Terse Message Amplification in the Boston Bombing Response

Jeannette Sutton
Trauma, Health & Hazards Center
University of Colorado
Jsutton2@uccs.edu

Emma S. Spiro
Department of Sociology
University of California
sean.fitzhugh@uci.edu

Sean Fitzhugh
Department of Sociology
University of California
sean.fitzhugh@uci.edu

Britta Johnson
Trauma, Health, & Hazards Center
University of Colorado
Bjohns17@uccs.edu

Ben Gibson
Department of Sociology
University of California
cbengibson@gmail.com

Carter T. Butts
Department of Sociology
Department of Statistics
Institute for Mathematical Behavioral Sciences
University of California
buttsc@uci.edu

ABSTRACT

On the morning of April 15, 2013, an Improvised Explosive Device (IED) was detonated near the finish line of the Boston Marathon, resulting in a large number of casualties. This generated a week-long response under the US National Incident Management System. In this paper, we examine online, terse messages broadcast by responding organizations and their amplification by other official entities via retransmission. Content analysis of official messages shows strong similarities with posting patterns previously observed in response to natural hazards, with the primary exception of themes related to the criminal investigation, suggesting a possible revision of guidelines for public information in light of the needs arising from extended counterterrorism operations undertaken in an urban environment. Network analysis demonstrates message posting and amplification were dominated by local actors, underscoring the importance of local readiness for management of official public information activities in the context of extremely high-profile events.

Keywords

Message Amplification, Terse Messaging, Twitter, Terrorism, Public Information, Boston Marathon Bombing

INTRODUCTION

New communication channels and terse messaging technologies, such as social media, have recently garnered considerable attention because of their heightened use during times of crisis as platforms for exchanging alert and warning information. Messaging strategies have moved from audible sirens overhead to mobile "sirens" in the pockets of the everyday smartphone user. With this move has come an increased interest in sharing and disseminating warnings through online networks via terse messaging. Terse messages are defined here as brief messages that are easily shared and quickly propagated, have the potential to reach large numbers of online users, in real time, disseminating information at critical points of a hazard event. While not communicated exclusively via technology, terse messages can be readily identified on such channels as SMS or text messaging (limited to 160 characters), Wireless Emergency Alerts, or WEAs (limited to 90 characters), and Twitter messages (limited to 140 characters). The content of terse messages and their online amplification by user accounts of public officials via Twitter is the focus of this analysis.

This paper will provide the first examination of terse messaging by public officials following a domestic terrorist attack, the Boston Marathon bombing. Drawing from a dataset of 31 official Twitter accounts that were actively tweeting during the week of the bombing and manhunt, we examine the content of terse messages and their amplification across online social networks. Our analysis focuses on (1) how the content of these terse messages conforms to guidance for risk communication about Improvised Explosive Devices (IED) and (2) the message generation and retransmission activities of official public safety organizations. Most specifically, we explore which organizations amplify each other's messages during a high profile IED event. We begin by providing background on terse messaging and the IED hazard. We then describe our research context and methods. Finally we conclude with a discussion of the implications of our results for terse messaging strategies.

BACKGROUND

Terse Messaging for Hazard Events

There is an extensive history of research on alerts and warnings for disaster events (Mileti and Sorensen 1990), focusing on messaging channels (Sorensen 2000), sources (Lindell and Perry, 1987; Stephens, Barrett, and Mahometa, 2013), content (Mayhorn and McLaughlin, 2012; Mileti and Fitzpatrick, 1991), and hazard type (Drabek, 1999) in relation to decisions to take protective action (Mileti and Sorensen, 1990). Importantly, Mileti and Sorensen (1990) identified message content and message style as the primary motivators for public protective action taking. Until recently these studies focused almost entirely on long messages, i.e. those that could be delivered over broadcast channels and were unrestricted in their contents and length. With the advent of social media and other short messaging channels, alerts and warnings have become part of the "terse communication regime" as messaging moves to online and mobile devices. Recent research examining terse messaging in disaster has identified distinct patterns of message content and style (Sutton et al., 2013) that differ from guidance developed for longer broadcast messages. In addition, this research has indicated that message amplification, via public retransmission of messages at periods of heightened stress, can be predicted in part from message content and style (Sutton et al., 2013; Spiro et al., 2013). Amplification is of primary interest because it increases the size of the population exposed to the warning/hazard message. Messages that use directive and instructional sentence style, are organized along an identifiable hashtag channel, and include content about the impact of the hazard and protective action guidance will receive considerably more retweets than those that do not (Sutton et al., 2013). While previous studies offer preliminary explanations of the terse messaging regime, many open questions remain, particularly during IED events where guidance to the public on which protective actions to take may differ.

