Effective Risk Communications for the Counter Improvised Explosive Devices Threat

Communication Guidance for Local Leaders Responding to the Threat Posed by IEDs and Terrorism

Volume II

Principal Investigator
Vincent Covello, Ph.D.

Co-Principal Investigators
Steven Becker, Ph.D.
Michael Palenchar, Ph.D.
Ortwin Renn, Ph.D.
Piet Sellke

Support Team
Theodore Tzavellas
Paul Morrell
Mark Pfeifle
Alex Tzavellas
Rachael Bynum

December 2010

The U.S. Department of Homeland Security (DHS), Science and Technology Directorate, Human Factors/Behavioral Sciences Division provided support for this project under a contract (HSHQDC-10-C-0022) awarded to S4 Inc. for "Effective Risk Communications for the Counter Improvised Explosive Devices Threat".

S4 Inc.
8 NE Executive Park
Suite 180
Burlington, MA 01803
703-418-0040

TABLE OF CONTENTS

Chapter 1

Anticipated Questions for Leaders Following an Improvised Explosive Device (IED) Attack

Author: **Vincent Covello, Ph.D.**
Center for Risk Communication

A critical first strategic step in Improvised Explosive Device (IED) risk communication is to identify a complete list of potential questions that would be asked by key stakeholders. Without such as list, it is almost impossible to do advance preparation and effective IED risk communication training.

Questions and concerns typically fall into two categories:

- **Informational Questions**
  The following are examples of informational questions. What do people need to know? What do people want to know? Am I safe? Is my family safe? What should people do? Is it safe for people to leave their homes?
- **Challenge Questions**
  The following are examples of challenge questions. Why should people trust what you are telling them? Why did you not do more to prevent this from happening? Can you give an absolute guarantee that people will be safe? Are you telling us the same things you are telling your own family?

Questions can be further refined by grouping them into categories. For example, one way to group questions is by the stakeholder who is asking the questions. For example, questions can be grouped based on whether they are being asked by journalists, by elected officials, by the families of victims, or by the public.

A second way to group questions is by phase of the emergency. For example, questions can be grouped by pre-event, event, response, and recovery.

A third way to group questions is by category of concern. For example, questions can be grouped by broad categories of concern such as the following.

- Health concerns
- Safety concerns
- Environment/ecological concerns
- Quality of life concerns
- Political concerns
- Economic concerns
- Social concerns (e.g., trust, fairness, concerns about the welfare of children, vulnerable populations, or populations with specific needs)
- Ethical concerns
- Cultural concerns

Lists of specific stakeholder questions and concerns can be generated through research, including:

- Review and analysis of media stories (print and broadcast).
- Review and analysis of web sites.
- Review and analysis of public meeting records.
- Review and analysis of public hearing records and legislative transcripts.
- Review and analysis of complaint logs, hotline logs, toll-free number logs, and media logs.
- Review and analysis of blogs and social media sites (for example, Twitter, Youtube, and Facebook).
- Focused interviews with subject matter experts.
- Facilitated workshops or discussion sessions with stakeholders, special interest groups, and groups with special governance agreements (for example, Native American Tribal Governments).
- Interviews with individuals experienced in managing or communicating during the specific type of emergency situation.
- Consultations with individuals or organizations that represent, or are members of, the target audience.
- Consultations with colleagues who have successfully developed other communication products for the target audience.

Leaders are likely to be asked a large number of questions following an IED attack. Tables 1, 2, and 3 contain a sampling of these questions. These questions are derived in part from a review of questions asked during and after (a) the terrorist attack on September 11, 2001 of the World Trade Center in New York City; (b) the terrorist attacks in London on July 7, 2005; (c) the terrorist attack in Oklahoma City on April 19, 1995; and (d) the terrorist attacks in Mumbai, India in November, 2008.

Table 1 contains questions leaders are likely to be asked in any emergency or disaster situation. Table 2 contains questions leaders are likely to ask following an IED or other type of terrorist attack. Table 3 contains sample questions leaders are likely to be asked about a specific type of protective actions following an IED attack: evacuation.

==========

Table 1: Questions Leaders are Likely to be Asked by Journalists Following Any Emergency or Disaster

1. What is your name and title?
2. How do you spell and pronounce your name?
3. What are your job responsibilities?
4. Can you tell us what happened? Were you there? How do you know what you are telling us?
5. When did it happen?
6. Where did it happen?
7. Who was harmed?
8. How many people were harmed?
9. Are those that were harmed getting help?
10. How are those who were harmed getting help?
11. Is the situation under control?
12. How certain are you that the situation is under control?
13. Is there any immediate danger?
14. What is being done in response to what happened?
15. Who is in charge?
16. What can we expect next?
17. What are you advising people to do? What can people do to protect themselves and their families -- now and in the future – from harm?
18. How long will it be before the situation returns to normal?
19. What help has been requested or offered from others?
20. What responses have you received?
21. Can you be specific about the types of harm that occurred?
22. What are the names, ages and hometowns of those that were harmed?
23. Can we talk to them?
24. How much damage occurred?
25. What other damage may have occurred?
26. How certain are you about the damage?
27. How much damage do you expect?
28. What are you doing now?
29. Who else is involved in the response?
30. Why did this happen?
31. What was the cause?
32. Did you have any forewarning that this might happen?
33. Why wasn't this prevented from happening? Could this have been avoided?
34. How could this have been avoided?
35. What else can go wrong?
36. If you are not sure of the cause, what is your best guess?
37. Who caused this to happen?
38. Who is to blame?
39. Do you think those involved handled the situation well enough? What more could or should those who handled the situation have done?

Table 2 -- continued

40. When did your response to this begin?
41. When were you notified that something had happened?
42. Did you and other organizations disclose information promptly? Have you and other organizations been transparent?
43. Who is conducting the investigation? Will the outcome be reported to the public?
44. What are you going to do after the investigation?
45. What have you found out so far?
46. Why was more not done to prevent this from happening?
47. What is your personal opinion?
48. What are you telling your own family?
49. Are all those involved in agreement?
50. Are people over-reacting?
51. Which laws are applicable?
52. Has anyone broken the law?
53. How certain are you about whether laws have been broken?
54. Has anyone made mistakes?
55. How certain are you that mistakes have not been made?
56. Have you told us everything you know?
57. What are you not telling us?
58. What effects will this have on the people involved?
59. What precautionary measures were taken?
60. Do you accept responsibility for what happened?
61. Has this ever happened before?
62. Can this happen elsewhere?
63. What is the worst-case scenario?
64. What lessons were learned?
65. Were those lessons implemented? Are they being implemented now?
66. What can be done now to prevent this from happening again? What steps need to be taken to avoid a similar event?
67. What would you like to say to those who have been harmed and to their families?
68. Is there any continuing danger?
69. Are people out of danger? Are people safe?
70. Will there be inconvenience to employees or to the public? What can people do to help?
71. How much will all this cost?
72. Are you able and willing to pay the costs?
73. Who else will pay the costs?
74. When will we find out more?
75. What steps need to be taken to avoid a similar event? Have these steps already been taken? If not, why not?
76. Why should we trust you?
77. What does this all mean?

Table 2. Questions Leaders are Likely to be Asked Following an IED or Other Type of Terrorist Attack

"Who" Questions

1. Do you know who is in the terrorist group?
2. Do you know who the leader of the terrorist group is?
3. Does the terrorist group have a name? If so, what is it?
4. Is the terrorist group associated with Al Qaida?
5. Has this terrorist group struck before?
6. Where are the terrorists from?
7. What is the nationality of the terrorists?
8. Is there more than one terrorist group involved?
9. Do you believe any foreign governments are involved?
10. Has any terrorist group claimed responsibility for the attack?
11. How many terrorists were (are) involved in the attack?
12. Who is (has) responded to the terrorist attack?
13. Has a SWAT (Special Weapons and Tactics) team arrived on scene? If so, what organization are they from?
14. Who was the first to report that a terrorist attack was happening?
15. Who responded first to the terrorist attack?
16. Who was (is) in charge of the response to the terrorist attack?
17. Who was in charge of security at the site of the bombing?
18. What is the role of the local police? Are they currently at the site?
19. What is the role of the state police? Have they been called in to assist? Are they currently at the site?
20. What is the role of the FBI? Have they been called in to assist? Are they currently at the site?
21. What is the role of the Department of Homeland Security? Have they been called in to assist? Are they currently at the site?
22. What is the role of the Federal Emergency Management Agency? Have they been called in to assist? Are they currently at the site?
23. What is the role of the National Guard and military? Have they been called in to assist? Are they currently at the site?
24. What types of background checks are done for employees and contractors at the site?
25. Are there any disagreements about who should be in charge of the response to the terrorist attack?
26. Who is on the team responding to the terrorist attack?
27. What are the qualifications of the leader of the response team?
28. Have you called for help from specialists in anti-terrorism? If so, who are they?
29. Have any of the terrorists been captured?
30. If any of the terrorists have been captured, have they provided useful information to the authorities?
31. Who is in charge of questioning the captured terrorists?
32. What methods are (will) be used to extract information from captured terrorists?
33. Will you use torture to extract information from captured terrorists?
34. Have any of the terrorists been killed? If so, where were the bodies sent?
35. Who was the first to report there was the terrorist attack?
36. Who was the first to respond to the terrorist attack?

37. How many people are involved in the response?
38. Has anyone been injured or killed?
39. How many people have been injured or killed?
40. Who has been injured or killed in the terrorist attack? Can you tell us their names?
41. Have any security personnel been injured or killed in the terrorist attack? Can you tell us their names?
42. Who in the community has been injured or killed in the terrorist attack? Can you tell us their names?
43. Have all people at the site of the bombing been accounted for? Is anyone missing? If people are missing, can you tell us their names?
44. Has anyone been taken to the hospital? If so, what is their status?
45. Have steps been taken to protect [insert name, such as the Mayor or President]. What are these steps?
46. Do you believe the terrorists had help from others?
47. Who do you believe helped the terrorists?
48. Who did you notify first when you found out there was a terrorist attack?
49. Have the relatives of those injured or killed been notified?
50. Who is in charge of notifying relatives of the dead and injured?
51. If a family or friends want to know about the safety of a particular person, whom should they call?

What Questions

52. What happened?
53. What type of bomb was used?
54. Did the bomb contain anything in addition to explosives?
55. How much damage has been done to property?
56. What do the terrorists want?
57. What cause do the terrorists represent?
58. What are the goals of the terrorists?
59. Have the terrorists told you their names?
60. Have the terrorists made any demands?
61. Are you willing to negotiate with the terrorists if they threaten additional bombings?
62. Could the terrorists use the threat of more explosions and attacks as a means of extortion?
63. How was the attack carried out?
64. What damage has been done to [insert name of facility or structure]?
65. If damage was done, what consequences are expected?
66. What weapons are the terrorists using? If they are armed, have they used them?
67. Do the terrorists have bombs? Have they used them?
68. Do the terrorists have access to nuclear materials?
69. Do the terrorists have biological or chemical weapons?
70. Could the terrorists blow up other structures?
71. What will be your response if the terrorists threaten to set off other bombs if their demands are not met?
72. Are you willing to sacrifice the safety of the community if you cannot meet the demands of the terrorists?
73. What do expect next?

74. Is it possible this is a diversion?
75. Are further attacks expected?
76. If further attacks are expected, where do you think they will take place?
77. Have you received reports of other terrorist activity in this community or in other communities?
78. What preventive and protective actions have been taken?
79. What preventive and protective actions have other communities taken?
80. What preventive or protective actions have you taken to protect leaders?
81. What preventive or protective actions have you taken to protect children?
82. Is the community going to lose electricity?
83. What actions did you take when you first learned of the attack?
84. Did you have any warning that an attack was about to take place?
85. What actions did you take to stop the attack?
86. What actions are you taking now to prevent additional attacks?
87. What actions [have] [are] being taken by others?
88. What experience do you have in dealing with a terrorist attack?
89. What are the qualifications of the leader of the response team? What experience does that person have dealing with terrorists?
90. Which agencies are involved in the response?
91. What support or help have you received from community agencies and organizations?
92. What support or help have you received from organizations outside the community?
93. What resources have other organization offered?
94. What are you advising people to do?
95. What are you advising schools to do?
96. What are you advising community leaders to do?
97. What are you advising other communities to do?
98. Should people stay where they are?
99. Should people seek shelter?
100. Should people evacuate the community?
101. What should people do if there is another attack in the community?
102. What orders have been given to the community?
103. What restrictions will be imposed on the community as this event goes on?
104. Will the terrorist attack prevent people from being able to travel?
105. What effect will the terrorist attack have on basic utilities services?
106. What effect will the terrorist attack have on community services?
107. What are other communities doing in response to the attack?
108. What happens if there is another attack?
109. What is the worst-case scenario?

"Where" Questions

1. Where did terrorists attack?
2. Have you found the terrorists?
3. Where are the terrorists now?
4. Do you expect the terrorists to attack again?
5. Are other communities under attack?
6. Are community members safe where they are?
7. Are school children safe where they are?

8. Should parents go to pick up their kids at school?
9. Where is your emergency operations center?
10. Where are the leaders of the community?
11. Where are the families of the leaders of the community?
12. Where are the injured and dead being sent?

"When" Questions

1. When did the terrorists attack?
2. Was there any warning?
3. Do expect the terrorists to attack again?
4. When did you first learn about the attack?
5. When do you expect the threat will be over?
6. Will life ever return to normal?

"Why" Questions

1. Why did the terrorists attack this site?
2. Why did it take so long for authorities to arrive at the scene?
3. Why have you not called for more help?
4. Why were you not better prepared for the attack?
5. Why do you think the terrorists choose this time to attack?

"How" Questions

1. How did the terrorists gain access to the site?
2. How did the terrorists get past security at the site?
3. Had you prepared for an event such as this?
4. Did the terrorists have accomplices?
5. How are you finding out what is going on at the site?
6. Do you have surveillance cameras?
7. Are you interviewing people who witnessed the attack?
8. How can relatives and friends find out the status of their friends and loved ones at the site?
9. How often will updates be provided?
10. How can you be sure the terrorists do not have accomplices inside the site or in the community?
11. How far are you willing to go to prevent another attack?
12. How can people in the community ever feel safe again?
13. How sure can people be about the accuracy of the information they are receiving?
14. Can you assure people they are not receiving false or misleading information about protective actions?
15. Can you assure people they are not receiving false or misleading information about the incident, including information about the safety of site, and the safety of people in the community, including children?
16. What will you do if the terrorists strike again?
17. What will you if the terrorists begin attacking against secondary targets, such as schools, government office buildings, telecommunications, electric utilities, and water treatment facilities?
18. Is the place where the bomb went off a crime scene?

