The Continued Relevance of the November, 2008 Mumbai Terrorist Attack: Countering New Attacks With Old Lessons

Joshua L. Kelly and Shahrzad Rizvi

ABSTRACT

The 2008 terrorist attack in Mumbai was characterized by a sense of public confusion and frustration. Throughout the event, the attackers were able to avoid an operationally superior counterterrorism force and for four consecutive days managed to spread terror in India's most populous city. One of the main contributing factors in the LeT and JuD's success was their innovative use of lean everyday technology. Not only did technology give the attackers detailed information about their targets before the attack, but the information they received during the attack gave the terrorists a sustained tactical edge. After the attacks two primary questions remain. How did this happen? What, if anything, can be done to disrupt and prevent this style of terrorist attack? This essay will review the background of the pre-attack phase, provide an analysis of the attack itself, and finally conclude with a set of actionable items and lessons learned for practitioners.

INTRODUCTION

The November 26, 2008 terrorist attack in Mumbai was an eye opening experience for many in the public safety community and signaled a new wave of small-arms attacks that has continued steadily for the past seven years.[1] The main question from the aftermath of the attack is still relevant today. How do a small number of terrorist operatives run a disciplined, coordinated, and sustained attack on a large metropolitan area with virtual impunity? The short answer was, and still is, technology. The situational use of cell phones and other low-fi tools gave the Lashkar-e-Taiba (LeT) and Jamaat ul Dawa (JuD) attackers detailed information about their targets before the attack and a sustained tactical advantage during the attack.[2] This essay will analyze the use of technology in the Mumbai attack, and will conclude with a set of lessons learned and recommendations for practitioners moving forward.

Background

This essay is not intended to provide a comprehensive analysis of the social and political climate that led to the attacks, but rather to review the use of technology during the attack itself, and to provide recommendations for practitioners to mitigate or prevent another Mumbai. For a more thorough background see Christine Fair's analysis in her testimony before the Committee on Homeland Security Subcommittee on Transportation Security and Infrastructure Protection."[3] Having said that, in order to provide a foundation for the overall analysis, it is necessary first to review how the attackers planned, acquired, and used technology during the lead up to the Mumbai attack.

Preparation

To overcome a militarily superior adversary during a terrorist or guerrilla style operation, it is essential for the attackers to capitalize on the element of surprise. To maximize that advantage during this event, planners from the LeT and JuD determined that their operators would require advanced situational awareness; handlers in Pakistan would need to study their targets meticulously beforehand and find a way to feed the attackers real-time information during the event itself.

David Headley (aka Daood Gilani) was tapped to accomplish this task. In the months leading up to the attack, Headley visited Mumbai five times to collect video, photographs, and GPS locations of key targets.[4] The most valuable of his visits was used to map the landing site. By mapping the landing site in advance via Google Earth, Headley allowed the attackers to enter India at a predetermined site where he knew they would face limited resistance.[5] It is clear that David Headley's use of everyday technology (Google Earth, handheld camera, etc.) helped him avoid detection, but how was he able to acquire such in-depth intelligence without any red flags being raised on the front end? Again, the answer lies in how the LeT and JuD acquired their technology and the kinds of technology they used.

How the Terrorists Acquired Technology

The consumerization of technology in Southern Asia has not only allowed the cities of Bangalore and Mumbai to become regional "silicon valleys", but has also increased the access to information and communications technologies for criminals and terrorists. Hasan Gafoor, Mumbai's police commissioner, provided an excellent summary following the attacks. "Once complicated technologies, including GPS systems and satellite phones have become simpler to operate, terrorists, like everyone else, have become adept at using them."[6] Basically, the Mumbai attackers were able to avoid detection because the tools that they used--GPS markers, Google Earth, camera phones, and cable television--are virtually impossible for public safety officials to track and limit.

The only exception to their reliance on low-fi tools was the operative's choice of phones. Analysts found out rather quickly during the attack that the on-the-ground managers and remote planners were masking their locations.[7] The operators in Mumbai used satellite phones to communicate with their handlers in Lahore, Pakistan, who were themselves supposedly using VoIP (internet) operated phones to further cover their tracks.