Terrorism Communication: The Hazard, Message Content and Message Amplification

Terrorist activity is described as violent, premeditated acts, motivated by a political, religious, or ideological objective, intended to have psychological and social impacts beyond the immediate violence, targeted toward unarmed, non-combatant persons unable to defend themselves (Banks et al., 2007). It often occurs without forewarning, with the possibility of multiple attacks, and thus presents a highly unfamiliar hazard to the public (Gerber et al., 2006). Terrorist activity is intended to increased levels of fear and uncertainty in a target community, and it is often successful in doing so (Marshall et al., 2007). IEDs are widely recognized as being a weapon of choice among those engaged in terrorist attacks; they are frequently used by terrorists throughout the world (National Science and Technology Council, 2008). However, IEDs have been less utilized in the United States: before the 2013 Boston Marathon bombing there were relatively few high-profile instances of such attacks (e.g. the Atlanta Olympic Park Bombing in 1996 and the Oklahoma City Bombing in 1995). As a result, local civic leaders have had few opportunities to issue warnings or instructions about direct threats to public safety and security posed by terrorists via IEDs (Covello et al., 2010). Recent studies on *public* uses of Twitter in the aftermath of terrorist incidents have revealed broad and widespread attention (Cheong and Lee, 2010) that may be useful for official situational awareness tracking (Oh et al., 2010). Our research centers on the communication strategies and terse messages generated by *public officials* in the aftermath of an IED attack.

Despite limited historical precedents, there is a growing recognition that effective risk communication strategies are needed for IEDs, even in the absence of official protective action guidance from Federal level agencies (Bean et al., 2013). Recently the U.S. Department of Homeland Security released a report (Covello et al., 2010) that draws from a comprehensive overview of general risk communication guidance. From this, the leading recommendation stated that a "a primary goal of IED risk communication is to inoculate people against, or counteract, the social and economic messages that terrorists intend to convey" (p 14), which can be accomplished through four key messages: (1) Warn citizens of imminent attack; (2) provide instructions to reduce potential injuries, casualties, and disruption; (3) gain the assistance of citizens in identifying suspicious activities or indicators of terrorist activities; and (4) enhance social cohesion, social resilience, and confidence in authorities (p. 15). These communication strategies, while not unique to risk communication, are novel when they are delivered in real time, via terse messaging channels, over the course of a disaster event.

In addition to distinct risk communication strategies, terrorism incidents, such as for an IED event, result in complex response contexts. Responsibility for response activities during the incident and subsequent law enforcement investigation shifts over the course of the response period. The National Incident Management System (NIMS) is part of the National Response Framework, developed by the Federal Emergency Management Agency as a way to standardize command and communication structures in response to disaster events at a local, State and national level by outlining Emergency Support Functions (ESFs) that delineate responsibilities and resources to organizations in a disaster scenario (DHS, 2008). According to NIMS, local authorities are the first to respond. When their resources are overwhelmed, NIMS activates State Emergency Operations Plans, and when State resources are overwhelmed the Federal level activation begins. While the FBI leads the criminal investigation related to the incident (DHS, 2004), the Public Information function remains a coordinated effort among local, State, and Federal public safety agencies throughout the response (DHS, 2004). How these coordinated communication activities play out, in a publicly visible, online communication space, following a terrorist incident, is understudied.

This research builds upon prior work on terse messaging over social media in natural disaster incidents, and extends findings to a recent terrorist event, the Boston Marathon bombing and subsequent manhunt.

METHODS

The Research Context

On Monday morning, April 15, two Improvised Explosive Devices went off near the finish line of the Boston Marathon, killing three spectators and injuring more than 200 others. During the week that followed, memorials were held (April 17), two suspects were identified (April 18), and a shootout occurred resulting in the death of the first suspect and an MIT campus police officer (April 18). The events lead to shelter-in-place orders and more than one million people across the city of Boston and contiguous areas were placed on lockdown for close to 24 hours while a massive search was undertaken. The manhunt resulted in the capture of the second bombing suspect in the late hours of the day on Friday, April 19.

In preparation for the Boston Marathon, the MA State Emergency Management Plan was already in "full activation" for the race, meaning that all State ESFs were present and prepared to respond to the marathon itself. When the bombings occurred on the day of the race, it was the responsibility of the State Public Information Officer from, Massachusetts Emergency Management Agency, to provide and disseminate information to the general public. Within moments following the bombings, MA Governor Deval Patrick requested an Emergency Declaration, activating a Federal level response. FEMA Region 1 assumed responsibility for coordinating information between media, Congressional, Federal and local agencies, while local and State agencies took on a supporting role to keep the public informed and safe.

Over the course of the week, social media sites, Twitter in particular, gained significant attention due to their utilization by both the general public and government officials. Popular media sites posted articles about social media use by local public officials (govloop.com; computerworld.com). The reports also noted the benefits and drawbacks of such community engagement, as members of the public tweeted police chatter (nbcnews.com) and banded together in attempts to identify suspects from images captured at the scene of the event (cbsnews.com). In addition to mass media attention on the heightened use of Twitter, previous research also supports the convergence of attention online. Key Twitter accounts held by local public officials experienced dramatic surges in attention as they provided real time updates from the scene of the bombing and additional messages throughout the week. Boston Police gained 273,000 new followers, Massachusetts State Police picked up nearly 26,000 followers and the Mayor of Boston, Tom Menino, experienced an increase of nearly 17,000.