19. What are the implications for local businesses and residents of the location of the bombing is a crime scene?

Table 3: Sample Questions Local Leaders are Likely to be Asked Following an IED Attack if Evacuation is Recommended

1. How will you notify and warn the public (including residential, custodial, and transient populations) about on-going evacuation plans?
2. What should people do who do not have a car or other transportation?
3. Will it be safe for people to wait at the bus stop?
4. How long will people have to wait for a bus?
5. How long will people be gone from their homes and businesses?
6. What should I do if an evacuation seems likely?
7. What do I do with my pets?
8. What are the boundaries of the evacuation areas?
9. Is my neighborhood part of the evacuation area?
10. My children are at school and in the evacuation zone. Where will they be taken?
11. How can I get in touch with my children who were evacuated from their school?
12. My (insert name of relative or friend) is sick and in the hospital that is being evacuated. Where are they moving him/her?
13. How can I get in touch with my [insert name of relative or friend] evacuated from [insert location, such as a hospital or nursing home]?
14. My house is right over the boundary of the evacuation area. Am I safe?
15. If the boundaries of the evacuation zone change, how will people be notified?
16. Will people be escorted out of the evacuation zone?
17. If I drive my car out of an evacuated area, will the car be contaminated? Will it be confiscated?
18. I've been told they are evacuating my neighborhood. What streets should I use to get out safely?
19. Is there more than one evacuation route from where I live?
20. I've been told to evacuate. Will someone pick me up or am I supposed to drive my own car?
21. How will I know I am going the right way? What happens if I get lost?
22. What I have to drive through a dangerous area to evacuate?
23. Will people be checking my identification before letting me out of the evacuation zone? If so, what will happen to me, my car, and my possessions?
24. How will emergency responders know when the threat is over?
25. Will there be more than one shelter for each area being evacuated? What will happen if a shelter is full? Will people be sent to another shelter?
26. Will they check people's identification before letting them into a shelter? If a person has no ID, what will happen to them?
27. Where do I go to evacuate? I don't have a radio or television.
28. Are all evacuation centers the same?
29. Do some evacuation centers have better accommodations and amenities than others? Where can I find this information?
30. Will evacuation centers have [insert item, such as televisions, radios, telephones, toys for children; rooms for smokers, microwaves, or refrigerators]?
31. Will children being evacuated from schools be sent to the same evacuation centers as their parents?
32. How long will people have to stay at the evacuation centers?
33. I have special medication I need to take. What happens if I run out while I am at the evacuation center?

34. I am on a special diet from my doctor due to my health. Will the evacuation center be able to make the food I need?
35. I am on oxygen and I have only one canister. Will the evacuation center be able to help me get more?
36. My understanding is evacuation centers will not accept pets. Will they make exceptions for small pets [for example, turtles, rabbits, gerbils, and canaries)?
37. I don't like being around people I don't know. Will they give me a room by myself?
38. Will there be different evacuation centers for VIPs (Very Important People)?
39. Will the evacuation centers have safes or safety deposit boxes?
40. My [insert name of relative or friend] is in [insert custodial facility name, such as a hospital, nursing home] inside the evacuation zone. They are being told to stay put. Are they going to be safe?
41. Will I be able to go to the [insert custodial facility name] and pick up [insert name of relative or friend]?
42. Will the people who are not able to evacuate die?
43. A number of homeless people live under the bridge by the edge of town. Who is going to make sure they get told about the evacuation?
44. I know of campers who are in the forest. Who is going to make sure they evacuate?
45. Have arrangements been made with adjacent cities, towns, and municipalities to shelter folks evacuated from this emergency?
46. What facilities have been designated in these communities as evacuation centers?
47. Are the hospitals in the adjacent communities able to take care of people who have been evacuated?
48. Who is in charge of ensuring folks get to the right evacuation center?
49. Will an attempt be made to get families reunited?
50. How are you going to get people out of the evacuation zone who are visually or hearing impaired?
51. Should I give a ride to people who are hitchhiking or need a ride out of the evacuation zone? Is it safe to give rides to strangers?
52. When I leave my home to go to the evacuation center, will my house be safe from vandals and thieves? Will the police stay behind to protect my property?
53. What happens if I return home and someone has broken into my house? Who will be responsible? Will those who forced me to evacuate be liable?
54. What happens if my house catches fire after I have evacuated. Will firemen stay behind to put out fires?
55. I heard they are evacuating my neighborhood. What happens if I refuse to leave my home? Will I be forced to leave? Will they arrest me?
56. Do the law enforcement officials have the legal right to force me to evacuate?
57. Who will pay for property and personal effects lost or damaged following an evacuation?
58. Who will protect my business if I evacuate?
59. Will the National Guard be called in to make sure there is no looting?
60. Who will be responsible for property damage or theft at businesses in the evacuation zone?
61. Who will pay for losses to businesses closed because of the evacuation?
62. What happens if there is a traffic jam? Have you planned for traffic jams?
63. Who made the decision to evacuate? Why didn't they evacuate earlier?

64. My children go to a school outside the evacuation zone. Who will tell them they cannot go home?
65. How much time will people told to evacuate have to pack their things? What should they take with them?
66. What are you telling people not affected by this emergency but who are self-evacuating and clogging evacuation routes?
67. What are you telling people outside the evacuation zone who nonetheless want to evacuate?
68. Are you setting up roadblocks to prevent people from entering the evacuation zone?
69. If you evacuate but forgot something at home, will you be allowed back into the evacuation zone?
70. Who will stay behind in the evacuation zone? What will happen to them?
71. Can locking yourself in your house or business personal protect those who stay behind in the evacuation zone?
72. Will ambulances be allowed into the evacuated areas?
73. Will houses and businesses in the evacuation area continue to get electricity and water?
74. What are you telling your own family to do?
75. I can stay with [insert name]. Will you provide funds to get me there?
76. Will martial law be declared?
77. Will there be a curfew?
78. Will water, telephone, mobile phone, internet, and electricity services be affected?
79. Will this bombing affect transportation schedules, such as [insert type of transportation, such as airlines, trains, and buses]?
80. What steps are being taken to control traffic?
81. What steps are being taken to control of access to the affected area?
82. What steps are you taking to prevent looting from homes or businesses that have been evacuated?
83. When will people be able to re-schedule community and social events, such as [insert name of event, such as community meetings, concerts, memorial services, and weddings]?
84. How will the incident affect mail delivery?
85. How, where, and when will people get their mail?
86. Who will water my plants?
87. Who will take care of the pets I had to leave behind?
88. Will ATMs be working for those who don't have enough cash with them?
89. Will authorities provide cash or coupons to people without cash or credit?

Chapter 2

Public Perceptions of Improvised Explosive Devices (IEDs): Results from Focus Group and Survey Research

Author: **Steven Becker, Ph.D.**
University of Alabama at Birmingham

An important source of information related to public perceptions of Improvised Explosive Devices (IEDs) comes from (1) focus group research; and (2) survey research. Provided below are findings from recent research.

1. Focus Group Research

In 2005, CDC asked four leading U.S. schools of public health to conduct three focus groups on public perceptions, concerns, information needs and information preferences related to the threat of terrorist bombings. The request was made as part of the Pre-Event Message Development Project, a groundbreaking, CDC-funded national study of communication issues and emergency messaging for emerging threats.

The locations of the three groups were Los Angeles, St. Louis and Oklahoma City. Across the three groups in this exploratory study, a total of 25 people were included. The results are being published here for the first time.

To foster discussion and elicit feedback, a progressively developing, hypothetical suicide bombing scenario was used in the groups. Participants were told that at lunchtime, the local news was being interrupted with a report that there had been at least three suspected terrorist suicide bombings in the city. Two occurred at food courts in shopping malls and another took place at a restaurant outside a large office building. More than three-dozen people had been confirmed dead so far, and over a 100 had been wounded at each site.

Topics covered in the focus groups included:

- **Immediate Reactions and Concerns** (for example, what was their immediate reaction to the scenario and what actions they would take);
- **Information Needs** (for example, what they would want to know);
- **Information Sources** (for example, who they would turn to for information);
- **Factors That Could Impede Effective Risk Communication** (for example, what would prevent them from believing the information they would receive);
- **Factors that Could Facilitate Effective Risk Communication** (for example, what would make information more believable).

Among the key findings are the following:

a. Immediate Reactions and Concerns

Many participants indicated their immediate reaction to the scenario was fear. Some also characterized their reaction as "overwhelming."

> "You can just get kind of overwhelmed initially with knowing that, right here, right in our little city and State, that now we're faced with a worldwide terrorist

[attack]. And it's very frightening to think that it has come to us. That it really reached us. It [is] just a little overwhelming to think about that."

Several individuals, particularly African Americans, mentioned prayer as an immediate reaction.

"First thing I would do is pray."

For many of the focus group participants, an immediate reaction was to be concerned about children and family.

"You're going to be worried about family members."

"I'd probably be scared to death. Wondering...the first things you wonder is where my family is."

"I want to know where my family is at that moment."

"I want to know where my children [are]."

Another immediate reaction was to want to help others.

"My first reaction is [what] can I do to help?"

Several respondents said that there was little that could be done, and that they would stay put.

"You know there's very little you can do except pray and stay put."

"I mean basically there's not a whole lot that you can do."

Several respondents said they would immediately take actions related to their children and family.

"I'd be calling my children and find out where they are, and where my grandchildren are."

"I would try to gather everybody that belongs in the household. Tell them to come home now."

"I'm going to get my children and I'm going to go home."

Several participants said they would take action to help friends and neighbors.

"I live in an apartment complex and we're really close. All of the neighbors are really close we know each other. I would check on the elderly neighbor."

b. Information Needs

Participants indicated that they would want several types of information.

One type of information requested related to protective actions.

> "I would want to know what to do and how to keep safe."

> "I would want to know something more specific. For example, if you're in restaurant or a store, what can you do to protect your body? How should you protect your eyes? Should you get under a table?"

Many participants wanted to know whether they should stay or go somewhere else:

> "First of all I would like to know where not to be. Where is the safest place?"

> "I would like to know, where should you go?"

A second type of information requested related to how to help others.

> "If I "see somebody crushed, should I try to help them? Should I pull them out?

> "How can I help? How can help my fellow citizens?"

c. Information Sources

Many of the participants indicated they would seek information from the mass media, with television mentioned frequently. Other responses included the Internet, radio and cell phone.

d. Factors that Could Impede Effective Risk Communication

Participants identified a number of factors that they believed could impede the effectiveness of communication related to a terrorist bombing attack.

One impediment identified by participants was people might not pay attention to anything distributed beforehand.

> "That's the concern about distributing these ahead of time. Whether people would read them."

> Most of us think about it, but until it happens somewhere else..."

Another potential impediment identified by participants was misinformation, inaccurate information, and hype.

> "Even on television they get in the heat of the moment. And if it was a real terrorist attack that just happened, we sometimes get so much misinformation."

> "I'd be worried about TV being inaccurate."

> "I don't trust the network news all that much."

e. Factors that Could Facilitate Effective Risk Communication

Focus group participants identified several factors they believed could help facilitate effective risk communication.

One factor strongly expressed was the need to have specific, rather than general, information about the threat and the situation (for example, what happened, where it happened, how will it impact health). Participants indicated the more specific the information reported, the more likely they would believe it and take action.

Participants also indicated they would look for multiple sources for information. Participants indicated it was important to have information available through multiple channels.

"I'd probably have 2 or 3 sources going. If I had access to a TV I'd put that on but radio would always be my first. And then I'd be looking stuff up on the internet if I could and be trying to communicate via my cell phone."

Finally, several participants indicated if emergency communications came through email or text messaging, it is important to be able to establish it was not a hoax. For example, participants recommended authorities announce ahead of time (1) they will be sending email or text messages and (2) the name the site from which the message will come.

2. Survey Research Findings

a. Public Lack of Knowledge

Studies show that:

- Only about half of the U.S. population is familiar with community warning systems and alerts.
- Only a third of the US population is familiar with official sources of public safety information.

b. Perceptions of Risk

Studies show there is a critical need to analyze and understand local conditions in detail, including the size of community, secondary targets within the community, the quality of local leadership, and the local emergency response infrastructure. For example, studies show that:

- Terrorism is a significant concern for many Americans. However, although many Americans expect additional attacks on the U.S., the vast majority of Americans do not think such attacks will occur where they live.

- The effectiveness in emergency risk communication following a mass casualty event can be measured along five perceptual dimensions: a sense of hope, community- and self-efficacy, calm, safety, and connection to others.

- People's behavior following a terrorist attack will typically follow predictable patterns. For example, the average person checks with four to five sources (such as a trusted news person, a neighbor, a friend, a co-worker, a spouse, a trusted public official, or a Web site) before deciding whether to evacuate an area.

- Communication in an emergency is most effective when information is delivered through multiple channels of information. These channels should be the channels used primarily by the target audience, such as texting and social media used by young people.

- The manner in which hazard and risk information is framed and presented by officials influences peoples perceptions of critical psychological and decision-making factors such familiarity, control, and trust in authorities

- The medium through which the message is delivered (for example, via formal warning and emergency broadcast systems; via print and electronic media; and via hand-held digital devices such as cell phones and hand-held PDAs) influences people's perceptions of critical psychological and decision-making factors such familiarity, control, and trust in authorities.

- The way the message is received by its intended audience and its effectiveness in accurately conveying information influences peoples perceptions of critical psychological and decision-making factors such familiarity, control, and trust in authorities

c. The Value of Advance Preparation

Nearly half of the U.S. population thinks advance preparation for a bomb or explosion would help them deal with the situation.

d. Perceptions of Efficacy

- Large numbers of people are not confident they would know what to do in case of a terrorist attack.

e. Perceptions of Credibility of Sources of Information

- The current low level of trust and confidence in government poses a serious challenge to effective messaging during and after a terrorist attack

- At the national level, health agencies are seen as credible sources of information following a terrorist attack.

- At the local level, the uniformed services, especially fire and police, are seen as credible sources.

- Key elements in building trust following a terrorist event are: (1) expressing empathy for affected stakeholders, (2) acknowledging uncertainty, (3) a commitment to transparency, and (4) consistency among emergency response partners in messaging.

References

After a Terrorist Bombing: Health and Safety Information for the General Public. Centers for Disease Control and Prevention. See http://www.bt.cdc.gov/masscasualties/afterbombing.asp

Alerting America: Effective Risk Communication: Summary of a Forum. A Summary of the Natural Disasters Roundtable by R Floroiu, RT Sylves, The National Academies, October 31, 2002.

Analysis of Focus Groups with Blind and Visually Impaired Individuals Concerning Emergency Alerts. Prepared by the American Foundation for the Blind for CPB/WGBH's National Center for Accessible Media, February 14, 2006.

AP-GfK-Roper poll. Telephone survey of the American general population, June 2010.

Becker SM (2001). Meeting the Threat of Weapons of Mass Destruction Terrorism: Toward a Broader Conception of Consequence Management. Military Medicine 166(S2):13-16.

Becker SM (2004). Emergency communication and information issues in terrorism events involving radioactive materials. Biosecurity and. Bioterrorism. 2(3), 195–207.

Becker SM (2007). Communicating Risk to the Public after Radiological Incidents. British Medical Journal 335(7630):1106-7.

Becker SM (2009). Social, Psychological and Communication Impacts of an Agroterror Attack. In: Wiley Handbook of Science and Technology for Homeland Security, JG Voeller, Editor, Wiley Publishers.

Bomb-Making Materials Awareness Program (BMAP): Private Sector User Guide. U.S. Department of Homeland Security.

Burns WJ, Slovic P (2007). The diffusion of fear: Modeling community response to a terrorist strike. The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology 4; 298.