While these phones were being procured in the weeks leading up to the attack, an inconsistency with one of the purchasers actually raised a red flag that almost gave the attackers up. The individual who purchased the phones for Lashkar-e-Taiba through providers in New Jersey, USA, claimed that his name was Kharak Singh and that he was from India, yet he provided a Pakistani Passport number for the transaction.[8] The vendor of the technology, Callphonex, asked via e-mail, "If you're from India, why do you have a Pakistani passport?"[9] Unfortunately, this question was asked on November 25, 2008, and by then the attackers had already left for Mumbai. This event is an example of the speed at which terrorists can operate and a reminder that the current counterterrorism measures designed to flag suspicious behavior may be inadequate to uncover and disrupt operations by agile terror networks of this sort.

Attack Phase

While the groundwork for the operation was years in the making, the attack itself lasted from November 26, 2008 to November 29, 2008 and was carried out by the LeT and JuD using four attack teams operating initially on five different targets: Chhatrapati Shivaji Terminus ; Leopold Café ; Taj Mahal Hotel ; Oberoi Trident ; and Nariman House Jewish Community Center. In order to maximize confusion and distract first responders, the attackers detonated two taxi bombs at Wadi Bunder and Vile Parle. When all was said and done the attackers killed 172 individuals and wounded an additional 308. On top of the civilian casualties nine out of ten of the attackers were themselves killed during the attack.[10]

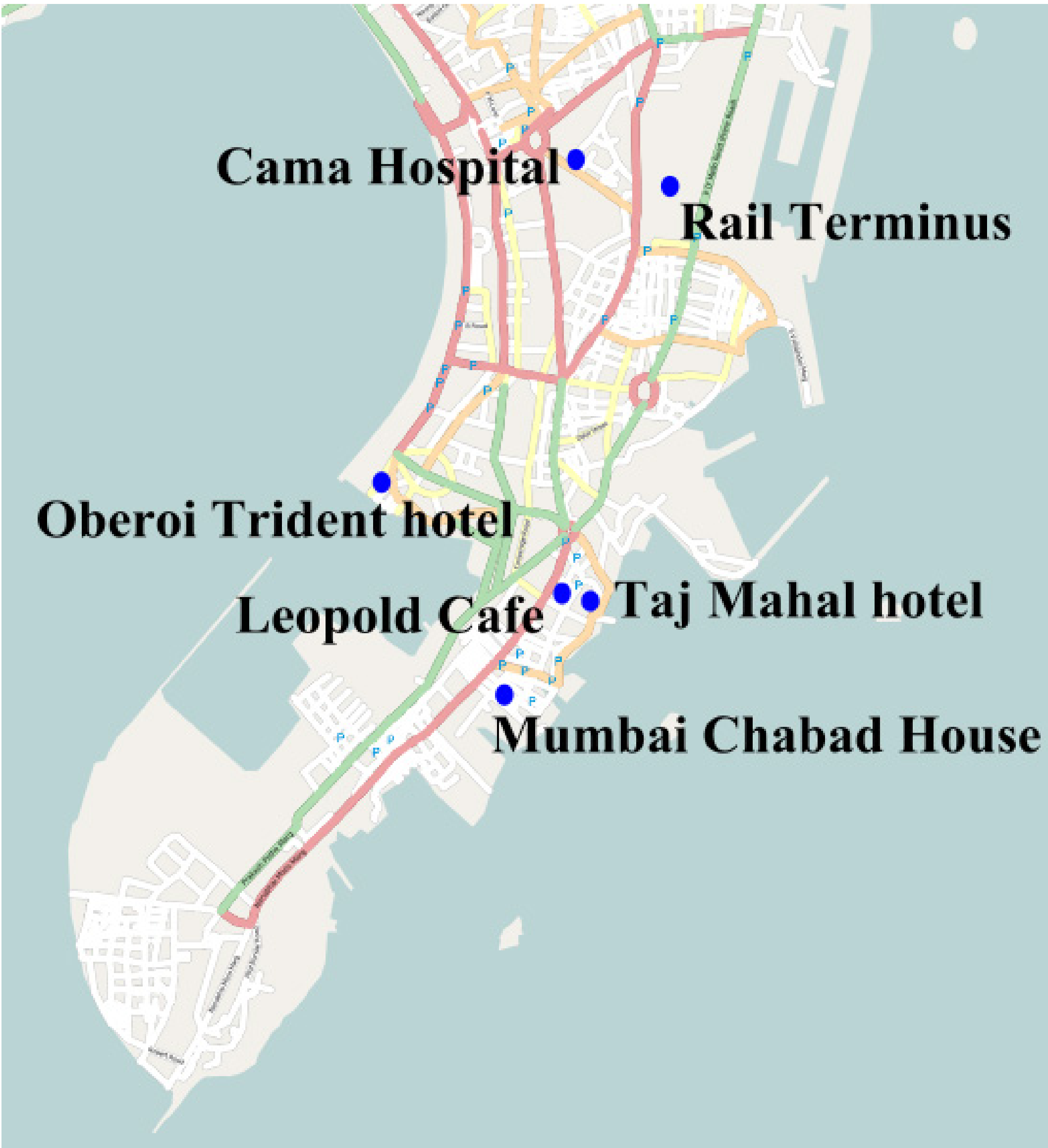

Figure 1. The Six Initial Target Locations[11]