Data Collection

We identified and enumerated a census of 31 Twitter accounts for the Boston event analysis. These targeted accounts were identified because they represent the population of public officials at the local, State, and Federal level who were serving in a public safety capacity prior to the marathon and actively tweeted over the course of the week. The set of accounts satisfying these criteria were identified through two processes. First, we searched through our set of user accounts that were already in our data collection system and were within the geographical boundaries of the Boston region, the State of Massachusetts, or represented Federal response agencies having a role in terrorism and disaster. Secondly, we manually sifted through the Twitter Friend lists of local official organizations to identify additional accounts that may not routinely tweet, but could play a public information role, and we looked for any account that was mentioned or retweeted in posted content from the official accounts. We did not choose to include local media as part of the targeted account set because our interest lay in the message content and amplification from public officials during a terrorist incident. In total we have 31 accounts: 17 represent local, 10 represent State, and 4 represent Federal entities, making a combined total of 1122 tweets.

For each of the enumerated targeted accounts, we retrieved their posting behavior history, along with actor level attributes using the Twitter REST API. The data collection query allows one to obtain all messages posted to the public timeline and the timestamp for each post (up to some historical limit). The data collection query was performed daily over the week long period of interest to ensure no messages were missed. For each message we also obtained a count of the number of times that each message was retweeted (at the time of last data collection). Actor or user level attributes collected include the number of followers of that account at the time of collection, the location of the user, the account creation date, and the time zone of the account. For the subsequent analysis, we consider the all messages posted by our set of targeted accounts, from April 15, 2013 12:01 am (the day of the marathon and bombing) until 11:59pm on April 19, 2013 (after the manhunt was concluded).

Data Analysis

We examine the content of publicly visible terse messages (i.e. tweets) disseminated by officials over the course of a week; this encompasses the period immediately following the bombing and the entire course of the manhunt, and concludes with the period in which the suspects were captured. Moreover, we also explore message amplification by analyzing the networks of information propagation among official Twitter users, in order to identify which organizations support the online communication processes of other organizations.

Content Coding

Two researchers manually coded the entire set of official tweets for the week long period, utilizing a closed coding strategy that was developed during previous research on terse messaging via Twitter during a wildfire event (Sutton et al., 2013). To begin, we independently scanned all original tweets to determine that the original coding categories fit with the Boston event data. We also met to discuss any emerging themes. Next, the set of original tweets was split-recoded by both researchers, with one half being blind recoded by each researcher and then exchanged and checked for intercoder agreement. Coders agreed on primary theme codes in approximately 98% of cases, and on both primary and secondary theme codes in 94% of cases. Disagreements were resolved by consensus, following discussion of problematic cases by the coders. We found 10 primary themes (plus two additional categories; one for tweets that are not on-topic and one that did not fit into any category), ranging from evacuation guidance (including pre-evacuation and sheltering) to hazard information (such as phone numbers and resources).

A second round of content coding was conducted by a single researcher, to identify content that addressed the four categories of IED risk communication recommended by Covello et al. (2010). These included: (1) warning themed messages (which conformed to guidance and advisory messages); (2) instructional messages (advisory and information themed messages); (3) requests for assistance (information themed messages); and (4) resiliency enhancing messages (prayers and thanks, hazard impact, and emotive content). In total 320 out of 1122 messages analyzed conformed to the IED message recommendations.

Both researchers also manually coded each tweet for aspects of message style. Style aspects, which emphasize how content is relayed or displayed to affect message specificity or clarity (Mileti and Sorensen, 1990) include the following: how each tweet sentence functions within the English language as either declarative, imperative, interrogative, or exclamatory; whether a tweet includes a word or phrase in ALL CAPS and if these words function as either a category signifier or to emphasize a portion of the tweet. For both content and style, messages were coded in a non-mutually exclusive manner; a single tweet could contain several types of content as well as multiple sentence features or other stylistic aspects. In addition, we used automated procedures to code for conversational microstructure elements within the tweet (i.e. conventional aspects of Twitter-based syntax that lend to message retransmission or engagement with other users). These include whether the tweet was directed at or responding to another Twitter user (@name), whether it was a retweet (RT), the presence of a hashtag keyword, and a reference to further information available online in the form of links to URLs (usually shortened by using bit.ly or another short URL service).

Amplification Network

We create a social network to represent our targeted accounts' amplification of one another's messages over our week-long period of interest. In this network, a tie from actor A to actor B reflects actor B's retweet of one of actor A's messages. *The directed ties thus reflect the flow of messages from originator to amplifier.* We illustrate the network below in Figure 1, where each colored circle represents one of the Twitter accounts in our targeted set and an arrow represents an amplification relationship as described previously. Although we have 31 targeted accounts, we only illustrate the 26 accounts that retweeted or were retweeted by at least one of our targeted accounts. Below we illustrate message amplification among these targeted accounts.