Clarke L, Chess C, Holmes R, O'Neill KM (2006). Speaking with One Voice: Risk Communication Lessons from the US Anthrax Attacks. Journal of Contingencies and Crisis Management 14 (3): September 2006.

Communicating in the First Hours: Suicide Bombing. Short and extended messages. Centers for Disease Control and Prevention. See http://emergency.cdc.gov/firsthours/suicidebomb/index.asp

Coppola DP and Maloney EK (2009). Communicating Emergency Preparedness: Strategies for Creating a Disaster Resilient Public. CRC Press.

Corley C (2010). Blacks Show New Trust In U.S. Government. National Public Radio. April 29, 2010.

Economist/YouGov Poll of General Population Respondents. July 24-27, 2010.

Emergency Communications: Improving Communications with Train Passengers Trapped Underground following a Mass Casualty Incident. Lessons Learned Information System (LLIS).

"Explosions." Section 4.2 in Are You Ready? Federal Emergency Management Agency (FEMA).

Explosions. Ready.gov. Department of Homeland Security. See http://www.ready.gov/america/beinformed/explosions.html

Explosions Visual Guide. Ready.gov. Department of Homeland Security. See http://www.ready.gov/america/_downloads/explosions.pdf

FEMA (December 2009). Personal Preparedness in America: Findings from the 2009 Citizen Corps National Survey. August 2009 (Revised December 2009). Federal Emergency Management Agency.

FEMA (June 2009). Personal Preparedness in America: Findings from the Citizen Corps National Survey. June 2009. Federal Emergency Management Agency.

Fernandez M (2010). A Phrase for Safety After 9/11 Goes Global. New York Times, May 11, 2010, page A 17.

Freedman L (2005). The politics of warning: Terrorism and risk communication. Intelligence and National Security 20(3): 379 – 418.

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.

Gershon RRM, Hogan E, Qureshi KA, Doll L (2004). Preliminary results from the World Trade Center evacuation study - New York, 2003. Centers for Disease Control and Prevention Morbidity and Mortality Weekly Reports 55(35) 815-816.

Guide to Mail Center Security. U.S. Postal Inspection Service. Publication 166. March 2008.

Halloran L (2010). Pew Poll: Trust In Government Hits Near-Historic Low. National Public Radio, April 18, 2010. See http://www.npr.org/templates/story/story.php?storyId=126047343

Heroes of N.Y. Times Square bomb attempt show why vigilance matters. Editorial. The Washington Post, Tuesday, May 4, 2010.

Hildebrand S, Bleetman A (2007). Comparative study illustrating difficulties educating the public to respond to chemical terrorism. Prehospital and Disaster Medicine 22(1): 35–41.

Hobbs J, Kittler A, Fox S, Middleton B, Bates DW (2004). Communicating Health Information to an Alarmed Public Facing a Threat Such as a Bioterrorist Attack. Journal of Health Communication, Volume 9: 67–75.

Homeland Security Advisory Council. Homeland Security Advisory System Task Force Report and Recommendations. September 2009.

IED Attack: Improvised Explosive Devices. A Fact Sheet from the National Academies and the Department of Homeland Security. Project on News and Terrorism: Communicating in a Crisis. National Academy of Engineering of the National Academies. See http://www.dhs.gov/xlibrary/assets/prep_ied_fact_sheet.pdf

Injuries and Mass Casualty Events: Information for the Public. Centers for Disease Control and Prevention. See http://www.bt.cdc.gov/masscasualties/injuriespub.asp

Kearon T, Mythen G, Walklate S. Making Sense of Emergency Advice: Public Perceptions of the Terrorist Risk. Security Journal, 2007, 20, (77 – 95).

Lasker RD (2004). Redefining Readiness: Terrorism Planning through the Eyes of the Public. New York, NY: The New York Academy of Medicine.

Luck and Vigilance. Editorial. The New York Times, May 3, 2010.

Maher D (2002). Homeland Security. New York Magazine, June 24, 2002.

Manzi C, Powers MJ, Zetterlund K (2002). Critical Information Flows in the Alfred P. Murrah Building Bombing: A Case Study. Terrorism Studies Series, Special Report 3, Chemical and Biological Arms Control Institute.

Margetta R (2010). Survey: Majority of U.S. Citizens Expect Terrorists to Attack with IEDs. CQ Homeland Security. April 6, 2010.

Marist College Institute for Public Opinion. How Americans Feel About Terrorism and Security: Two Years After 9/11. Survey conducted on behalf of the National Center for Disaster Preparedness and the Children's Health Fund; August 2003.

Mayhorn CB (2005). Cognitive Aging and the Processing of Hazard Information and Disaster Warnings. Natural Hazards Review 6(4): November 1, 2005.

McDermott R and Zimbardo PG (2007). The psychological consequences of terrorist alerts. Chapter 23 in Psychology of Terrorism, B Bongar, LM Brown, LE Beutler, JN Breckenridge, PG Zimbardo, eds., Oxford University Press.

Meredith LS, Shugarman LR, Chandra A, Taylor SL, Stern S, Beckjord EB, Parker AM, Tanielian T (2008). Analysis of Risk Communication Strategies and Approaches with At-Risk Populations to Enhance Emergency Preparedness, Response, and Recovery: Final Report. Prepared by RAND for the United States Department of Health and
Human Services, Office of the Assistant Secretary for Planning and Evaluation, WR-598-HHS, December 2008.

Mileti DS, Sorensen JH (1990). Communication of Emergency Public Warnings: A Social Science Perspective and State-of-the-Art Assessment. Washington, DC: Federal Emergency Management Agency.

Mileti DS, R Bandy, LB Bourque, A Johnson, M Kano, L Peek, J Sutton, M Wood (2006). Bibliography for Public Risk Communication on Warnings for Public Protective Actions Response and Public Education. Revision 4.

Miller Steiger D (2010). Improvised Explosive Devices: Perceptions and the Domestic Threat. Gallup Government. Presentation given by D Miller Steiger at the Homeland Security Policy Institute (HSPI) Forum on Improvised Explosive Devices: Perceptions and the Domestic Threat, George Washington University, April 6, 2010.

Morales L (2010). In U.S., Confidence in Newspapers, TV News, Remains a Rarity. Gallup Poll, August 13, 2010.

National Council on Disability (2009). Effective Emergency Management: Making Improvements for Communities and People with Disabilities. August 12, 2009.

NRC (2007). Countering the Threat of Improvised Explosive Devices: Basic Research Opportunities: Abbreviated Version. Committee on Defeating Improvised Explosive Devices: Basic Research to Interrupt the IED Delivery Chain, National Research Council of the National Academies. Washington, DC: The National Academies Press.

NRC (2008). Disrupting Improvised Explosive Device Terror Campaigns: Basic Research Opportunities: A Workshop Report. Committee on Defeating Improvised Explosive Devices: Basic Research to Interrupt the IED Delivery Chain, National Research Council of the National Academies. Washington, DC: The National Academies Press.

NSTC (2000). Effective Disaster Warnings. Report by the Working Group on Natural Disaster Information Systems, Subcommittee on Natural Disaster Reduction, National Science and Technology Council, Committee on Environment and Natural Resources.

NSTC (2008). Research Challenges in Combating Terrorist Use of Explosives in the United States. Executive Office of the President, National Science and Technology Council, Subcommittee on Domestic Improvised Explosive Devices.

Perry RW, Lindell MK (2003). Understanding citizen response to disasters with implications for terrorism. Journal of Contingencies and Crisis Management, 11(2), 49-60.

Pew Research Center (2010). The People and Their Government: Distrust, Discontent, Anger and Partisan Rancor. Pew Research Center for the People & the Press. April 18, 2010.

PPW (2004). Partnership for Public Warning. Protecting America's Communities: An Introduction to Public Alert & Warning.

Preparing for a Terrorist Bombing: A Common Sense Approach. Centers for Disease Control and Prevention. See http://www.bt.cdc.gov/masscasualties/preparingterroristbombing.asp

Public Response to Terrorism (2008). Findings from the National Survey of Disaster Experiences and Preparedness. Prepared by M Kano, MM Wood, DS Mileti, LB Bourque. November 12, 2008.

Rogers MB, Amlot R, Rubin GJ, Wessely S, Krieger K (2007). Mediating the social and psychological impacts of terrorist attacks: The role of risk perception and risk communication. International Review of Psychiatry 19(3): 279–288.

Ronan KR and Johnston DM (2005). Promoting Community Resilience in Disasters: The Role for Schools, Youth, and Families. Springer.

Ropeik D. Risk Communication – An Overlooked Tool in Combating Terrorism. In: Wiley Handbook of Science and Technology for Homeland Security, JG Voeller, Editor, Wiley Publishers.

Saad L (2009). Majority of Americans Think Near-Term Terrorism Unlikely. Gallup Poll, December 2, 2009.

Sahm C. Hard Won Lessons; Transit Security. Safe Cities Project, March 2006.

Tierney K. Strength of a City: A Disaster Research Perspective on the World Trade Center Attack. Social Science Research Council – After Sept. 11. Accessed Jan 18, 2010. See http://essays.ssrc.org/sept11/essays/tierney.htm

Vanderford ML (2004). Breaking new ground in WMD risk communication: the pre-event message development project. Biosecurity and Bioterrorism 2(3), 193–194.

Wray RJ, Becker SM, Henderson N, Glik D, Jupka K, Middleton S, Henderson C, Drury A, Mitchell EW (2008). Communicating with the public about emerging health threats: Lessons from the Pre-Event Message Development Project. American Journal Public Health 98: 2214-2222.

Chapter 3

Current Communication Initiatives Related to Improvised Explosive Devices (IEDs) and Terrorist Attacks

Author: **Steven Becker, Ph.D.**
University of Alabama at Birmingham

Future efforts to improve Improvised Explosive Device (IED) risk communications can benefit from current risk communication initiatives and materials that have been developed by various agencies. There are actually relatively few such items, which is surprising given the growing concern about IEDs. However, initiatives and materials that have been produced to date have often been highly innovative.

In this section, three types of risk communication and information initiatives are reviewed:

- **Fact Sheets and Web Content;**
- **Messages Templates;**
- **Outreach and Awareness Programs**.

1. Fact Sheets and Web Content

The Federal Emergency Management Agency (FEMA) has produced several web- based informational resources on terrorist use of explosives. The Terrorism section of the "Plan and Prepare" page includes a link to resources on Explosions, including the following:

- **How can I protect myself from explosions?**
- **What to do if you receive a bomb threat**
- **What to do during an explosion**
- **What to do after an explosion**
- **Be wary of suspicious packages and letters**

(See: http://www.fema.gov/hazard/terrorism/exp/index.shtm)

Likewise, FEMA's PDF publication entitled "Are You Ready: An In-Depth Guide to Citizen Preparedness" (available in English and Spanish) includes a short section on Explosions.

(See: http://www.fema.gov/areyouready/explosions.shtm)

Other resources are available through "www.ready.gov." Ready.gov is a searchable, web-based portal intended to provide disaster preparedness information and resources to the American public. The site, which includes downloadable fact sheets, checklists, planning tools and preparedness guides, and provides information for three general populations including the general public, businesses and young persons.

On the "Be Informed" page of the Ready America section, there is a link to fact sheet with information on what to do if there is an explosion. In addition, there is a link to a visual guide showing people what actions to take to protect themselves.

A particularly innovative fact sheet specifically focusing on IEDs has been prepared by a project entitled "News and Terrorism: Communicating in a Crisis." News and Terrorism is a joint effort of the National Academy of Engineering of the National Academies, the Radio-Television Digital News Foundation, and the U.S. Department of Homeland Security. The project seeks to provide journalists, news managers, public information officers, public officials and others with the opportunity to explore public information and communication issues related to terrorism. A centerpiece of the program has been the development of fact sheets on terrorism threat agents.

The CDC's National Center for Injury Prevention and Control has developed an extensive series of web-based fact sheets on terrorist bombings. These fact sheets are available in Spanish, Chinese, and French. Found in the "Mass Casualties" and "Blast & Explosion Injuries" section of the Injury Response page (located at http://www.cdc.gov/injuryresponse/index.html), the sheets cover a wide variety of topics. The fact sheets are mainly intended for use by healthcare professionals. This is also true of several other innovative products prepared by the Center (in conjunction with the American College of Emergency Physicians), including a pocket guide entitled "Bombings: Injury Patterns and Care" and a large poster of the same title. Likewise, the Center and its partners have developed a highly regarded specialized training curriculum for clinicians. It includes a CDC containing an instructor-led course and another CD with interactive scenario-based training.

In addition to these items for healthcare professionals, the Center has developed fact sheets/web content specifically for the general public. These include the following:

Preparing for a Terrorist Bombing: A Common Sense Approach
(Available at http://emergency.cdc.gov/masscasualties/preparingterroristbombing.asp)
After a Terrorist Bombing: Health and Safety Information for the General Public
(Available at http://emergency.cdc.gov/masscasualties/afterbombing.asp)

Injuries and Mass Casualty Events: Information for the Public
(Available at http://emergency.cdc.gov/masscasualties/injuriespub.asp)

Brain Injuries and Mass Casualty Events: Information for the Public
(Available at http://emergency.cdc.gov/masscasualties/braininjuriespub.asp)

Mass Casualties: Burns
(Available at http://emergency.cdc.gov/masscasualties/burns.asp)

Coping With a Traumatic Event: Information for the Public
(Available at http://emergency.cdc.gov/masscasualties/copingpub.asp)

Various local and state health departments use these fact sheets, either by reproducing the content or by providing links to the CDC site. In some cases, the health departments also provide links to the DHS/FEMA materials.

Several examples of health department websites with terrorist bombing content are also provided below.

- Minnesota Department of Health
- Virginia Department of Health
- Southern Nevada Health District

2. Message Templates

In addition to the fact sheets/web content described above, there is one publicly available site where message templates are provided for use in terrorist bombing incidents. The site is called "First Hours." The site was developed by the Office of Public Affairs of the U.S. Department of Health and Human Services (HHS) and the Centers for Disease Control and Prevention (CDC). It was designed to aid local and state agencies in their message development efforts for emerging threats. "First Hours" draws on various studies, including the Pre-Event Message Development Project, and includes sample messages, templates, and other risk communication resources for use in several types of incident. One set of templates deals specifically with suicide bombing incidents. (See http://emergency.cdc.gov/firsthours/intro.asp)

3. Public Outreach and Awareness Programs

At the local level, several innovative outreach and awareness efforts have been undertaken to deal with the threat of IEDs/terrorist bombings. Selected examples are highlighted here.

1. Southern Nevada Health District

With a TIIDE grant ("Terrorism Injuries: Information, Dissemination and Exchange") from the CDC's National Center for Injury Prevention and Control, the Southern Nevada Health District has undertaken a unique effort to help make hotel and casino security officers more aware of the terrorist bombing threat and acquaint them with appropriate actions to be taken should an actual bombing occur.

The rationale is clear: hotels and casinos are places where large numbers of people congregate. The metro Las Vegas area, which has a resident population of about 2 million people, sees a visitor volume estimated to be 39 million people a year. In addition, hotels and casinos are high profile locations. Both facts make them potentially attractive as targets for terrorists. In light of this, it is important for hotel and casino security personnel to know how to recognize possible explosive devices. In addition, these members of staff, rather than the traditional first responders, would be first on the scene after a bombing. Thus, it is important for them to know what to do to manage the incident and render assistance to the affected public.