Technology and Situational Awareness

The Mumbai attack was not the first terror attack in which the media and other public sources were used inadvertently to release tactical information to the wrong audience. In 1972 during the Munich massacre, the hostage takers watched the television broadcast within the Olympic dorms. In the Westgate mall attack in Kenya, the Al Shabaab attackers received updates via their cell phones.[12] In order to understand the extent to which the Mumbai attackers were reliant on public source technology for on-the-ground advantages, it is helpful to review the following captured conversation between the attackers and their handlers that was intercepted during the event.[13]

The following conversation occurred at the Taj Mahal Hotel early in the attack.

	November 27, 2008 - 3:10 a.m.
Terrorist:	Greetings!
Handler:	Greetings! There are three Ministers and one Secretary of the Cabinet in your hotel. We don't know in which room.
Terrorist:	Oh! That is good news! It is the icing on the cake!
Handler:	Find those 3 - 4 persons and get whatever you want from India.
Terrorist:	Pray that we find them.

(Ministry of External Affairs India, 2009)[14]

From that communication it is clear that the terrorists had a mission with specific targets and were being fed intelligence from the outside. Marc Goodman, from the Future Crimes Institute, provided another example of this information-sharing pattern from that same day.

> Terrorists entered the hotel room of a hostage who claimed to be a teacher. It did not make sense that a teacher stayed in a suite. The attackers called their handlers with the name of the hostage. The handlers in the operations center 'Googled' this person's named and asked the attackers. 'Is this person bald? Does he wear glasses? Is he heavyset?' the attackers responded yes whereby the handlers told them 'we found him online, kill him'.[15]

This could very well be the first example of terrorists using Google as a tactical tool during an event. Additionally, at one point the handlers picked up on a Twitter image that was broadcast by the BBC and relayed it directly to the attackers. The "Tweet pic" actually gave away the location of the Indian counterterrorism forces storming the Nariman House during the waning moments of the event, and resulted in the terrorists counter-attacking the assault forces storming the building from the roof.[16]

Lessons Learned and Actionable Next Steps

While a slow response by the Indian Security Forces certainly played a part in the 172 deaths during the event, an arguably more important factor is the LET's innovative use of technology.[17] Using this assumption as a starting point, the following section provides four recommendations for public safety officials to mitigate this style of attack. In order to help counter this fluid use of low-fi technology and increase the speed at which they can respond, managers should work to integrate improvisation into their planning and exercise process, limit bureaucratic red tape that prevents inter-organizational cooperation, double down on community-centric active shooter training, and be open to operationally adopting new and innovative technology.

Planning and Exercising for Improvisation

In the United States, the Incident Command System (ICS) has been almost universally adopted by Emergency Managers and Homeland Security organizations across the country.[18] During the Mumbai attack, Indian emergency managers had planned for attacks, but they lacked a modular and flexible structure when it came to communicating and responding in a non-routine fashion.[19] ICS provides a structure and starting point with which, at least theoretically, these challenges can be overcome. However, over a decade of research shows that while ICS can be effective in helping managers respond flexibly to events, it can also be hampered by issues with training depth and may need to be supplemented with focused bottom up planning.[20]

Managers need to acknowledge the strengths and limitations of ICS and focus their planning efforts on capability-based frameworks such as

Stripling's Evidence-Based Planning Criteria, which help foster improvisation and which may help managers to avoid situation-based planning.[21] In addition to leaner planning, exercises that incorporate things like McEntire's Spontaneous Planning concept and Kendra and Wachtendorf's research into improvisation are great ways to start building flexibility into the culture of an organization.[22]

Limit Bureaucracy

Para, the special forces unit of the Indian Army, was delayed in responding to the event because they did not have their own air assets to travel from New Delhi to Mumbai. Another bureaucratic weakness that characterized the response to the event was the fact that the Indian Navy, which is stationed within Mumbai itself, initially could not respond to the attack because they needed a Navy officer to sign off on their release before they could use military assets on a civilian response.[23] However small, these delays prevented responders from engaging before the terrorists had a chance to settle into their environment and assault their primary objectives. While it is always advisable to try and streamline processes wherever possible, the Mumbai attack is a great reminder of what happens when bureaucracy handcuffs responders who are facing a tech savvy, lean, and adaptable adversary.