In Figure 1 we colored nodes according to their sphere: local, State, and Federal, as shown in the legend. The figure illustrates 17 local accounts, 8 State accounts, and 1 Federal account. We have scaled the size of nodes based on the number of times they amplified others' messages. Therefore, nodes who retransmitted many messages are the largest nodes in the above network.

RESULTS

Content

Across the entire corpus of tweets for this event, "information" messages (such as non-instructional messages that include situational updates, links to available resources, and images of the suspects) were most prevalent (40%), followed by "closures and openings" of transportation, roads, and services (19%), and "advisory" messages requesting that people clear the area of the bombing and the actions to take while the city was on lockdown (15%). "Shelter in place" messages are a variant of advisory messages that provide specific guidance about how to protect oneself in a disaster. These were observed at the end of the week (5%) during the manhunt. Messages that include "thanks" or "emotive content" about the heroism of the first responders, condolences for those who died, and encouragement for Boston Community to stay strong followed (5% and 7% respectively). Few tweets focused on specifics about the "hazard impact" (3%), and "correcting" misinformation (1%). We show how these content themes vary across organization by sector in Figure 2 below.

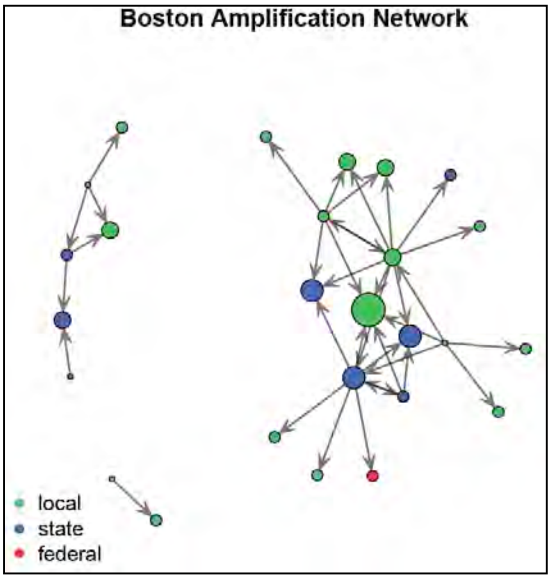

Figure 1: Message amplification network among targeted accounts. Nodes represent actors, with ties from original poster to retweeters.

IED-related Content

While most of the tweets considered in the content analysis did not include content that directly complied with recommended message content for IED attacks (Covello et al., 2010), we do observe messages that speak directly to IED guidance. Approximately 25% of the total tweet corpus contains content conforming to the four recommendations. Some messages warned citizens of imminent attack (recommendation #1); these messages fall into the categories of "guidance" and "information" in our coding scheme. These messages instructed people to be vigilant and on alert (on the day of the bombings), and provided notice that armed and dangerous persons were at large and under pursuit (on the day of the manhunt). Other tweets provided instruction to reduce potential injuries casualties, and disruption, (recommendation #2). These kinds of tweets fall primarily into the categories of general "advisories" and "shelter in place" notices. The majority of these tweets advised people to clear the area around the marathon finish line, not to congregate in large crowds or travel in large groups, stay home, away from windows, with doors locked, and to comply with authorities. Additional instructional messages were provided to reduce mental health related disruption and service closures, but did not directly address issues related to potential injuries or casualties. The largest number of messages that comply with recommended IED message content focus on gaining the assistance of citizens in identifying suspicious activities or indicators of terrorist activities (recommendation #3). In our categorization, these tweets were "advisory" and "information" themed messages. Many messages of this type include requests to submit tips, video, and photos, as well as the dissemination of tipline numbers, email and website addresses. In addition, requests were made that the public not broadcast tactical information during the manhunt on the last day of the week. Finally, we find messages that may aid in enhancing social cohesion, social resilience, and confidence in authorities (recommendation #4). These messages were represented by "thank you" and "emotive" content in our schema. Many of these tweets include statements about coordination of leadership across all levels of government, heroism by the first responders, thanks to the generosity of volunteers, remembering those who were injured or killed, and calling up images of strength, neighborliness, and resiliency of the city of Boston.