The Southern Nevada Health District Office of Emergency Medical Services, in cooperation with CDC and the American College of Emergency Physicians, created a special training DVD plus supporting materials. The course, entitled, "Bombings: Awareness, Injury Patterns and Care," includes content on such key topics as types of explosives and explosive incidents, identifying possible explosive devices, what to do should a device be found, disaster response, scene safety, the various causes and types of blast injuries, military experience, the use of tourniquets, special needs patients (children, disabled, elderly, pregnant women, people with language barriers) and where to find additional information.

As of late-June 2010, approximately 800 DVDs and related materials had been distributed to 115 organizations. In addition to local distribution in the Las Vegas area, the Health District has provided DVDs and related materials to hotel/casino security and gaming control boards/commissions from eleven states, several Native American tribes and three foreign countries.

In an effort to gauge the effectiveness of the training, the District asks those using the materials to submit pre-tests/post-tests. However, this is not mandatory. Thus, the response rate has been relatively low, with only 115 tests being returned (76 from individuals in local hotel/casino security and 39 from healthcare professionals). Nevertheless, the results obtained thus far suggest that the materials have been useful.

Across the 115 people, the average score on the pre-test was 50% and the average score on the post-test was 80%. Meanwhile, a slightly larger number of people have returned course evaluation forms. Out of a total of 124 evaluations returned, 98% of respondents indicated they would recommend the course to others.

2. New York City (NYPD)

In New York City, an innovative project has been undertaken to provide terrorism awareness and response training to two key groups: security personnel in commercial office buildings, and doormen in residential buildings.

The overall project is known as the NY Safe & Secure. The training for security personnel in commercial office buildings is a "collaborative effort between property owners, security managers, tenants and security officers with technical assistance and cooperation from security experts and the City of New York." The program provides a 40-hour course to help security officers recognize and deal effectively with potential terrorist threats. The training is conducted by off-duty NYPD officers and recently retired instructors from the Police Academy. Among the specific topics covered in the course are terrorism awareness and response (including substantial attention to conventional explosive devices and improvised explosive devices, as well as the way to handle a report of a "suspicious package" or bomb threat), observation skills, access control, effective communication, laws and liabilities, incident response (including preparation of the scene for responding personnel), tactics used by perpetrators, fire protection and use of fire extinguishers. In addition, as part of the course, security personnel are trained and become certified to administer Cardio-Pulmonary- Resuscitation (CPR) and use an automated external defibrillator (AED).

The second component of the NY Safe & Secure program has focused on doormen in residential buildings. The residential program is a "collaborative effort among building service workers, property management companies, emergency service personnel and tenants." Its centerpiece is a four-hour course that trains doormen to "observe, evaluate and respond to terrorist attacks and infrastructure emergencies." Among the topics included in the curriculum are the following: observation skills and the role that observation plays in deterring criminal activity, effective communication, access control, indicators of a terrorist event, the role of a building service worker at the scene, fire safety and fire extinguishers, weapons of mass destruction, suspicious packages and bomb

threats, emergency kits, sheltering in place, and the psychological effect of emergency preparedness.

"We'd like to be the third leg, after fire and police," the president of SEIU Local 32-B-J (which represents doormen, supers and building staff) was quoted as saying in New York magazine (Maher, June 24, 2002). "We'd like to coordinate citywide procedures like evacuation plans, even checklists on how to look for terrorist behavior." Literally hundreds of buildings with thousands of service personnel are participating in the NY Safe & Secure residential program.

3. New York City (MTA)

Another innovative terrorism awareness program in New York is the "If You See Something, Say Something" campaign. The year after the 9/11 terror attacks, the Metropolitan Transportation Agency (MTA) made the decision to launch a campaign to encourage subway, bus and train riders to be more aware of unattended bags or packages and to report suspicious activity to authorities.

The agency conducted foundational research and also enlisted a respected advertising firm to help. The result was the "If You See Something, Say Something" campaign, which began placing posters and placards on the transportation system in 2003. The current version of the campaign encourages people to "Be Suspicious of Anything Unattended" and advises them to call the counter-terrorism hot line, 1-888-NYC-SAFE, which is operated by the police department. The campaign is extensive.

The transportation authority has spent $2 million to $3 million a year on the "If You See Something, Say Something" campaign for radio, television and print advertisements, with much of the money coming from grants from the federal Homeland Security Department (Fernandez, 2010).

Furthermore, it has reportedly had a huge influence on terrorism awareness and transit security campaigns around the globe:

Since obtaining the trademark in 2007, the authority has granted permission to use the phrase in public awareness campaigns to 54 organizations in the United States and overseas, like Amtrak, the Chicago Transit Authority, the emergency management office at Stony Brook University and three states in Australia (Fernandez, 2010).

Other agencies in New York City are also involved in awareness and information efforts. For example, the Office of Emergency Management (OEM) has a major campaign entitled Ready New York. Although the campaign focuses on preparedness for emergencies in general, it does include significant information about terrorism and explosions in its signature guide and web content. OEM's outreach efforts are extensive. According to figures provided by the agency, OEM distributed over 550,000 guides in 2009 via 3-1-1, requests, events and mailings. Over 100,000 guides were also downloaded via the OEM website. All Ready New York guides are now available on audio tape. OEM was also was represented at 408 events in 2009, giving it many opportunities for direct contact with citizens. Other activities included the Ready New York Kids Pilot Program (with the Department of Education) in Brooklyn and the Ready

Schools Initiative, which aims to educate children in second and third grades in emergency preparedness; Ready New York for Business; and Ready New York for Seniors and People with Disabilities, which reaches out to senior centers and senior fairs and also recorded a radio spot for the visually impaired.

References

After a Terrorist Bombing: Health and Safety Information for the General Public. Centers for Disease Control and Prevention. See http://www.bt.cdc.gov/masscasualties/afterbombing.asp

Alerting America: Effective Risk Communication: Summary of a Forum. A Summary of the Natural Disasters Roundtable by R Floroiu, RT Sylves, The National Academies, October 31, 2002.

Analysis of Focus Groups with Blind and Visually Impaired Individuals Concerning Emergency Alerts. Prepared by the American Foundation for the Blind for CPB/WGBH's National Center for Accessible Media, February 14, 2006.

AP-GfK-Roper poll. Telephone survey of the American general population, June 2010.

Becker SM (2001). Meeting the Threat of Weapons of Mass Destruction Terrorism: Toward a Broader Conception of Consequence Management. Military Medicine 166(S2):13-16.

Becker SM (2004). Emergency communication and information issues in terrorism events involving radioactive materials. Biosecurity and. Bioterrorism. 2(3), 195–207.

Becker SM (2007). Communicating Risk to the Public after Radiological Incidents. British Medical Journal 335(7630):1106-7.

Becker SM (2009). Social, Psychological and Communication Impacts of an Agroterror Attack. In: Wiley Handbook of Science and Technology for Homeland Security, JG Voeller, Editor, Wiley Publishers.

Bomb-Making Materials Awareness Program (BMAP): Private Sector User Guide. U.S. Department of Homeland Security.

Burns WJ, Slovic P (2007). The diffusion of fear: Modeling community response to a terrorist strike. The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology 4; 298.

Clarke L, Chess C, Holmes R, O'Neill KM (2006). Speaking with One Voice: Risk Communication Lessons from the US Anthrax Attacks. Journal of Contingencies and Crisis Management 14 (3): September 2006.

Communicating in the First Hours: Suicide Bombing. Short and extended messages. Centers for Disease Control and Prevention. See http://emergency.cdc.gov/firsthours/suicidebomb/index.asp

Coppola DP and Maloney EK (2009). Communicating Emergency Preparedness: Strategies for Creating a Disaster Resilient Public. CRC Press.

Corley C (2010). Blacks Show New Trust In U.S. Government. National Public Radio. April 29, 2010.

Economist/YouGov Poll of General Population Respondents. July 24-27, 2010.

Emergency Communications: Improving Communications with Train Passengers Trapped Underground following a Mass Casualty Incident. Lessons Learned Information System (LLIS).

"Explosions." Section 4.2 in Are You Ready? Federal Emergency Management Agency (FEMA).

Explosions. Ready.gov. Department of Homeland Security. See http://www.ready.gov/america/beinformed/explosions.html

Explosions Visual Guide. Ready.gov. Department of Homeland Security. See http://www.ready.gov/america/_downloads/explosions.pdf

FEMA (December 2009). Personal Preparedness in America: Findings from the 2009 Citizen Corps National Survey. August 2009 (Revised December 2009). Federal Emergency Management Agency.

FEMA (June 2009). Personal Preparedness in America: Findings from the Citizen Corps National Survey. June 2009. Federal Emergency Management Agency.

Fernandez M (2010). A Phrase for Safety After 9/11 Goes Global. New York Times, May 11, 2010, page A 17.

Freedman L (2005). The politics of warning: Terrorism and risk communication. Intelligence and National Security 20(3): 379 – 418.

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.

Gershon RRM, Hogan E, Qureshi KA, Doll L (2004). Preliminary results from the World Trade Center evacuation study - New York, 2003. Centers for Disease Control and Prevention Morbidity and Mortality Weekly Reports 55(35) 815-816.

Guide to Mail Center Security. U.S. Postal Inspection Service. Publication 166. March 2008.

Halloran L (2010). Pew Poll: Trust In Government Hits Near-Historic Low. National Public Radio, April 18, 2010. See http://www.npr.org/templates/story/story.php?storyId=126047343

Heroes of N.Y. Times Square bomb attempt show why vigilance matters. Editorial. The Washington Post, Tuesday, May 4, 2010.

Hildebrand S, Bleetman A (2007). Comparative study illustrating difficulties educating the public to respond to chemical terrorism. Prehospital and Disaster Medicine 22(1): 35–41.

Hobbs J, Kittler A, Fox S, Middleton B, Bates DW (2004). Communicating Health Information to an Alarmed Public Facing a Threat Such as a Bioterrorist Attack. Journal of Health Communication, Volume 9: 67–75.

Homeland Security Advisory Council. Homeland Security Advisory System Task Force Report and Recommendations. September 2009.

IED Attack: Improvised Explosive Devices. A Fact Sheet from the National Academies and the Department of Homeland Security. Project on News and Terrorism: Communicating in a Crisis. National Academy of Engineering of the National Academies. See http://www.dhs.gov/xlibrary/assets/prep_ied_fact_sheet.pdf

Injuries and Mass Casualty Events: Information for the Public. Centers for Disease Control and Prevention. See http://www.bt.cdc.gov/masscasualties/injuriespub.asp

Kearon T, Mythen G, Walklate S. Making Sense of Emergency Advice: Public Perceptions of the Terrorist Risk. Security Journal, 2007, 20, (77 – 95).

Lasker RD (2004). Redefining Readiness: Terrorism Planning through the Eyes of the Public. New York, NY: The New York Academy of Medicine.

Luck and Vigilance. Editorial. The New York Times, May 3, 2010.

Maher D (2002). Homeland Security. New York Magazine, June 24, 2002.

Manzi C, Powers MJ, Zetterlund K (2002). Critical Information Flows in the Alfred P. Murrah Building Bombing: A Case Study. Terrorism Studies Series, Special Report 3, Chemical and Biological Arms Control Institute.

Margetta R (2010). Survey: Majority of U.S. Citizens Expect Terrorists to Attack with IEDs. CQ Homeland Security. April 6, 2010.

Marist College Institute for Public Opinion. How Americans Feel About Terrorism and Security: Two Years After 9/11. Survey conducted on behalf of the National Center for Disaster Preparedness and the Children's Health Fund; August 2003.

Mayhorn CB (2005). Cognitive Aging and the Processing of Hazard Information and Disaster Warnings. Natural Hazards Review 6(4): November 1, 2005.

McDermott R and Zimbardo PG (2007). The psychological consequences of terrorist alerts. Chapter 23 in Psychology of Terrorism, B Bongar, LM Brown, LE Beutler, JN Breckenridge, PG Zimbardo, eds., Oxford University Press.

Meredith LS, Shugarman LR, Chandra A, Taylor SL, Stern S, Beckjord EB, Parker AM, Tanielian T (2008). Analysis of Risk Communication Strategies and Approaches with At-Risk Populations to Enhance Emergency Preparedness, Response, and Recovery: Final Report. Prepared by RAND for the United States Department of Health and Human Services, Office of the Assistant Secretary for Planning and Evaluation, WR- 598-HHS, December 2008.

Mileti DS, Sorensen JH (1990). Communication of Emergency Public Warnings: A Social Science Perspective and State-of-the-Art Assessment. Washington, DC: Federal Emergency Management Agency.

Mileti DS, R Bandy, LB Bourque, A Johnson, M Kano, L Peek, J Sutton, M Wood (2006). Bibliography for Public Risk Communication on Warnings for Public Protective Actions Response and Public Education. Revision 4.

Miller Steiger D (2010). Improvised Explosive Devices: Perceptions and the Domestic Threat. Gallup Government. Presentation given by D Miller Steiger at the Homeland Security Policy Institute (HSPI) Forum on Improvised Explosive Devices: Perceptions and the Domestic Threat, George Washington University, April 6, 2010.

Morales L (2010). In U.S., Confidence in Newspapers, TV News, Remains a Rarity. Gallup Poll, August 13, 2010.

National Council on Disability (2009). Effective Emergency Management: Making Improvements for Communities and People with Disabilities. August 12, 2009.

NRC (2007). Countering the Threat of Improvised Explosive Devices: Basic Research Opportunities: Abbreviated Version. Committee on Defeating Improvised Explosive Devices: Basic Research to Interrupt the IED Delivery Chain, National Research Council of the National Academies. Washington, DC: The National Academies Press.

NRC (2008). Disrupting Improvised Explosive Device Terror Campaigns: Basic Research Opportunities: A Workshop Report. Committee on Defeating Improvised Explosive Devices: Basic Research to Interrupt the IED Delivery Chain, National Research Council of the National Academies. Washington, DC: The National Academies Press.

NSTC (2000). Effective Disaster Warnings. Report by the Working Group on Natural Disaster Information Systems, Subcommittee on Natural Disaster Reduction, National Science and Technology Council, Committee on Environment and Natural Resources.

NSTC (2008). Research Challenges in Combating Terrorist Use of Explosives in the United States. Executive Office of the President, National Science and Technology Council, Subcommittee on Domestic Improvised Explosive Devices.

Perry RW, Lindell MK (2003). Understanding citizen response to disasters with implications for terrorism. Journal of Contingencies and Crisis Management, 11(2), 49-60.

Pew Research Center (2010). The People and Their Government: Distrust, Discontent, Anger and Partisan Rancor. Pew Research Center for the People & the Press. April 18, 2010.

PPW (2004). Partnership for Public Warning. Protecting America's Communities: An Introduction to Public Alert & Warning.

Preparing for a Terrorist Bombing: A Common Sense Approach. Centers for Disease Control and Prevention. See http://www.bt.cdc.gov/masscasualties/preparingterroristbombing.asp

Public Response to Terrorism (2008). Findings from the National Survey of Disaster Experiences and Preparedness. Prepared by M Kano, MM Wood, DS Mileti, LB Bourque. November 12, 2008.