The Importance of Active Shooter Training and Resources

Surprisingly, in November of 2008, Mumbai front line responders had not active shooting training, and the city of Mumbai had no rapid response force or SWAT team unit to speak of.[24] While local law enforcement organizations in the U.S. train frequently for active shooter scenarios, unfortunately the training often stops there. As recommended in the FBI's 2013 study on active shooter events and the Final Report of the Sandy Hook Advisory Commission, non-law enforcement community organizations such as schools and businesses need to leverage active shooter events such as Mumbai to gain access to better resources and to justify organization-wide training.[25]

Counter Technology with Technology

The biggest advantage that the perpetrators of the Mumbai attack had was a monopoly of pre-event information and the element of surprise. This advantage can be mitigated by employing some fairly new tools, such as real-time analytics and pre-event data mining, to stop attacks in progress and to balance the information asymmetry that occurs during the early phase of an attack.

Currently, most Emergency Operations Centers (EOC) have live television feeds from several outlets to choose from during an event. EOC's are formatted in this way so that managers may have real-time information in the quickest manner possible. To further increase situational awareness during fluid events, emergency responders must now expand their sources of information to include social media and other developing networks.

Monitoring social media can easily become overwhelming for emergency managers. At one point during the Mumbai attack there were over 1,000 Twitter messages being posted per minute regarding the event.[26] This is where responders should utilize social media aggregators to monitor trends and to relay relevant information in real time. Such technologies include Hootsuite, which collects social media information, and SwiftRiver which aggregates social media data.[27] These technologies include natural language processing, which gives geo-referential context and information validation to previously raw information. Simply put, social media situational and crisis awareness needs to be "outsourced" to the appropriate software so that more resources can be redirected towards responding to an event.[28] One of the most successful real world uses of this style of monitoring was when the Boston Police Department was able to monitor its social media channels in real time during the Boston Marathon Bombing and use that information to assist in identifying and locating the two bombing suspects in rapid succession.[29]

Moving Forward

The increased availability and affordability of technology will only make it easier for another terrorist group to replicate the results of the Mumbai attack. Unfortunately, attacks such as the Westgate Mall attack in 2013, the 2014 Peshawar school massacre in Pakistan, and the 2015 attack on the Charlie Hebdo office in Paris serve to remind us that Mumbai- style attacks are the new normal for terrorists.[30] Just as the Boston Police Department did during the 2013 Marathon Bombing, responders need to know, digitally speaking, where to look during an event and also how to integrate outside agencies quickly and seamlessly into their response.[31] There is a particular need to leverage the increase in publicly available data and to process that data in real time using things like data aggregators (i.e. HootSuite, SwiftRiver, etc.) and social media monitors.[32] On top of adapting new technology and promoting inter-organizational coordination, it is also important for organizations to double down on community-centric active shooter training and to adopt a culture of flexible planning using frameworks such as Stripling's Evidence-Based Planning Criteria and McEntire's Spontaneous Planning concept.[33] By integrating some of these new tools and tweaking some old best practices such as planning and training, managers can stay one step ahead of an active shooter style attack and mitigate, if not prevent, the next Mumbai. [34]

About The Authors

Shahrzad Rizvi *is a Budget and Policy Analyst in the Dallas-Fort Worth Metroplex. Shahrzad's professional background includes work related to policy, social systems, and government innovation. He specializes in the nexus between law, technology, and local government. He received his bachelor's degree in Social Sciences from Michigan Technological University and a Masters of Public Administration degree from the University of North Texas. The views and opinions expressed in this essay are his own. He may be reached at Shazoo+Rizvi@gmail.com.*

Joshua L. Kelly *is an Emergency Manager in the Dallas-Fort Worth Metroplex. He has worked in academia, local government, and in various disaster research- related positions. His current research interests revolve around citizen engagement, the sociology of disasters, and public safety policy. Joshua received a bachelor's degree from the University of Delaware, where he double majored in Sociology and Criminal Justice, and a Masters of Public Administration degree from the University of North Texas. He may be reached at Joshua.Logan.Kelly@gmail.com. The views and opinions expressed in this essay are his own.*

Notes

1. See http://en.wikipedia.org/wiki/List_of_Islamist_terrorist_attacks#2010s.

2. Caren Kaplan, "The Biopolitics of Technoculture in the Mumbai Attacks," *Theory Culture Society* 26, no. 301 (2009).

3. C. Christine Fair, "Antecedents and Implications of the November 2008 Lashkar-e-Taiba (LeT) Attack upon Several Targets in the Indian Megacity Mumbai," Testimony before the Committee on Homeland Security Subcommittee on Transportation Security and Infrastructure Protection," *Rand Corporation*, 2009, http://www.rand.org/content/dam/rand/pubs/testimonies/2009/RAND_CT320.pdf.