Microstructure

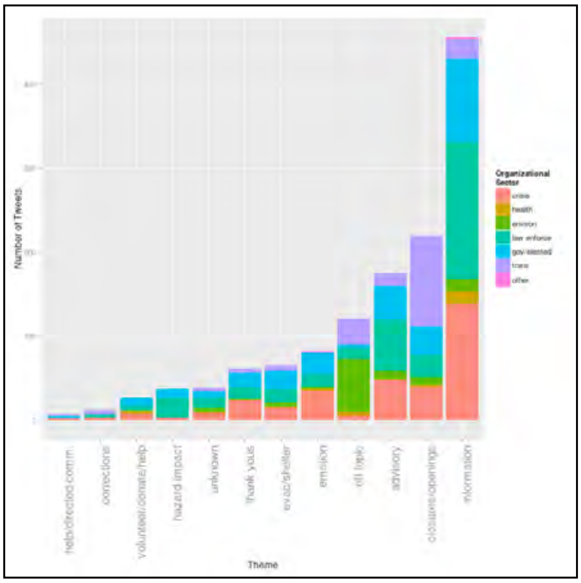

Figure 2: Number of themed tweets posted by each organizational sector over the period of observation.

An additional aspect of the message content focuses on the microstructure included within terse messages. Here we look at the mean proportion of messages containing each microstructure element, based upon the level of government in which they operate – the organizational sphere. We focus on the inclusion of a URL, the use of a hashtag, and directed messages.

The most consistently included microstructure element is a URL, providing a link to additional information; in general, included URLs point primarily to the websites of official organizations, images from the scene, and pictures of the suspects. URL inclusion ranges from nearly 80% of messages posted by Federal accounts to 60% of messages posted by local and State accounts. The second most consistently included microstructure element is the hashtag; 41.7%of local accounts' messages and 34.1% of state accounts' messages contained hashtags. Federal accounts had the highest percentage of messages with hashtags (60.0%), but the lowest number of total messages (15), by a substantial margin. Interestingly, unlike other crisis events, there was no indication that a consistent hashtag was used by official organizations to organize their content into a traceable stream. Hashtags that were utilized varied by sector, such as #tweetfromthebeat, #WANTED, and #CommunityAlert by law enforcement, and #oneboston from local government, indicating different aspects of the response. The least used microstructure feature is the directed message (@username), indicating a message is targeted to a specific user, most likely in reply to a specific question or comment. While local accounts did make use this element more than other spheres, their use was still relatively infrequent.

One additional microstructure that we examine is the inclusion of the retweet (RT). Importantly, we see that most of the tweets with "original content" (non-retweets) come from local and State organizations. Nearly 40% of Federal tweets are retweeted messages, signifying a role of reinforcing or echoing local and State messages in a disaster response.

DISCUSSION

Terrorism has been described as "a form of communication employing physical violence in the hopes of achieving specific political objectives" (Covello et al., 2010, p 3). The use of modern online communication tools in response to violent attacks is a demonstration of the ability of public officials and emergency responders to provide information quickly and accurately, which "is critical to saving lives, preventing widespread damage, and maintaining social cohesion and the citizens' trust in government" (Covello et al., 2010, p 6). This research has shown that terse messages for an IED attack are disseminated and amplified via social media at key points in the response. While the broad corpus of messages included information outside of the four recommended risk communication guidance areas (as seen in Figure 2)., there was considerable attention directed to reducing harm, soliciting help from the public, and offering reassurances to enhance community resilience.

Message Content and Post Event Instructions

The messages generated and disseminated by public officials during the Boston marathon response, spanned a variety of content areas many of which were consistent with findings from other recent events (Sutton et al., 2013). Importantly, the content themes identified in terse messages disseminated in the warning phase of a disaster are similar regardless of the hazard, be it a natural disaster or terrorist attack, with a great deal of advanced notice or none at all. Information about hazard impact, guidance on how to protect oneself, and public safety advisories are consistently relayed to the public in 140 characters or less at key points in time of the warning process. Aspects of the official communications following this event that appear to differ from natural hazard events (see Sutton et al., 2013; Spiro et al,. 2013), include the significant attention to messages that are specific to the criminal investigation, including requests for assistance, and those that promote social cohesion and resilience. Additional studies on human induced disasters and mass casualty incidents are needed to provide additional insight on these messaging activities.

Advisories and guidance-focused messages were provided during the initial event response, the city lockdown and resultant manhunt. These messages were largely imperative and articulated in prose style, telling users exactly what to do to protect themselves. Instructional messages have been found to increase protective action taking in hazard events (Sellnow et al., 2012). Importantly, the Department of Homeland Security has not yet identified the specific content on protective action guidance that should be included in a warning message for an IED (Bean et al, 2012). As new alert and warning technologies for mobile devices are developed, it will be important to develop post event instructional guidance based upon the restrictions found in the terse messaging regime.

Assistance of Citizens

Public officials utilized Twitter to request assistance from citizens throughout the week, primarily in response to the criminal investigation, and later to protect the safety of police officers. Immediately following the bombing, requests were made for video, photos, and any tips that may have been relevant. At the end of the week, additional requests were made to help identify and locate the suspects. In contrast with the response to other disaster events, where citizen volunteers have often been portrayed as a problem to be managed (Dynes and Tierney, 1994), the collaborative efforts of a distributed public may have contributed to a sort of self-organized digital volunteer activity (Starbird and Palen, 2011) contributing to collective intelligence (Vieweg et al., 2008), organized by officials utilizing public information. While many scholars have recognized the benefits of crowdsourcing and digital volunteers, there are also potential dangers. During the Boston manhunt, for example, some of these efforts led to the misidentification of a suspect (Kaufman, 2013).