Rogers MB, Amlot R, Rubin GJ, Wessely S, Krieger K (2007). Mediating the social and psychological impacts of terrorist attacks: The role of risk perception and risk communication. International Review of Psychiatry 19(3): 279–288.

Ronan KR and Johnston DM (2005). Promoting Community Resilience in Disasters: The Role for Schools, Youth, and Families. Springer.

Ropeik D. Risk Communication – An Overlooked Tool in Combating Terrorism. In: Wiley Handbook of Science and Technology for Homeland Security, JG Voeller, Editor, Wiley Publishers.

Saad L (2009). Majority of Americans Think Near-Term Terrorism Unlikely. Gallup Poll, December 2, 2009.

Sahm C. Hard Won Lessons; Transit Security. Safe Cities Project, March 2006.

Tierney K. Strength of a City: A Disaster Research Perspective on the World Trade Center Attack. Social Science Research Council – After Sept. 11. Accessed Jan 18, 2010. See http://essays.ssrc.org/sept11/essays/tierney.htm

Vanderford ML (2004). Breaking new ground in WMD risk communication: the pre-event message development project. Biosecurity and Bioterrorism 2(3), 193–194.

Wray RJ, Becker SM, Henderson N, Glik D, Jupka K, Middleton S, Henderson C, Drury A, Mitchell EW (2008). Communicating with the public about emerging health threats: Lessons from the Pre-Event Message Development Project. American Journal Public Health 98: 2214-2222.

Chapter 4

Trust, Confidence, Credibility, and Improvised Explosive Devices: International Perspectives

Authors: **Ortwin Renn, Ph.D. and Piet Sellke**
University of Stuttgart and
Dialogik: Non-Profit Institute for Communication and Cooperation Research

With the advent of ever more complex technologies and the progression of scientific methods to detect even smallest quantities of harmful substances, personal experience of risk has been more and more replaced by information about risks, as has individual control over risk been by institutional risk management. As consequence, people rely more than ever on the credibility and sincerity of those from whom they receive information about risk (Barber 1983; Blair 1987; Zimmerman 1987; Johnson 1999; Löfstedt 2003, 2005). Thus, trust in institutional performance has been a major key for risk responses. Trust in control institutions is able to compensate even for a negative risk perception and distrust may lead people to oppose risks, even when they are perceived as small.

To make these terms more operational, it makes sense to identify the major attributes that constitute trust, confidence, and credibility. The literature includes several approaches (McGuire 1985; Barber 1983; Sheridan 1985; Lee 1986; Earle and Cvetkovich 1996; Cvetkovich 2000, Löfstedt 2003). In their 1991 review (Renn and Levine 1991), Renn and Levine tried to amalgamate some of the proposed suggestions from the literature and developed a classification scheme consisting of six components. Renn later added empathy to this list (based on suggestions by Covello 1992, Peters at al.1997; see Renn 2008). Table 2 lists the seven components:

TABLE 1: Components of trust

Components	*Description*
Perceived competence	degree of technical expertise in meeting institutional mandate
Objectivity	lack of biases in information and performance as perceived by others
Fairness	acknowledgment and adequate representation of all relevant points of view
Consistency	predictability of arguments and behavior based on past experience and previous communication efforts
Sincerity	honesty and openness

Empathy	degree of understanding and solidarity with potential risk victims
Faith	perception of "good will" in performance and communication

Trust relies on all seven components. Still, a lack of compliance in one attribute can be compensated by a surplus of goal attainment in another attribute. If objectivity or disinterestedness is impossible to accomplish, fairness of the message and faith in the good intention of the source may serve as substitutes. Competence may also be compensated by faith and vice versa. Consistency is not always essential in gaining trust, but persistent inconsistencies destroy the common expectations and role models for behavioral responses. Trust cannot evolve, if social actors experience inconsistent responses from others in similar or even identical situations. Finally empathy signals the public that the institution cares about the effects of its performance. If people assign high competence to an organization, empathy helps but is not essential. If performance is in doubt, empathy can make all the difference in the world between trust and distrust.

For analytical purposes, it seems appropriate to differentiate between different levels of trust, confidence, and credibility, depending on the source and the situation. Renn and Levine developed, therefore, a classification scheme that is composed of five distinctive levels of analysis: trust in a message, confidence in a communicator, confidence in an institution based on source perception, credibility of institutions based on institutional performance, and climate for trust and credibility in a macro-sociological context.

Table 2: Factors of credibility for different levels of analysis

MESSAGE:

Positive	***Negative***
Timely Disclosure of Relevant Information[1]	Stalled or Delayed Reporting[1]
Regular Updating With Accurate Information[1]	Inconsistent Updating
Clear and Concise[1]	Full of Jargon[2]
Unbiased[3]	Biased[3]
Sensitive to Values Fears and Public Perception[3]	Inconsiderate of Concerns of Public[4,5]
Admits Uncertainty[1]	Claims the Absolute Truth
From a Legitimate Reputable Source[3,4]	From a Questionable Source
Organized Message[5]	
Use of Metaphors[5]	Too Abstract[5]
Explicit Conclusions[5]	Receiver Derives Own Conclusion[5]
Positive Information Recorded in Early Part of Message[5]	
Forceful and Intense[6]	Dull[6]

PERSON:

Positive	*Negative*
Admits Uncertainty[1,3]	Cockiness
Responds to Emotions of Public[3]	Indifference
Appears Competent[1,6]	
Similarity with Receiver[5,6]	Perceived as Outsider[3]
Has Some Personal Stake in the Issue[3]	
Clear and Concise[1]	Too Technical[2]
Perceived as 'Expert'[5,6]	
Perceived as 'Attractive'[5]	
Charismatic[5]	
Trustworthy-Honest, Altruistic, and Objective[6]	
Empathetic with Receiver	Displays no empathy

INSTITUTIONS:

Positive	*Negative*
Positive Personal Experience[7]	Negative Personal Experience[7]
Strong, Competent Leadership[7]	Perceived Incompetence[7]
Positive Labor Relations[7]	Layoffs/Hiring Freeze Strikes[7]
Sound Environmental Policy[7]	Irresponsible Environmental Policy
Produces Safe and Good Goods/Services[7]	Poor Quality Goods/Services[7]
Positive Past Record of Performance[7]	Negative Past Record of Performance[7]
Reasonable Rates[8]	Exorbitant Prices[8]
Undertakes Socially Relevant Tasks[9]	
Practical Contributions to Every Day Life[10]	
Benefits Outweigh Costs[11]	Magnitude of Risk Taking Greater than Benefits[11]

POLITICAL / CULTURAL CONTEXT

Positive	*Negative*
Faith in Institutional Structures[7]	Perception of Structural Decline[7]
Checks and Balance System Functioning Well[7]	Poor Leadership/Incompetence[7]
	Corruption/Scandal[7]
	Energy Crisis
	Perception of Unfair Taxation
New and Innovative Ideas[7]	
	Perception of Worsening Financial Situation[7]

Social Unrest[7]

Terrorism[7]

Notes for Tables:

1- New Jersey Department of Environmental Protection, Division of Science and Research: *Improving Dialogue with Communities.* By Billie Jo Hance, Caron Chess, and Peter Sandman. January 1988.

2- Parker, L.: Safety Board Hearings Focusing Public Atten tion Rather than Solving Crisis. Washington Post, July 29, 1988.

3- Gricar, B. G. H. and Baratta, A.J.: Bridging the In formation Gap at Three Mile Island: Radiation Monitoring by Citizens. *Journal of Applied Behavioral Science.* Volume 19, 1983.

4- Anderson, C. Abstract and Concrete Data in the Perseverance of Social Theories: When Weak Data Lead to Unshakeable Beliefs. *Journal of Experimental Social Psychology*. 19, (1983), 93-108

5- Lee, T.: Effective Communication of Information About Chemical Hazards. *The Science of the Total Environment,* 51 (1986), 149-183.

6- Covello, V.T.; Slovic , P. and von Winterfeldt, D. 1986: Risk Communication: A Review of the Literature. Risk Abstracts , 3, 4(1986), 172-182

7- Lipset, S. M. and Schneider, W.:. *The Confidence Gap; Business, Labor, and Government, in the Public Mind.* The Free Press : New York 1983.

8- Burnham, J. C.; American Medicine's Golden Age: What Happened to It? *Science*. 215, 19 (1982).

9- La Porte, T. R and Metlay, D.: Technology Observed: Attitudes of a Wary Public. *Science*, 188, 11, (April 1975).

10- Pion G. M. and Mark W. Lipsey, M.W.: Public Attitudes Toward Science and Technology: What Have the Surveys Told Us? *Public Opinion Quarterly,* 45 (1981), 303-316

11- Slovic, P. Fischhoff, B. and Liechtenstein, S.: Perception and Acceptability of Risk from Energy Systems In: A. Baum & J. E. Singer (eds): *Advances in Environmental Psychology,* Vol. 3, *Energy: Psychological Perspectives.* Erlbaum: Hillsdale, New Jersey, 1981.

Improving Trust in a Personal Communicator

To improve *trust in a personal communicator,* the major goal is to develop a communication climate that enables the audience to identify with the communicator and to share his or her experiences and beliefs. The more a communicator manages to avoid the mask of an institutional spokesperson and the more he or she can express compassion and empathy for the audience, the more likely the audience will identify with the speaker and feel compelled to the arguments. Conveying probabilistic information is a real challenge, but can be done in reference to everyday experience of budget constraints and consumer products. Furthermore, evidence of successful uses of risk analyses in hazard management can serve as demonstration to define the role and limitations of risk analysis in improving public health and the environment. Peripheral cues should be confined to commonly shared symbols, appealing formats and surprises in openness and honesty, and should definitely avoid negative labeling of potential opponents or typical advertising gimmicks. Peripheral cues are important for successful communication, but cues have to be selected carefully to please the peripherally and centrally interested audience.

Improving the Credibility of an Institution

To improve the *credibility of an institution,* the vital factor is performance, not public relations. Confidence has to be gained by meeting the institutional goals and objectives. In addition, credibility is linked to the evidence of being cost-effective and open to public demands. These two goals are often in conflict with each other (Kasperson 1987), but they have to be treated as complementary, and not as substitutive goals. Fairness and flexibility are major elements of openness. In addition to assuring sufficient external control and supervision, public participation may be implemented as a means to demonstrate the compliance with the political mandate and to avoid the impression of

hidden agendas. On the premise of good performance, communication programs can be designed that reflect these accomplishments. Such programs should provide honest, complete and accurate information that is responsive to the needs and demands of the prospective audience. This can only be done if the source engages in an organized effort to collect feedback from the audience and establish a two-way communication process. Involvement of citizens, open house policies, discussion forums, open TV channels or other means should be explored to assure the functioning of the two-way communication structure.

Improving the Social Climate

To improve the social climate is not within the realm of possibilities for a single communicator. But large-scale organizations or association of organizations can affect the overall climate. One way to improve the climate is to accept and even endorse checks and balances in the control of the organization. The other obvious solution is to demonstrate the flexibility and foresight of the organization in meeting and anticipating new public claims and values. The impersonal nature of institutions may be mitigated by providing special local services and by engaging in community activities and programs. Governmental institutions will receive more credibility, if they do not leave the impression of permanent crisis management, but of competence and preparedness for long-term threats and challenges (in particular pertaining to environment and technology). Many different factors affect credibility. On the personal level, appearance, communication style, honesty and creating an atmosphere of identification of the audience with the communicator are major variables that influence credibility. On the institutional level, the actual performance in terms of role fulfillment, cost-effectiveness and public expectations as well as openness to new claims and demands constitutes confidence and helps to build credibility. Furthermore, the social climate and the level of controversy associated with the issue, affect the assignment of credibility, independent of the performance of the actors involved.

References

Adams, W.C. 1986: Whose Lives Count? TV Coverage of Natural Disasters. Communication, 36, (2), 113-122

Anderson, C. 1983: Abstract and Concrete Data in the Perseverance of Social Theories: When Weak Data Lead to Unshakeable Beliefs. Environmental Social Psychology, 19, 93-198

Arpan, L.M. & Pompper D. 2003: Stormy weather: testing "stealing thunder" as a crisis communication strategy to improve communication flow between organisations and journalists, Public Relations Review, 29, 291–308.

Barber, B. 1983: The Logic and Limits of Trust. Rutgers University Pres: New Brunswick

Baker, E. J. 1987 Evacuation in response to hurricanes Elena and Kate. Unpublished draft report. Tallahassee, FL: Florida State University.

Blair, E.H. 1987: Discussion on Responsibilities of Risk Communication. In: J.C. Davies, V.T. Covello, and F.W. Allen (eds): Risk Communication. The Conservation Foundation: Washington, D.C., pp. 35-38

Boano, C. (2010). Disasters, crisis and communication; a literature review. CrisComScore Studies, No. 1.1

Boholm, A. 1998: Comparative Studies of Risk Perception: A Review of Twenty Years of Research. Journal of Risk Research, 1 (2), 135-163

Brehmer, B. 1987: The Psychology of Risk. In: Singleton W.T. and Howden J. (eds.): Risk and Decisions. Wiley: New York, 25-39

Breakwell, G. M. and Barnett, J. 2002: The Impact of Social Amplification of Risk on Risk Communication. Health & Safety Executive, Contract Research Report 332/2001, HMSO, London.

Brown R. 1965: Social psychology. The Free Press: New York.

Chess, C.; Hance, B.J. and Sandman, P.M. 1988: Improving Dialogue with Communities: A Short Guide for Government Risk Communication. Submitted to New Jersey Department of Environmental Protection, Division of Science and Research, Trenton, New Jersey. Environmental Communication Research Program. Rutgers University: New Brunswick, New Jersey.

Chess, C.; Hance, B.J. and Sandman, P.M. 1989: Planning Dialogue with Communities: A Risk Communication Workbook. Environmental Communication Research Program. Rutgers University: New Brunswick, New Jersey.

Chess, C., Clarke L., Holmes, R. & O'Neill, K. M. (2006). Speaking with One Voice: Risk Communication Lessons from the US Anthrax Attacks. Journal of Contingencies & Crisis Management, 14(3), 160-169

Coombs, W.T (2007). Ongoing Crisis Communication: Planning, Managing and Responding. Los Angeles : Sage

Covello, V.T. 1983: The Perception of Technological Risks: A Literature Review. Technological Forecasting and Social Change, 23, 285-297

Covello, V.T. 1992: Trust and Credibility in Risk Communication. Health and Environmental Digest, 6, (1), 1-3

Covello, V.T.; Slovic, P. and von Winterfeldt, D. 1986: Risk Communication: A Review of the Literature. Risk Abstracts, 3 (4), 172-182

Covello, V.T. and Allen, F. 1988: Seven Cardinal Rules of Risk Communication. U.S. Environmental Protection Agency: Washington, D.C.

Covello, V.T. and Sandman, P.M. 2001: Risk Communication: Evolution and Revolution. In: A. Wolbarst (ed.): Solutions to an Environment in Peril. Johns Hopkins University Press: Baltimore, pp. 164-178. http://www.psandman.com/articles/covello.htm

Covello, V.T.; Sandman, P.M. and Slovic, P. 1988: Risk Communication, Risk Statistics and Risk Comparisons: A Manual for Plant Managers. Chemical Manufacturers Association: Washington, D.C.