4. Donald Van Duyn, "Hearing, Senate Committee on Homeland Security and Governmental Affairs," *Homeland Security and Governmental Affairs*, 2009, www.hsgac.senate.gov/media/majority-media/committee-hears-lessons-learned-from-mumbai-terrorist-attack. ; Jeremy Kahn, "Mumbai Terrorist Relied on New Technology for Attacks," *The New York Times*, December 8, 2008, www.nytimes.com/2008/12/09/world/asia/09mumbai.html?_r=1.

5. William LaRaia and Michael Walker, "The Siege in Mumbai: A Conventional Terrorist Attack Aided by Modern Technology," in *A New Understanding of Terrorism*, edited by M.R Haberfield, (U.S.: Springer, 2009), 309 – 340.

6. Ibid.

7. Ibid.

8. C. Christine Fair, "Antecedents and Implications of the November 2008 Lashkar-e-Taiba (LeT) Attack upon Several Targets in the Indian Megacity Mumbai."; Donald Van Duyn, "Hearing, Senate Committee on Homeland Security and Governmental Affairs."

9. See note 8 above.

10. See note 8 above; Angel Rabasa et al., "The Lessons of Mumbai", *Rand Corporation,* 2009, http://www.rand.org/content/dam/rand/pubs/occasional_papers/2009/RAND_OP249.pdf, 1- 4.

11. See OpenStreetMap, 2008, Wikimedia Commons,
http://www.openstreetmap.org/?lat=18.921&lon=72.8339&zoom=14&layers=B000FTF.

12. Freedom C. Onuoha, "Westgate Attack Al-Shabaab's Renewed Transnational Jihadism," *AlJazeera Center for Studies*, 2013, http://studies.aljazeera.net/en/reports/2013/11/2013111112818580417.htm.

13. Jeremy Kahn, "Mumbai Terrorist Relied on New Technology for Attacks."

14. India Ministry of External Affairs, "Mumbai Terrorist Attacks 2008," *BACM Research*, 2009, https://archive.org/details/MumbaiTerrorAttacksDossier.

15. Marc Goodman, "The Business of Illegal Data: Innovation from the Criminal Underground," www.strataconf.com, September 22, 2011, http://www.youtube.com/watch?v=6ueKilyThQg.

16. Ibid.

17. Ibid.; Fred Burton and Scott Stewart, "Mitigating Mumbai," *Stratfor Global Intelligence*, 2009, www.stratfor.com/weekly/20090114_mitigating_mumbai.

18. See https://www.fema.gov/national-incident-management-system.

19. William LaRaia and Michael Walker, "The Siege in Mumbai." ; Angel Rabasa, et al., "The Lessons of Mumbai."

20. Joshua L. Kelly, et al., "The Challenges for Unconventional Response Agencies in Serving Haitian Earthquake Survivors: The Needs in ICS Training and Practices," *Disaster Research Center*, Working Paper No. 368 (2011), http://udspace.udel.edu/handle/19716/13432. ; Theodore J. Moody, "Filling the Gap between NIMS/ICS and the Law Enforcement Initial Response in the Age of the Urban Jihad," *Naval Postgraduate School,* 2010, http://calhoun.nps.edu/handle/10945/5182. ; Dick A. Buck, Joseph E. Trainor, and Benigno E. Aguirre, "A Critical Evaluation of the Incident Command System and NIMS," *Journal of Homeland Security and Emergency Management* 3, no. 3 (2006), 1-27.

21. James Kendra and Tricia Wachtendorf, “Improvisation, Creativity, and the Art of Emergency Management,” *Disaster Research Center*, Preliminary Paper No. 357 (2006), http://udspace.udel.edu/handle/19716/3054.