Social Cohesion

Terrorist events often occur suddenly and without warning; they expose many to horror, appear to be beyond the control of any one person, threaten life and the lives of family members and friends, and place excessive demands on coping (Sattler, 2002). Research suggests that many of these characteristics are associated with survivors' reporting that they feel some loss of their sense of control, predictability, safety, and trust (Baum, 1991; Updegraff and Taylor, 2000). Because of the potential for negative psychological effects, communication strategies following a terrorism event include messages of social cohesion and resilience. After the events in Boston, public officials used terse messages to reassure the public that government agencies were responding collaboratively and expeditiously while exhorting the community of Boston that they are "one Boston" and "Boston strong." Here the terse message platform of Twitter served as a public soapbox for officials to exhibit empathy for those directly affected and show leadership through their words.

Coordination, Amplification, and Engagement

Coordination among disaster response agencies came under particular scrutiny following the September 11, 2001 attacks on the World Trade Center (9/11 Commission Report). As a result, the National Incident Management System (FEMA, 2004) was created to systematize communication processes among response organizations. Message coordination is important for establishing lines of authority, preventing the sharing of conflicting information, and garnering public trust (Mileti and Sorensen, 1990). During the Boston bombing, we found that local organizations remained the lead communicators and were amplified at both the local and State level as seen in Figure 1. This demonstrates that some coordination was present among civic government agencies while the State performed a supporting role. This is consistent with the axiom that "all disasters are local," (Quarantelli, 1982) even under circumstances where significant Federal resources are deployed. However, a single, consistent Twitter hashtag as an event-related information channel, supported by the leading response agencies, was never reached during this event. Hashtags aid the formation of ad-hoc publics, and emerge through pre-planning or consensus. As such they serve to means of "coordinating a distributed discussion between more or less large groups of users, who do not need to be connected through existing 'follower' networks." (Bruns and Burgess, 2011). Given that the bombing and manhunt gained significant international attention, the lack of a hashtag raises questions about the nature of coordinated interorganizational communication during this event.

Risk communication can, and should, function as a dialogue among organizations, government agencies, and all relevant stakeholders (NRC, 1989). Although crisis situations create an inherent constraint on dialogue (Heath and O'Hair, 2009), social media offers a channel for direct engagement with the public -- shifting away from traditional patterns of linear warnings (Sellnow, Ullmer, Seeger and Littlefield, 2009). The lack of direct public engagement or conversations with the public through online channels during this event demonstrates patterns consistent with those identified in prior studies (Sutton et al., 2013). Local organizations have more directed communication with individual followers, however the limited nature of this engagement shows that transactional communication strategies (Seeger and Sellnow, 2013) with feedback loops, have not yet been fully integrated. In contrast with direct message engagement, we found that a significant number of messages posted by official accounts included URLs. Many of these linked to images of the suspects, first requesting public help to identify them, later to physically locate them and facilitate their capture. This use of social media -- as a criminal investigation tool -- is not unusual (Heverin and Zack, 2010), however when viewed as a tool for public engagement, it demonstrates a link between public safety and stakeholders, offering opportunities for the public to collaborate and assist through a backchannel communication tool at a period of heightened stress (Sutton et al., 2008). At the same time, this kind of messaging behavior points to use of social media as additional broadcasting channels, rather than as a conversation mechanism.

CONCLUSION

In September 2013, Twitter announced that it was launching an alert service for emergency management organizations to share time sensitive and safety critical information with Twitter users (Protalinski, 2013). With this new service, it becomes imperative that online public communicators develop effective terse messaging strategies. Attention must be directed to message content, as well as networked coordination and strategies to amplify key messages to a broader audience. This study serves as the first examination of terse messaging over Twitter in response to an IED event.

In this research, we find that only a quarter of the messages provided by official accounts over the week long IED response and manhunt conformed to recommended guidance for risk communication content in this situation. Many of these messages included links to additional information and were amplified by networked user organizations. More broadly, these findings suggest that there is a specific set of messages that can be preliminarily drafted to meet the standards and character limitations of terse messaging formats, such as Twitter, SMS, and Wireless Emergency Alerts. As we learn more about appropriate protective actions for IED attacks, very specific instructional messages (Sellnow et al., 2012) can be created to prevent further casualties. Such messages will become vital for communicating with the public in the immediate aftermath of any attack without forewarning where reducing loss of lives and increasing safety is the first priority.