Covello, V.T.; McCallum, D.B. and Pavlova, M. (eds.) 1989: Effective Risk Communication: The Role and Responsibility of Government and Non-Government Organizations. Plenum Press: New York

Cvetkovich, G. 2000: Attributions of Social Trust. In Cvetkovich, G. and Löfstedt, R. (eds.): Social Trust and the Management of Risk: Advances in Social Science Theory and Research. . Earthscan Press: London.

DeFleur, M.L. and Ball-Rokeach,S. 1982: Theories of Mass Communication. 4th edition. Longman: New York.

De Marchi, B. 1995: Environmental Problems, Policy Decisions and Risk Communication. What is the Role for Social Sciences? Science and Public Policy, 22, 157-161

Dillman, D., Schwalbe, M., & J. Short, J. 1983: Communication behavior and social impacts following the May, 18, 1980, eruption of Mt. St. Helens. In S.A.C. Keller (Ed.) Mt. St. Helens One Year Later, pp. 191-198. Cheny, WA: Eastern University Press.

Drabek, T. E. 1969: Social processes in disaster: Family evacuation. Social Problems, 16, 336-349

Drottz-Sjöberg, B.-M. 2003: Current Trends in Risk Communication Theory and Practice, Directory of Civil Defense and Emergency Planning. Norway. Document: Oslo 2003 http://www.dsb.no/article.asp?ArticleID=1216&Rank=3.

Drury, J. & Cocking, C. 2007. The mass psychology of disasters and emergency evacuations: A research report and implications for practice. Unpublished manuscript. University of Sussex, Brighton. Available at; http://www.sussex.ac.uk/affiliates/panic/applications.html

Dunwoody, S. 1992: The Media and Public Perception of Risk: How Journalists Frame Risk Stories. In: D.W. Bromley and K. Segerson (eds.): The Social Response to Environmental Risk: Policy Formulation in an Age of Uncertainty. Kluwer: Dordrecht and Bostom, pp. 75-100

Dunwoody, S. 1999: Scientists, Journalists and the Meaning of Uncertainty. In: S. M. Friedman, S. Dunwoody and C.L. Rogers (eds.): Communicating Uncertainty: Media Coverage of New and Controversial Science. Lawrence Erlbaum: Mahwak, New Jersey, pp. 59-79

Dunwoody, S. and Peters, H.P. 1992: Mass Media Coverage of Technological and Environmental Risks: a Survey of Research in the United States and Germany. Public Understanding of Science, 1 (2), 199-230

Earle, T.C. and Cvetkovich, G. 1996: Social Trust: Toward a Cosmopolitan Society. Praeger: Westport, CT

Fischhoff, B. 1995: Risk Perception and Communication Unplugged: Twenty Years of Process. Risk Analysis, 15 (2), 137-145

Fischhoff, B. (2005). Scientifically Sound Pandemic Risk Communication, Paper prepared for House Science Committee Briefing, December 14, 2005. Retrieved November 26, 2009 from: https://www.healthsystem.virginia.edu/internet/ciag/conference/articles/s2006/fischhoff_pandemic_risk_communication.pdf

Fischhoff, B.; Lichtenstein, S.; Slovic, P. Derby, S.L. and Keeney, R.L. 1981: Acceptable Risk . Cambridge University Press: Cambridge, Mass.

Freudenburg, W.R. 1988: Perceived Risk, Real Risk: Social Science and the Art of Probabilistic Risk Assessment. Science, 242, 44-49

Gould, L.C.; Gardner, G.T.; DeLuca, D.R.; Tiemann, A.; Doob, L.W.; and Stolwijk, J.A.J. 1988: Perceptions of Technological Risks and Benefits. Russel Sage Foundation: New York.

Gutteling, J.M. and Wiegman, O. 1996: Exploring Risk Communication. Kluwer Academic Publishers: Dordrecht.

Hance, B.J.; Chess, C. and Sandman, P.M. 1988: Improving Dialogue with Communities: A Risk Communication Manual for Government. Environmental Communication Research Program, Rutgers University: New Brunswick, New Jersey.

Harro-Loit, H., Vihalemmm T. & Ugur, K. (2010). Reception of information during crises, information channels and response patterns. CrisComScore Studies No. 2.3

Horlick-Jones, T. 1998: Meaning and Conextualisation in Risk Assessment. Reliability Engineering and Systems Safety, 59, 79-89

Hovland, C. J. 1948: Social Communication. Proceedings of the American Philosophical Society, 92, 371-375

Jaeger, C.C.; Renn, O.; Rosa, E.A. and Webler, Th. 2001: Risk, Uncertainty and Rational Action. Earthscan: London.

Jasanoff, S. 1993: Bridging the Two Cultures of Risk Analysis. Risk Analysis, 13 (2), 123-129

Jasanoff, S 1999: The Songlines of Risk. Environmental Values. Special Issue: Risk, 8 (2), 135-152

Johnson, N.R. 1988. Fire in a crowded theatre: A descriptive investigation of the emergence of panic. International Journal of Mass Emergencies and Disasters, 6, 7-26

Johnson, B.B. 1999: Exploring Dimensionality in the Origins of Hazard-Related Trust. Journal of Risk Research, 2, 325-454

Jungermann H., Schütz, H. and Thüring M. 1988: Mental Models in Risk Assessment: Informing People about Drugs. Risk Analysis, 8, 147-155

Kahlor, L.-A.; Dunwoody, S. and Griffin, R.J. 2004: Accounting for the Complexity of Causal Explanations in the Wake of an Environmental Risk. Science Communication, 26 (1), 5-30

Kasperson, R.E. 1986: Six Propositions for Public Participation and Their Relevance for Risk Communication. Risk Analysis, 6 (3), 275-281

Kasperson, R.E. 1992: The Social Amplification of Risk: Progress in Developing an Integrative Framework" in S. Krimsky and D. Golding (eds.): Social Theories of Risk, Praeger: Westport

Kasperson, R.E. and Kasperson, J.X. 1983: Determining the Acceptability of Risk: Ethical and Policy Issues. In: J.T. Rogers and D.V. Bates (eds.): Assessment and Perception of Risk to Human Health. Conference Proceedings. Royal Society of Canada: Ottawa, pp. 135-155

Kasperson, R.E. and Palmlund, I. 1988: Evaluating Risk Communication. In: V.T. Covello; D.B. McCallum and M.T. Pavlova (eds.): Effective Risk Communication. The Role and Responsibility of Government and Nongovernment Organizations. Plenum: New York, pp. 143-158

Kasperson, R.E. and Stallen, P.M. 1991: Introduction. In: R.E. Kasperson and P.M. Stallen (eds.): Communicating Risk to the Public. Kluwer Academic Press: Dordrecht, pp. 1-11

Kasperson R.E. and Kasperson, J.X. 1996: The Social Amplification and Attenuation of Risk. Annals of the American Political and Social Sciences, 545, 95-105

Kasperson, R E.; Renn, O.; Slovic P.; Brown, H.S.; Emel, J.; Goble, R.; Kasperson, J.X.; and Ratick, S. 1988: The Social Amplification of Risk. A Conceptual Framework. Risk Analysis, 8, (2), 177-187

Kasperson, J.X.; Kasperson, R.E.; Pidgeon, N.F. and Slovic, P. 2003: The Social Amplification of Risk: Assessing Fifteen Years of Research and Theory. In: N.F. Pidgeon, R.K. Kasperson and P. Slovic (eds.): The Social Amplification of Risk. Cambridge University Press: Cambridge, Mass., pp. 13-46.

Keating, J.P. 1982. The myth of panic. Fire Journal, 147,

Keeney, R. and von Winterfeldt, D. 1986: Improving Risk Communication. Risk Analysis, 6 (4), 417-424

Kitzinger, J and Reily, J. 1997: The Rise and Fall of Risk Reporting. Media Coverage of Human Genetics Research. `False Memory Syndrome' and `Mad Cow Disease. European Journal of Communication. 12 (3), 319-350

Lasswell, H.D. 1948: The Structure and Function of Communication in Society. In: L. Brison (ed.): The Communication of Ideas. New York, pp. 32-51

Lee, T.R. 1986: Effective Communication of Information about Chemical Hazards. The Science of the Total Environment. 51, 149-183

Leiss, W. (ed.) 1989: Prospects and Problems in Risk Communication. University of Waterloo Press: Waterloo, Ontario Canada

Leiss, W. 1996: Three Phases in Risk Communication Practice. In: H. Kunreuther and P. Slovic (eds.): Challenges in Risk Assessment and Risk Management. Annals of the American Academy of Political and Social Science, Special Issue on Risk Sage: Thousand Oaks, pp.85-94

Leiss, W. 2004: Effective Risk Communication Practice. Toxicology Letters, 149, 399-404

Lipset, S.M. and Schneider, W. 1983: The Confidence Gap. Business, Labor, and Government, in the Public Mind .The Free Press: New York

Löfstedt, R. 2003: Risk Communication: Pitfalls and Promises. European Review, 11 (3), 417-435

Löftstedt, R. 2005: Risk Management in Post Trust Societies. Palgrave Macmillan: London

Lundgren, R.E. 1994: Risk Communication: A Handbook for Communicating Environmental, Safety, and Health Risks. Battelle Press: Columbus, Ohio

Mazur, A. 1994: Technical Risk in the Mass Media. Risk: Health, Safety & Environment, 53, 189-192

Maxwell, Terrence A. (2003): The public need to know: emergencies, government organizations, and public information policies. In: Government Information Quarterly, H. 20 (3), S. 233–258.

McGuire, W.J. 1985: Attitude and Attitude Change. In: G. Lindzey and E. Aronson (eds.): Handbook of Social Psychology. Vol. 2. Random House: New York, pp. 223-346

Morgan, M.G.; Fischhoff, B.; Bostrom, A.; Lave, L. and Atman, C. 1992: Communicating Risk to the Public. Environmental Science and Technology, 26 (11), 2049-2056

Morgan, M.G.; Fishhoff, B.; Bostrom, A. and Atmann, C.J. 2001: Risk Communication. A Mental Model Approach. Cambridge University Press: Cambridge, Mass.

Mulligan, J.; McCoy, E. and Griffiths, A. 1998: Principles of Communicating Risks. The Macleod Institute for Environmental Analysis, University of Calgary: Alberta, Canada

OECD 2002: Guidance Document on Risk Communication for Chemical Risk Management, Series on Risk Management, No. 16. Prepared by O. Renn, H. Kastenholz and W. Leiss. Environment, Health and Safety Publications, Organisation for Economic Co-operation and Development: Paris

OECD, 2003: Stakeholder Involvement Tools: Criteria for Choice and Evaluation, Proceedings of a Topical Session at the 4th meeting of the NEA [Nuclear Energy Agency] Forum on Stakeholder Confidence. Organisation for Economic Co-operation and Development: Paris
http://www.nea.fr/html/rwm/docs/2003/rwm-fsc2003-10.pdf

Otway, H. and Wynne, B. 1989: Risk Communication: Paradigm and Paradox. Risk Analysis, 9 (2), 141-145

Peltu, M. 1985: The Role of Communications Media. In: H. Otway and M. Peltu (eds.): Regulating Industrial Risks. Butterworth: London, pp. 128-148

Peltu, M. 1989: Media Reporting of Risk Information: Uncertainties and the Future. In: H. Jungermann; R.E. Kasperson and P.M. Wiedemann (eds.): Risk Communication. Research Center KFA: Jülich, pp.11-32

Peters, H.P. 1984: Entstehung, Verarbeitung und Verbreitung von Wissenschaftsnachrichten am Beispiel von 20 Forschungseinrichtungen. Report Jül-Spez-1940. Research Center KFA: Jülich, Germany

Peters, H.P. 1986: Public Opinion As a Channel of Communication Between Science and Other Parts of Society. Paper presented at the 11th World Congress of Sociology. New Delhi: August 18-22, 1986

Peters, H.P. 1995: The Interaction of Journalists and Scientific Experts: Co-operation and Conflict Between Two Professional Cultures. Media, Culture & Society, 17 (1), 31-48

Peters, H.P. 2000: The Committed are Hard to Persuade. Recipients' Thoughts During Exposure to Newspaper and TV Stories on Genetic Engineering and Their Effect on Attitudes. In: New Genetics & Society, 19 (3), 367-383

Peters, R.G.; Covello, V.T. and McCallum, D.B. 1997: The Determinants of Trust and Credibility in Environmental Risk Communication: An Empirical Study. Risk Analysis, 17, 43-54

Petts, J.; Horlick-Jones, T. and Murdock, G. 2001: Social Amplification of Risk: The Media and the Public. Health & Safety Executive, Contract Research Report 329/2001. HMSO: London, 2001.

Plough, A. and Krimsky, S. 1987: The Emergence of Risk Communication Studies: Social and Political Context. Science, Technology, and Human Values, 12, 78-85

Quarantelli, E.L. 1960. "Images of Withdrawal Behavior in Disasters: Some Basic Misconceptions." Social Problems 8: 68-79

Rayner, S. 1988: Muddling Through Metaphors to Maturity: A Commentary on Kasperson et al: The Social Amplification of Risk. Risk Analysis , 8 (2), 201-204

Rayner, S. 1990: Risk in Cultural Perspective: Acting under Uncertainty. Kluwer: Dordrecht and Norwell

Rayner, S. 1992: Cultural Theory and Risk Analysis. In: S. Krimsky and D. Golding (eds.): Social Theories of Risk. Praeger: Westport, pp. 83-115

Reich, Z./Bentman, M./Jackman, O. 2009: Crisis communication guide for public organizations, submitted to the European Community's Seventh Framework Programme (FP7), December 2009

Renn, O. 1988: Risk Communication: Concepts, Strategies, and Pitfalls. In: Air Pollution Control Association (ed.): Managing Environmental Risks. Proceedings of the APCA Special Conference in Washington D.C., October 1987 APCA: Washington, D.C., pp. 99-117

Renn, O. 2004: Perception of Risks. The Geneva Papers on Risk and Insurance, 29 (1), 102-114

Renn, O. and Levine, D. 1991: Credibility and Trust in Risk Communication. In: R. Kasperson and P.J. Stallen (eds.): Communicating Risk to the Public. Kluwer Academic Publishers: Dordrecht, pp. 175-218

Renn, O. and Levine, D. 1991: Credibility and Trust in Risk Communication. In: R. Kasperson and P.J. Stallen (eds.): Communicating Risk to the Public. Kluwer Academic Publishers: Dordrecht, pp. 175-218

Renn, O.; Burns, W.; Kasperson, R.E.; Kasperson, J.X. and Slovic, P. 1992: The Social Amplification of Risk: Theoretical Foundations and Empirical Application. Social Issues, 48, (4), 137-160

Reynolds, B. (2002). Crisis and Emergency Risk communication. Center for Disease Control and Prevention.

Reynolds, B. & Seeger M. W. (2005). Crisis and Emergency Risk Communication as an Integrative Model. Journal of Health Communication, 10 (1), 43-55.