22. David McEntire, Joshua L. Kelly, James M. Kendra, and Laurie C. Long, “Spontaneous Planning after the San Bruno Gas Pipeline Explosion: A Case Study of Anticipation and Improvisation during Response and Recovery Operations,” *Journal of Homeland Security and Emergency Management* 10, no. 1 (2013), 161-185. ; Mitch Striplin, “Managing Chaos: The Disaster Planner’s Handbook in Eight Parts,” *The New York City Department of Health and Mental Hygiene*, 2013, http://www.nyc.gov/html/doh/downloads/pdf/em/mc-disaster-handbook.pdf.

23. K. Alan Kronstadt, “Terrorist Attacks in Mumbai, India, and Implications for U.S. Interests,” Congressional Research Service, (2008).

24. Neil C. Livingstone, “Mumbai: The Lessons Learned: What Not To Do-Implications for the West,” *DomPrep Journal* 1, no. 9, (2009). ; Fred Burton and Scott Stewart, “Mitigating Mumbai.”

25. Federal Bureau of Investigation, “A Study of Active Shooter Incidents in the United States Between 2000 and 2013,” *U.S. Department of Justice*, 2013, http://www.fbi.gov/news/stories/2014/september/fbi-releases-study-on-active-shooter-incidents/pdfs/a-study-of-active-shooter-incidents-in-the-u.s.-between-2000-and-2013. ; Sandy Hook Advisory Commission, “Final Report of the Sandy Hook Advisory Commission,” *State of Connecticut,* 2015, http://www.shac.ct.gov/SHAC_Final_Report_3-6-2015.pdf.

26. Sarita Azad and Arvind Gupta, “A Quantitative Assessment on 26/11 Mumbai Attack Using Social Network Analysis,” *Journal of Terrorism Research* 2, no. 2 (2011), http://ojs.st-andrews.ac.uk/index.php/jtr/article/view/187. ; Marc Goodman, “The Business of Illegal Data: Innovation from the Criminal Underground.”

27. See https://hootsuite.com/. ; https://github.com/ushahidi/SwiftRiver.

28. Joshua Kelly and Shahrzad Rizvi, “Communicating Emergency Information on a Budget,” *Public Management* 96, no. 2, (2014), 31-32, http://icma.org/en/press/pm_magazine/article/104188.

29. Christopher A. Cassa et al., “Twitter as a Sentinel in Emergency Situations: Lessons from the Boston Marathon Explosions,” *PLoS Currents*, 2013, http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3706072/.

30. Freedom C. Onuoha, “Westgate Attack Al-Shabaab’s Renewed Transnational Jihadism.” ; Sana Jamal and M. Ahsan, “TTP – Analyzing the Network of Terror,” *International Relations Insights and Analysis*, Report no. 6, (2015), http://www.ir-ia.com/reports/IRIA-TTP.pdf.

31. Christopher A. Cassa et al. “Twitter as a Sentinel in Emergency Situations.” ; Leonard J. Marcus et al., “Crisis Meta-Leadership Lessons From The Boston Marathon Bombings Response: The Ingenuity of Swarm Intelligence” *National Preparedness Leadership Initiative*, 2014, http://npli.sph.harvard.edu/wp-content/uploads/sites/8/2014/09/NPLI-Marathan-Bombing-Leadership-Response-Report-dist.pdf. ; U.S. House of Representatives Committee on Homeland Security, “The Road to Boston: Counterterrorism Challenges and Lessons from the Marathon Bombings,” *House Homeland Security Committee Report,* 2014, https://homeland.house.gov/sites/homeland.house.gov/files/documents/Boston-Bombings-Report.pdf.

32. Joshua Kelly and Shahrzad Rizvi, “Communicating Emergency Information on a Budget.” ; Joshua Kelly and Shahrzad Rizvi, “Digital Volunteers and Social Media,” *IAEM Bulletin* 31, no. 3 (2014) 9;17 http://www.iaem.com/members/201403bulletinonline.pdf.

33. Federal Bureau of Investigation, “A Study of Active Shooter Incidents in the United States Between 2000 and 2013.” ; Sandy Hook Advisory Commission, “Final Report of the Sandy Hook Advisory Commission.” ; Mitch Striplin, “Managing Chaos: The Disaster Planner’s Handbook in Eight Parts.” ; David McEntire, Joshua L. Kelly, James M. Kendra, and Laurie C. Long, “Spontaneous Planning after the San Bruno Gas Pipeline Explosion: A Case Study of Anticipation and Improvisation during Response and Recovery Operations.”

34. See https://hootsuite.com/. ; https://github.com/ushahidi/SwiftRiver.