Pre-event coordination for utilizing social media platforms during future events should not be limited only to who leads, but also to who amplifies messages and who serves in a supporting role. Our findings suggest that messages generated at the local level are amplified at the local level, but also distributed more broadly by State agencies. In contrast, Federal agencies, while not promoting messages from local agencies, offer a supporting role by posting information relevant to the broader public. Such coordination could be included as part of future strategic planning. In addition, pre-planning must include strategies to develop and converge around event-specific channels via Twitter hashtags (or other kinds of metadata/tags) in order to coordinate terse messaging across a distributed and remote audience facilitating both searching and dissemination of relevant information. Such efforts will benefit those who follow a disaster event and serve to validate the effective coordination of public information and response functions.

ACKNOWLEDGEMENTS

This research us supported by the National Science Foundation awards CMMI-1031853 and CMMI-1031779. Any opinions, findings and conclusions, or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of NSF.

REFERENCES

1. Averill, J. D., D.S. Mileti, R.D. Peacock, E.D. Kuligowski, N. Groner, G.Proulx, P.A. Reneke, and H.E. Nelson. (2007). *Federal building and fire safety investigation of the World Trade Center disaster: Occupant behavior, egress, and emergency communications*. NIST NCSTAR 1-7.
2. Banks, W. C., De Nevers, R., and Wallerstein, M. B. (2007). *Combating terrorism: Strategies and approaches*. Washington D.C.: CQ Press.
3. Baum, A. (1991). Toxins, technology, and natural disasters (97–139). *Stress and Coping: An Anthology (3d Edt.)*. Columbia University Press: New York, NY.

4. Bean, H., Fisher, B., Madden, S., Mileti, D., Sutton, J., and Wood, M. (2013). *Hazards and protective actions sequence matrix: Comprehensive testing of imminent threat public messages for mobile devices.* College Park, MD: National Consortium for the Study of Terrorism and Response to Terrorism, Department of Homeland Security Science and Technology Center of Excellence, University of Maryland.
5. Bruns, A., and Burgess, J. E. (2011). *The use of Twitter hashtags in the formation of ad hoc publics*. In 6th European Consortium for Political Research General Conference, 25 - 27 August 2011, University of Iceland, Reykjavik
6. Cheong, M. & Lee, V.C.S. (2010). A microblogging-based approach to terrorism informatics: Exploration and chronicling civilian sentiment and response to terrorism events via Twitter. *Information Systems Frontiers*. 13(1), 45-59.
7. Chuck, E. (2013, April 19). Tweeting police chatter creates confusion over Boston suspect. *U.S. News.* Retrieved from http://usnews.nbcnews.com/
8. Covello, V., Becker, S., Palenchar, M., Renn, O., Sellke, P. (2010). *Effective risk communications for the counter improvised explosive devices threat: Communication guidance for local leaders responding to the threat posed by IEDs and terrorism*. Burlington, MA: The U.S. Department of Homeland Security, Science and Technology Directorate, Human Factors/Behavioral Sciences Division.
9. Department of Homeland Security. (2008). *National Incident Management System* (FEMA Publication P-501). Washington, D.C.: U.S. Department of Homeland Security.
10. Department of Homeland Security. (2004). *National Incident Management System* (FEMA Publication). Washington, D.C.: U.S. Department of Homeland Security.
11. Department of Homeland Security. (2004). *National Response Plan* (Terrorism Incident Law Enforcement and Investigation Annex TER 1-14). Washington, D.C.: U.S. Department of Homeland Security.
12. Dynes, R. R., and Tierney, K. J. (Eds.). (1994). *Disasters, collective behavior, and social organization* (p. 130). Newark, DE: University of Delaware Press.
13. Drabek, T. E. (1999). Understanding disaster warning responses. *The Social Science Journal*, *36*(3), 515-523.
14. Gaudin, S. (2013, April 19). Update: Boston police use Twitter to inform residents during manhunt. *Computerworld*. Retrieved from http://www.computerworld.com/
15. Gerber BJ, Ducatman A, Fischer M, Althouse R, Scotti JR (2006). *The Potential for an uncontrolled mass evacuation of the DC Metro area following a terrorist attack: A report of survey findings*. Report presented to Secretary James W. Spears, West Virginia Department of Military Affairs and Public Safety. West Virginia University: Morgantown, WV. www.hsp.wvu.edu/r/download/20487
16. Heath, R. L., and O'Hair, H. D. (2009). The significance of crisis in risk communication. *Handbook of Risk and Crisis Communication* (pp 5-31). New York, NY: Taylor and Francis Group.
17. Heverin, T., and Zach, L. (2010). Twitter for city police department information sharing. *Proceedings of the American Society for Information Science and Technology*, *47*(1), 1-7.
18. Jarvis, E. (2013, May 28). @Boston_Police - CTO John Daley talks Twitter and the bombings [Blog post]. Retrieved from http://www.govloop.com/
19. Kaufman, L. (2013, April 28). Bombing trip up Reddit in its turn in spotlight. *New York Times*. Retrieved from http://www.nytimes.com/
20. Keeney, R. L., and Winterfeldt, D. (1986). Improving risk communication. *Risk analysis*, *6*(4), 417-424.
21. Lindell, M. K. (1987). Warning mechanisms in emergency response systems. *International Journal of Mass Emergencies and Disasters*, *5*(2), 137-53.
22. Marshall, R. D., Bryant, R. A., Amsel, L., Suh, E. J., Cook, J. M., and Neria, Y. (2007). The psychology of ongoing threat: relative risk appraisal, the September 11 attacks, and terrorism-related fears. *American Psychologist*,*62*(4), 304.
23. Mayhorn, C. B., and McLaughlin, A. C. (2012). Warning the world of extreme events: A global perspective on risk communication for natural and technological disaster. *Safety Science*.
24. Mileti, D. S., and Fitzpatrick, C. (1992). The causal sequence of risk communication in the Parkfield earthquake prediction experiment. *Risk Analysis*, *12*(3), 393-400.
25. Mileti, D. S., and Sorensen, J. H. (1990). *Communication of emergency public warnings: A social science perspective and state-of-the-art assessment*. Oak Ridge, TN: Oak Ridge National Laboratory, U.S. Department of Energy.
26. National Commission On Terrorist Attacks Upon the United States. (2004). *The 9/11 Commission Report: final report of the National Commission on Terrorist Attacks upon the United States*. New York, NY: WW Norton and Company.
27. National Science and Technology Council. (2008). *Research challenges in combating terrorist use of explosives in the United States.* Washington, D.C.: Executive Office of the President, National Science and Technology