Rogers, C.L. 1999: The Importance of Understanding Audiences. In: S. M. Friedman, S. Dunwoody and C.L. Rogers (eds.): Communicating Uncertainty: Media Coverage of New and Controversial Science Lawrence Erlbaum: Mahwak, New Jersey, pp. 179-200

Rohrmann, B. and Renn, O. 2000: Risk Perception Research – An Introduction. In: O. Renn and B. Rohrmann (eds.): Cross-Cultural Risk Perception. A Survey of Empirical Studies. Kluwer: Dordrecht and Boston, pp. 11-54

Rubin, D.M. 1987: How the News Media Reported on Three Mile Island and Chernobyl. Communication, 37, (3), 42-57

Sadar, A.J. and Shull, M.D. 2000: Environmental Risk Communication. Principles and Practices for Industry. Lewis Publishers: Boca Raton

Sandman, P.M. 2005: Tell it Like it is: 7 Lessons from TMI [Three Mile Island]. IAEA Bulletin, 47 (2): http://www.iaea.org/Publications/Magazines/Bulletin/Bull472/index.html

Sandman, P.M.; Weinstein, N.D.; and Klotz, M.L. 1987: Public Response to the Risk from Geological Radon. Communication, 37 (3), 93-108

Sellke, P. / Renn, O. 2010: Risk, Society and Environmental Policy: Risk Governance in a complex World. In: Gross, H. / Heinrichs, M.: Environmental Sociology. European Perspectives and Transdiciplinary Challenges. Springer: Dordrecht.

Sellnow, T.L, Ulmer, R.R, Seeger, M.W & Littlefield, R.S (2009). Effective Risk Communication: A Message-Centered Approach. New York: Springer

Shannon, C.E. and Weaver, W. 1949: The Mathematical Theory of Communication. The University of Illinois Press: Urbana

Sheehy, N.; Wylie, J. and McKeown, G. 2002: Quantifying Risk Amplification Processes: A Multi-level Approach. Health & Safety Executive, Contract Research Report 367/2002. HMSO: London

Sheridan, T.B. 1985: Trustworthiness of Command and Control Systems. Unpublished Manuscript. Massachusetts Institute of Technology: Cambridge, Mass.

Shoemaker, P.J. 1987: Mass Communication by the Book: A Review of 31 Texts. Communication, 37, (3), 109-133

Short, J.F. 1984: The Social Fabric of Risk: Toward the Social Transformation of Risk Analysis. American Sociological Review, 49, 711-725

Sime, J.D. 1983: Affiliative behaviour during escape to building exits. Journal of Environmental Psychology. (3) 21-41

Singer, E. and Endremy, P. 1987: Reporting Hazards: Their Benefits and Costs. Communication, 37, (3), 10-26

Singer, E. and Endremy, P.M. 1994; Reporting on Risk: How the Mass Media Portray Accidents, Diseases, Disasters, and Other Hazards. Risk: Health, Safety & Environment, 5, 184-188

Sjöberg, L. 2000: Factors in Risk Perception. Risk Analysis, 220 (1), 1-11

Slovic, P. 1987: Perception of Risk, Science, 236, (4799), 280-285

Slovic, P. 1992: Perception of Risk: Reflections on the Psychometric Paradigm. In. S. Krimsky and D. Golding (eds.): Social Theories of Risk. Praeger: Westport, pp.117-152

Slovic, P. Fischhoff, B. and Liechtenstein, S.: Perception and Acceptability of Risk from Energy Systems. In: A. Baum & J. E. Singer (eds): Advances in Environmental Psychology, Vol. 3, Energy: Psychological Perspectives. Erlbaum: Hillsdale, New Jersey, 1981

Sood, R.; Stockdale, G. and Rogers E.M. 1987: How the News Media Operate in Natural Disasters. Communication, 37 (3), 27-41

Sorensen, J. 1992: Assessment Of The Need For Dual Indoor/Outdoor Warning Systems And Enhanced Tone Alert Technologies In The CSEPP, ORNL/TM-12095. Oak Ridge, TN: Oak Ridge National Laboratory.

STARC 2006: Current Risk Communication Practices in Selected Countries and Industries, Deliverable D2, Report by the STARC Consortium to the European Commission: London http://starc.jrc.it

Thomas, L.M. 1987: Why We Must Talk About Risks. In: J.C. Davies, V.T. Covello, and F.W. Allen (eds.): Risk Communication. The Conservation Foundation: Washington, D.C., pp. 19-25

UK Department of Health 1998a: Communicating About Risks to Health: Pointers to Good Practice. UK Department of Health: London

[UK], Inter-Departmental Liaison Group on Risk Assessment 1998b: Risk Communication: A Guide to Regulatory Practice. London. http://www.hse.gov.uk/aboutus/meetings/ilgra/risk.pdf

Urquhart J & Heilmann, K. (1984). Risk Watch: the Odds of Life. New York: Facts on File Publications

US-National Research Council 1989: Improving Risk Communication. National Academy Press: Washington, D.C.

US-National Research Council 1996: Understanding Risk. Informing Decisions in a Democratic Society. National Academy Press: Washington, D.C.

Wahlberg, af A: and Sjöberg, L. 1998: Risk Perception and the Media. Final Research Report F14PCT950016. Stockholm. Center of Risk Research, Stockholm School of Economics

Wilkins, L. and Patterson, P. 1987: Risk Analysis and the Construction of News. Communication 37, (3), 80-92

Zimmerman, R. 1987: A Process Framework for Risk Communication. Science, Technology, and Human Values, 12, (3 & 4), 131-137

Zimmerman, R. and Cantor, R. 2004: State of the Art and New Directions in Risk Assessment and Risk Management: Fundamental Issues of Measurement and Management. In: T. McDaniels and M.J. Small (eds.): Risk Analysis and Society. An Interdisciplinary Characterization of the Field. Cambridge University Press, Cambridge, Mass, 451-458

Chapter 5

Social Media, Risk Communication, and the Improvised Explosive Devices (IEDs) Threat

Author: **Michael Palenchar, Ph.D.**
University of Tennessee

Abstract

The simultaneous reality of terrorism and the development of new online and digital capabilities require a re-evaluation of U. S. government strategies for communicating effective risk and crisis messages (Stephenson & Bonabeau, 2007). Technological advances have transformed how crisis management professionals and researchers view, interact with, and disseminate information to affected communities in a crisis situation. Early research shows that many organizations are struggling to define the best practices for using social media for risk and crisis communication and measuring its return on investment.

The purpose of this research report is to examine existing analyses and conduct interviews with experts about social media and the use of digital hand-held mobile devices in risk and crisis situations, to explore how responders and other emergency management personnel have used these devices as communication tools, and to highlight the opportunities and challenges presented by the use of these devices in communication efforts in disasters. Potential issues and implications, such as control, security, right to know, constant change, speed, training, intentionality, transparency, interoperability, information push, privacy, self-efficacy, leveraging stakeholders' communication, policies and guidelines, trust and authenticity, and information overload facing emergency management and risk communication professionals are identified. Discussions include risk communication opportunities and constraints related to social media/Web 2.0 media, whether in mobile devices or static systems.

Introduction

"*If communities depend on information for their survival in times of crisis, then communication technologies are their lifelines.*"
("United Nations Foundation," 2010, p.4)

"The social web is creating a fundamental shift in disaster response—one that will ask emergency managers, government agencies and aid organizations to mix time-honored expertise with real-time input from the public… We need to work together to better respond to that shift."
(American Red Cross, 2010, para. 6)

The dawn of the 21st century has seen the emergence of two themes that require the immediate attention and critical analysis of risk and crisis communication managers. First, we have moved from a state of conflict between well-defined nation states contained within distinct geographical

boundaries to conflict with "terrorist organizations that attack informally, using terror at any time and place, with the goal of undermining confidence in U.S. institutions and the American way of life" (Ressler, 2006, p. 1). Second, technological advances have transformed how crisis management professionals and researchers view, interact with, and disseminate information to affected communities in a crisis situation. As Steven Simon, senior fellow at the Council on Foreign Relations, and Jonathon Stevenson, professor of strategic studies at the U. S. Naval War College, stated in a recent *Washington Post* (2010, May 4), "a sustained urban terrorism campaign could disrupt American society as profoundly as the Sept. 11 attacks – if not more so. As the British and Spanish security forces have learned, there is a delicate balance between vigilant and panic, resilience and over-preparedness, vigorous law enforcement and a police state" (para. 7). How the emergence of Web 2.0 technologies, with a highlighted focus on digital hand-held devices, integrates into this balance is the focus of this report.

How can we make the most effective use of new communication technologies in response to new types of threats facing the governments, citizens, and communities of the United States? Research shows that many organizations are struggling to define the best practices for not only implementing but also measuring social media (Gillpin, 2008), whether it's with risk and crisis communication, customer relations, general public relations and even marketing. The simultaneous reality of terrorism and the development of new online and digital capabilities require a re-evaluation of U. S. government strategies for communicating effective risk and crisis messages (Stephenson & Bonabeau, 2007). New communication technologies provide both challenges and opportunities for risk communication and emergency management professionals. This is a developing focus for risk and crisis communication professionals, with numerous studies currently undergoing, and numerous meetings, such as the *International Conference on Information Systems for Crisis Response and Management* held in Washington DC in May 2008, the *Expert Roundtable on Social Media and Risk Communication During Times of Crisis* at the American Public Health Association headquarters in Washington DC in March 2009, and the recent *Emergency Social Data Summit* in August 2010 in Washington, D.C., *CrisisCongress* Washington, D. C. that convened 80 tech-savvy leaders from five countries to examine and create social media-based options for communities facing disasters, and the Science and Technology (S&T) Directorate, Department of Homeland Security (DHS)-sponsored working-level conference

Risk Communication and the Improvised Explosive Device (IED) Threat.

Among the relevant communication technologies are digital hand-held devices, including mobile phones, personal digital assistants (PDAs), and wireless tablets such as the iPad. The evolution of the mobile phone device has taken center stage in the communication technology realm, shaping the network communications framework and the ways we connect with each other. New applications including text messaging (signal messaging services; SMS), one-to-many communication messages, and photosharing transform messages into multimedia message services (MMS). Professional predictions point to the remarkable power of the hand-held device in the future (Baekel, June, 23, 2008). In 3-5 years the majority of people will no longer buy mobile phones 'to get a phone,' they but it to be online (Baekdal, 2008). According to another expert opinion, the very near future will see social networking done entirely on these mobile devices, as opposed to static workstations, and up to 80 percent of internet traffic will occur on mobile phones or other transferable devices (Baekel, June 23, 2008). Mobile web will be the dominant force for obtaining information no later than 2015 ("New study shows the mobile web will rule by 2015," April 2010). A Morgan Stanley analyst suggested that the world is currently in the

midst of the fifth major technology cycle of the past half-century, predicting that within the next five years more users will connect to the internet over their mobile devices than desktop PCs (Ingram, 2010).

Digital hand-held devices provide a number of advantages to professionals in a disaster or crisis situation, including the ability to maintain continuous communication and to better manage the flow of information (Stephenson & Bonabeau, 2007). In the past, disasters often collapsed the hard-lined communication infrastructures. Along with these advantages, however, come new classes of risk that must be anticipated and managed.

New technologies allow the entire online community – both domestically and internationally – to obtain information that can potentially create more problems for those tasked with managing a crisis. For example, professionals using mobile devices in a crisis or disaster situation must be prepared with adequate training. Otherwise, they might inadvertently consume the entire available bandwidth or cause a complete network crash (Stephenson & Bonabeau, 2007). Officials might experience "sousveillance," in which bystanders use their phones to record video or take photos of emergency personnel who are not acting professionally (Stephenson & Bonabeau, 2007). Under the stress of a crisis, the immediacy of digital communication might result in false information being communicated to stakeholders (Vieweg, et al., 2008). In addition, stakeholders can use digital technologies to create and disseminate their own influence, de-centralizing the dissemination of information and reducing official control.

IED attacks by their very nature, especially domestic attacks, would be a crisis that is chaotic, filled with uncertainty and dread and outrage, and thus a great opportunity for rumors and misperceptions to spread. According to Reynolds (2005), the combination of rumors and misperceptions with the growing plethora of information outlets "and the potential for serious miscommunications increases exponentially" (p. 251). While technology plays an important role in managing communication with all stakeholders, include risk bearers of an IED attack; those stakeholders now have access to more voices. "Although more voices are present in interaction via technology, these voices are largely unrestrained and uncoordinated – potentially creating noise or an illusion of dialogue without meaningful engagement among voices. Technology allows for access but does not necessarily contribute to the quality of arguments" (Meisenbach & Felder, in review).

The purpose of this research report is to examine existing analyses social media and the use of digital hand-held mobile devices in risk and crisis situations, to explore how responders and other emergency management personnel have used these devices as communication tools, and to highlight the opportunities and challenges presented by the use of these devices in communication efforts in disasters. Potential issues and implications facing emergency management and risk communication professionals are identified. Discussions include risk communication opportunities and constraints related to social media or Web 2.0 media, whether in mobile devices or static systems.

RESEARCH QUESTIONS

Five specific questions are raised in regarding social media and digital hand-held communication devices related to a domestic IED attack in the United States.

RQ1: Examine the use of digital hand-held communication devices (cell phones, PDAs, laptop computers, etc.) for transmitting hazard and risk warnings to members of the public who principally rely on these devices for news and communication.

RQ2: Examine current practices and plans for incorporating digital hand-held communication devices into more traditional hazard and risk warning systems.

RQ3: Examine the implications of these devices on public risk perceptions of terrorism and the counter-terrorism efforts of authorities and government officials, given the prevalence of these devices among citizens, and the recent use of these devices for disseminating awareness of local disasters and emergencies.

RQ4: Examine potential use of these devices by local authorities and first responders for communication and coordination of civil populations in the immediate aftermath of terrorist attacks, local emergencies and disasters.

RQ5: Examine the potential these devices hold for coordinating ad hoc search and rescue efforts and volunteer coordination among citizens and groups who do not have access to normal first responder channels.

METHODOLOGY

Two specific research orientations are being used to address the research questions. The first step is a literature review to organize existing information. Four tasks were involved in this process: (1) Collect CIED-related current state of and emerging practice research in the use of Web 2.0 digital communication; (2) Analyze reports undertaken to validate or test CIED risk communication strategies and messages in the use of Web 2.0 digital communication; (3) Analyze reports about experiences and evaluations of CIED communication strategies and messages in the use of Web 2.0 digital communication; and (4) Develop an overall strategic, systematic and structured approach to gathering both primary and secondary research. Establishing document's credibility is critical, with a coding formula based on content, authority and critical standards.

The second step is *empirical investigations* and four tasks are associated with this process. These include: (1) In-depth discussions with key public officials on the front-lines of using Web 2.0 digital communication related to direct threats to public safety and security; (2) In-depth discussions with key private-sector professionals on the front-lines of using Web 2.0 digital communication during risk and crisis events; (3) Analyze stakeholder evaluations of CIED risk communication strategies and messages in the use of Web 2.0 digital communication (as available); and (4) Effort to gain knowledge based on experience, most likely due to the limited amount of industry and scholarly research conducted in this evolving and emerging facet of risk communication.

