
- ⁷ "FEMA Administrator Fugate Addresses American Red Cross on Use of Social Media in Emergency Management," August 12, 2010, <http://www.fema.gov/news/newsrelease.fema?id=52362>.
- ⁸ This essay adopts the National Response Framework definition of response: "Immediate actions to save lives, protect property and the environment, and meet basic human needs;" and the 2006 Post-Katrina Emergency Management Reform Act definition of prevention: "any activity undertaken to avoid, prevent, or stop a threatened or actual act of terrorism."
- ⁹ 89 percent of Americans have cellular mobile phone subscriptions compared to 79 percent of Americans who use the Internet. Source: World Bank, "Mobile Cellular Subscriptions," http://data.worldbank.org/indicator/IT.CEL.SETS.P2?cid=GPD_43.
- ¹⁰ "comScore Reports December 2010 U.S. Mobile Subscriber Market Share," February 7, 2011, http://www.comscore.com/Press_Events/Press_Releases/2011/2/comScore_Reports_December_2010_U.S._Mobile_Subscriber_Market_Share.
- ¹¹ Barack Obama, *National Security Strategy*, May 2010: 16.
- ¹² Gregory Wilshusen, "Challenges in Federal Agencies Use of Web 2.0 Technologies," Government Accountability Office, July 22, 2010, <http://www.gao.gov/new.items/d10872t.pdf>.
- ¹³ For more information on FEMA's blog see: <http://blog.fema.gov>.
- ¹⁴ Federal Communications Commission, "New Commercial Mobile Alert System" (2010), <http://www.fcc.gov/cgb/consumerfacts/emas.html>.
- ¹⁵ Chris Foresman, "iPhone forensics expert creates AMBER Alert app for iPhone," February 17, 2009, <http://arstechnica.com/apple/news/2009/02/iphone-forensics-expert-creates-amber-alert-app-for-iphone.ars>.



Copyright © 2011 by the author(s). Homeland Security Affairs is an academic journal available free of charge to individuals and institutions. Because the purpose of this publication is the widest possible dissemination of knowledge, copies of this journal and the articles contained herein may be printed or downloaded and redistributed for personal, research or educational purposes free of charge and without permission. Any commercial use of Homeland Security Affairs or the articles published herein is expressly prohibited without the written consent of the copyright holder. The copyright of all articles published in Homeland Security Affairs rests with the author(s) of the article. Homeland Security Affairs is the online journal of the Naval Postgraduate School Center for Homeland Defense and Security (CHDS).

<http://www.hsaj.org>