Council, Subcommittee on Domestic Improvised Explosive Devices.

28. Oh, O., Agrawal, M., & Rao, H. R. (2010). Information control and terrorism: Tracking the Mumbai terrorist attack through twitter. *Information Systems Frontiers*, 13(1), 1–11.
29. Protalinski, Emil. (2013) "Twitter launches alerts service in the US, Japan, and Korea to keep users informed during emergencies. http://thenextweb.com/twitter/2013/09/25/twitter-launches-alerts-service-in-the-us-japan-and-korea-to-keep-users-informed-during-emergencies. Retrieved on 10/31/2013.
30. Quarantelli, E.L. (1982). "What is a disaster? An agent specific or an all disaster spectrum approach to socio-behavioral aspects of earthquakes?" in B. Jones & M. Tomazevic (Eds.) *Social and economic aspects of earthquake.* Ithaca, NY: Institute for Testing and Research in Materials and structures and Program in Urban and rEgional Studies, Cornell University.
31. Ngowi, R. (2013, April 18). Teen stunned at portrayal as Boston bombing suspect. *CBS News*. Retrieved from http://www.cbsnews.com/8301-201_162-57580370/
32. Sattler, D. N. (2003). Resiliency, posttraumatic growth, and psychological distress after the attacks on America. *Beyond September 11th: An Account of Post-Disaster Research*, 315-332.
33. Seeger, M.W. and Sellnow, T.L. (2013). *Theorizing crisis*. Hoboken, NJ: Wiley-Blackwell.
34. Sellnow, T.L., Ulmer, R.R., Seeger, M.W., and Littlefield, R.S. (2009). *Effective risk communication: A message-centered approach*. New York, NY: Springer Science and Business Media, LLC.
35. Sellnow, T. L., Sellnow, D. D., Lane, D. R., and Littlefield, R. S. (2012). The value of instructional communication in crisis situations: Restoring order to chaos. *Risk Analysis*, *32*(4), 633-643.
36. Sorensen, J. H. (2000). Hazard warning systems: Review of 20 years of progress. *Natural Hazards Review*, *1*(2), 119-125.
37. Spiro, E., Sutton, J., Johnson, B., and Butts, C. (2013). *Following the bombing* [Online Research Highlight]. Retrieved from http://heroicproject.org
38. Sutton, J., Spiro E., Johnson, B., Fitzhugh, S., Gibson, B., and Butts, C. (2013) Warning tweets: serial transmission of messages during the warning phase of a disaster event. *Information, Communication & Society*. 1-23.
39. Updegraff, J. A., and Taylor, S. E. (2000). From vulnerability to growth: Positive and negative effects of stressful life events. *Miller (Eds.), Loss and Trauma: General and Close Relationship Perspectives*, 3-28.
40. Wasserman, S. and Faust, K. (1994). *Social network analysis: Methods and applications* (Vol. 8). Cambridge: Cambridge University Press.
41. White, H. C., Boorman, S. A., and Breiger, R. L. (1976). Social structure from multiple networks: Blockmodels of roles and positions. *American journal of sociology*, 730-780.
42. Veil, S. R., and Ojeda, F. (2010). Establishing media partnerships in crisis response. *Communication Studies*, *61*(4), 412-429.
43. Venette, S. J., Veil, S. R., and Sellnow, T. L. (2005). Essential communication resources for combating bioterrorism: Some practical and generalizable recommendations. *Communication Research Reports*, *22*(1), 29-37.