At this point the researcher conducted 27 interviews with private industry, government, military, research labs, university researchers, and communication practitioners – all involved in the research of, critique of, or daily use of social media within their lines of research, teaching and practice. Interviewees were identified with purposeful snowball-sampling techniques with a combination of low and high moderator involvement called the "funnel" approach (Morgan, 1997). "Qualitative sampling is purposeful because its

practitioners strive to locate themselves at the sites of specific communicative performances and practices" (Lindlof, 1995, p. 126). Participants for the interviews and focus were systematically gathered from the relationships, networks, contacts, and general community knowledge developed during the initial phase of research. Data will be collected until no new significant themes emerged in later interviews. Interviews were conducted in the participants' businesses or homes when possible, via Skype and over the phone as necessary. Interviews began with broad, grand tour questions followed by more specific questions, inviting the participants to describe their own perceptions in their own words. It was anticipated that as the number of interviews conducted increased, there would be an increase in the use of more specific questions to test previous findings and expand on theoretical and practical issues, which was the case. Written memos were used as a device for ongoing evaluation of data, questions, and the decision to end data accrual. Analyzing data is a continuous process that occurs throughout the course of study. The use of an open-ended approach to data analysis lends itself to a more thorough and rich understanding of the phenomena being studied. However, reduction, explanation, and theory issues were addressed prior to conducting the study. Reduction – sort, categorize, prioritize, and interrelate data – followed emerging schemes of interpretations (Lindlof) utilizing the constant comparative coding method (Glaser, Barney & Strauss, 1967).

Risk Society & Right to Know

The principles a risk society and of the public's right to know, self-governance, and community involvement may constitute the core philosophy for using social media to counter IED. The right-to-know approach to public policy – also known as regulation through revelation – is based on the ideas of self-governance and public participation in the decision-making process (Florini, 2007; Hamilton, 2005) and was made into a U. S. federal law in the Emergency Planning and Community Right-to-know Act (EPCRA) of 1986. EPCRA has served as a model for more than 80 other countries since and was the first federal law in the United States to fully embrace the right-to-know approach to public policy.

Related to the concept of right to know, in the last decades of the 20th century, authors including Anthony Giddens (1991) and Ulrich Beck (1992) started to see how the rapidly growing complexity of modern social organizations made it virtually impossible for any governmental institution to deal with social problems, including those related to safety, relying solely on governmental apparatuses. At the same time, more and more authors in the social sciences and humanities have pointed out the failure of exclusively market-based policies in providing just and desirable conditions to society as a whole.

In 1986 Beck published *Risikogesellschaft - Auf dem Weg in eine andere Moderne*, translated to English six years later as *Risk Society*. In it, Beck portrayed a constantly changing world in its process of modernization and free of the traditional gridlocks of the industrial society. Beck's thesis was that society was "witnessing not the end but the *beginning* of modernity – that is, of modernity *beyond* its classical industrial design" (p. 10). For Beck, that new stage of modernity will be what Beck called *reflexive modernization*, one of his central theories: "The argument is that, while in classical industrial society the "logic" of wealth production dominates the "logic" of risk production, in the risk society this relationship is reversed" (p.12). Beck (1992, 1999) also proposed that, with the failure of social institutions to deal with the broad concept of risk, society would need to turn more and more to civic participation and self-governance in all

stages of government and society, such as the use of community residents via social media to address health, safety and environmental issues related to a risk or crisis event. For Beck, only through the inclusion of the public in the decision-making process would governments be able to prevent and ameliorate risk problems. He also defended the concept that well-informed local communities would be more able to monitor and react to local risks. According to Beck, the critique of the scientific development in a reflexive examination belongs in the public sphere, putting the lay public and the scientists at the same level of importance in the political process.

Opportunities and risk in the explosion in the growth of Web 2.0

There is not enough space to even begin to review the explosive growth in risk assessment and risk communication literature since September 11, 2001 (Goldstein, 2005), and though not exactly the same can be stated regarding new information technology literature there is a growing amount of literature. Within all that literature is the expansion of research into *intentionality.* Most risk communication and crisis communication research in the past addressed environmental, chemical or physical agents that are usually considered free of malice or forethought (Goldstein, 2005), but in sharp contrast, terrorist acts such as the use of IED on domestic soil is clearly with malice and forethought and significantly changes the research into the use of Web 2.0 technology within risk communication. Slovik (2002) among others (e.g., Palenchar & Heath, 2009) have added the psychological and cultural impact of terrorism into their risk communication research. Slovik pointed out that terrorist acts create a more disturbing sense of dread than which surrounds natural or manufacturing disasters, partly because there does not seem to be a specific end to the event. "The boundlessness of terrorism adds to its impact on the public perception of risk" (Goldstein, 2005, p. 153).

Numerous government, industry, trade and university research reports demonstrate the explosive growth of Web 2.0 or social media in all levels of the private and public sector. For example, according to a report issued by the Chief Information Officers Council (CIO Council) of the US federal government, "the use of social media for federal services and interactions is growing tremendously, supported by initiatives from the administration, directives from government leaders, and demands from the public" (p. 6). On January 21, 2009, President Barack Obama signed the Transparency and Open Government memorandum, which utilizes Web 2.0 technologies to engage with the public. Social media applications are becoming ever more present in the U. S. government, as evidenced by the numerous social media applications available for U. S. government employees and departments on Apps.gov. Overall, social media characteristics are about openness, conversation and dialogue, relationship development, multiple voices, and getting the message to stakeholders. A 2010 Pew Internet study showed that 82% of internet users (representing 61% of all American adults) looked for information or completed a transaction on a government web site in the past year, with 25% getting advice or information from a government agency about a health or safety issue (Smith, 2010). The study also showed how citizens are organized around new online platforms and beyond web sites, with nearly one-third (31%) of online adults using platforms such as blogs, social networking sites, online video, text messaging and portable digital devices. In addition, the Obama Administration embraced the Federal Communications Commission's National Broadband Plan released in March 2010, and the president signed a presidential memorandum in June 2010 that aims to make available for auction some 500 megahertz of spectrum that is now controlled by the federal government and private

companies that would be mostly designated for commercial use in mobile broadband (Wyatt, 2010).

One recent example demonstrates the possible role of social media during a risk or crisis event. On January 1, 2009, a US Airways flight was heading from New York to North Carolina when it was forced to make a crash landing into the Hudson River. Janis Krums, a citizen on a ferry, took a picture of the plane with his iPhone and uploaded it to TwitPic (a mobile photosharing site that posts directly to Twitter). Within three hours the photo was viewed online 40,000 times and was seen on several national news networks and newspapers (Terdiman, 2009). This is the impact of social media – intensified by mobile technology – to collect and spread instantaneous information.

Within Web 2.0, there is an incredible opportunity to use digital hand-held communication devices for transmitting hazard and risk warnings to the public. Though in the past these devices have been principally designed for news and communication, they are more and more being utilized for information sharing, real time coverage of events, dissemination of information to family and friends about a crisis, location and safety updates of family members and other loved ones, directions away from certain natural or man-made disasters, and other communication facets that relate to crisis and risk communication. For example, Sutton, Palen and Shklovski (2008) showed how community members who experienced the 2007 southern California wildfires sought information using mobile phones to contact friends and family, including the use of information portals and websites advertised in traditional media, individual blogs, web forums, photosharing sites such as Flickr and Picasa, and microblogs such as Twitter. Residents also used mobile technology devices to fill in the information dearth and get more detail that wasn't available in traditional media. In another non-crisis situation but could be applied to an IED attack, new mobile application City Sourced, which allows users in the United States to snap pictures of neighborhood blight and send to officials responsible to fix it. The application included global satellite positioning that pinpoints blight and then sends a Twitter message to City Sourced.

There are limitless and constantly changing utilizations of Web 2.0 media for risk and crisis communication purposes, including but not limited to the following genre of social media outlets and one example for each: (1) social bookmarks such as Dingo; (2) comment and reputation such as DISQUS; (3) crowdsourced content such as dig; (4) blog platforms such as MOVABLE TYPE; (5) blogs/conversations such as Technocrati; (6) blog communities such as MyBlogLog; (7) micromedia such as Twitter; (8) lifestreams such as Ping: (9) SMS/Voice such as pingme; (10) social networks such as Facebook; (11) niche networks such as LinkedIn; (12) customer service networks such as yelp; (13) location sites such as brightkite; (14) video services such as YouTube; (15) video aggregation such as magnify; (16) wiki sites such as TWiki; (17) Live Casting video and audio such as kyte; and (18) picture sharing such as Flickr.

A 2010 American Red Cross on-line survey of the U. S. population over age 18 showed that nearly three out of four participate in at least one online community or social network, with Facebook being the most popular (58%), followed by YouTube (31%), MySpace (24%), and Twitter (15%). Variations in the online communities and social networks include that respondents with children in the household are more likely to use social media (81% vs. 67% for those without children in the household). College graduates are more likely to use social media (78% vs. 67% for those with some college

or less), and 89% of respondents aged 18-34 use online communities or social networks compared to 65% of those aged 35 and older. One in six has used social media to get information about an emergency, including Facebook (14%), mobile apps (7%), Twitter (6%), text alerts from local governments (6%), and Flickr (2%). However, television news (66%) and radio (43%) continued to be the main source for emergency information during an emergency.

The survey also showed that about half of respondents would sign up for emails, text alerts, or applications to receive emergency communication, including for location of food and water (53%), evacuation routes (52%), shelter locations (50%), road closures (50%), location of medical services (50%), and how to keep yourself safe during an emergency (48%). About half of those who use social media also said they would post emergency information on their sites. More than half would send a text message to a responsible agency if someone they knew needed help. Also, during an emergency nearly half would use social media to let them know they are safe. More than two-thirds agree that response agencies should regularly monitor and respond to postings on their web sites. *Amazingly, three out of four would expect help to arrive in an hour.* "The first and best choice for anyone in an emergency situation is to call 9-1-1," said Gail McGovern, American Red Cross president and CEO. "But when phone lines are down or the 9-1-1 system is overwhelmed, we know that people will be persistent in their quest for help and use social media for that purpose" (American Red Cross, 2010, para. 4).

However, the challenge is in its use and application, taking into considerations technical challenges, security concerns, as well as access. However, some of the early work in this area shows promises for Web 2.0, especially on digital mobile devices, to play a constructive role in risk communication. According to Palen (2008), who along with a group of researchers at the University of Colorado who study social media and crisis from a multidisciplinary platform, argued, "Investigation of recent disasters reveals use of online social media as an emergent, significant, and often accurate form of public participation and backchannel communication" (para. 1)

Overview of mobile devices

According to the Digital Watermarking Alliance (2009), the mobile device has transformed over the years from simply a mobile telephone to a completely new, sophisticated device that not only allows a user to communicate by voice with others, but to take photographs and videos, send text messages, and perform powerful computing functions like any regular computer workstation. Users of mobile devices can organize tasks, take notes on site, and send press releases in the form of text messages to the media and other stakeholders. In addition, mobile devices have the capability to manage location based applications and systems (GPS). Use of the devices continues to grow at a very rapid pace. According to the United Nations Foundation report on Technology in Emergency situations, the number of individuals using mobile phones in 2010 has increased to four billion, or 61 out of every 100 people world wide ("New technologies in emergencies and conflicts report," 2010). In the United States alone, over 4 million text messages are exchanged each day, and use is continuing to increase with the evolution of technology and affordability of cell phones (Nichols, June 7, 2010).

Mobile phones offer a number of pathways for effective communication. Traditional one-to-one verbal communication has been augmented with other variations. In one-to-

many communication, a sender can broadcast information directly to a large segment of the population or to a large stakeholder group. The information can be disseminated in various forms, including visual information (photos and videos) and textual information (SMSs and short press releases) ("New technologies in emergencies and conflicts report," 2010). In many-to-many communication, the mobile device is used to connect groups of people using mobile internet capabilities and social networking sites, including Facebook, Twitter, Foursquare, and Gowalla ("New technologies in emergencies and conflicts report," 2010). Foursquare and Gowalla are particularly well suited to the mobile device, because they combine location based features such as geographical information with social networking capabilities. As we will see in a later section, these location based features are particularly useful for risk and crisis professionals in a disaster situation (Chan et al., 2004), but at the same time can be troubling. The implications of such location applications can be both concerning from a potential target perspective, as well as incredibly useful for friends to find out about each other if that location is successfully targeted. The growing use of mobile devices, especially smart phones, has increased recently and is evident in recent reports. According to a recent comScore MobiLens data study with mobile users, it was reported that 26 percent of the participants using smart phones used their mobile devices to get access to maps through applications, while 19 percent accessed this information via a web browser on their phone ("US mobile navigation on the rise," June 25, 2010).

Mobile devices support traditional connectivity while expanding the influence of the individual among larger communities. Mobile devices not only enhance the communication individuals have with their personal contacts, but the technology also forges connections with an entire online virtual community (Palen, 2002). Users not only receive information through the devices, but they can use the technology to create their own content or forward content to others. By doing so, users contribute directly to the media by providing eyewitness perspectives through video, photos, or texted accounts of an event, often bypassing the professional reporters on the scene and providing unfiltered views of what is happening in the world (Gordon, 2007).

Web 2.0 and mobile devices used in disasters

Disaster or crisis situations are "non-routine events that result in a host of non-routine behaviors and new social arrangements. Modern disaster and crisis situations reveal such innovative behavior extending to online settings," (Palen & Vieweg, 2007, p. 117). Both domestically and internationally, mobile devices have become more affordable and integrated into various cultures and societies, changing the ways people communicate with each other in a disaster situation ("Present Humanitarian Information Management," n.d.). CNN International supervising editor Paul Ferguson summarized the impact of mobile technology on disasters as follows: "Victims in a disaster zone can communicate more quickly over mobile networks. Journalists used to base themselves around their satellite dishes and generators to get word out to the world, but today we walk around with pocket satellite phones," (Bulkely, June 18, 2010, ¶4).

According to Gomez, Passerini, and Hare (2006), mobile devices "play a pivotal role in emergency situations by serving three purposes: to be reachable anywhere and at anytime, to obtain information while in an outreach situation; and, to be 'visible' and traceable through a device enabled with GPS positioning capabilities" (p. 439). Jaeger et al. (2007) stated mobile devices are helpful in disaster situations because they are "more readily

available than battery-operated radios, as an increasing number of residents carry them everywhere. Further, they can serve as both input and output devices, facilitating one-to-one, many-to-one, and many-to-many communication" (p. 599).

An analysis of disaster situations occurring over the last decade helps to illustrate the opportunities and challenges of using mobile devices in a crisis. In this section, we review a number of case studies that have focused on the role of new technologies in disaster and crisis situations, including the 9/11/2001 terrorist attacks in New York City and Washington D.C. (Woodhall, 2007; Midkoff & Bostain, 2002) the Southeast Asia Tsunami catastrophe in 2004 (Gordon, 2007), the Virginia Tech shootings of 2007 (Lui, et al., 2008; Vieweg, et al., 2008, Palen, 2008; Palen & Vieweg, 2007), the California wildfires of 2007 (Palen, 2008), the Mumbai terrorist attacks of 2008 ("New technologies in emergencies and conflicts report", 2010) and the Haiti Earthquake of 2010 (Bulkely, June 18, 2010).

The events of 9/11 comprised an influential turning point in the communication of emergency response messages during a disaster (Midkoff & Bostain, 2002). The awareness of crisis managers about the need for more resources and technological advancements increased dramatically. The 2001 communication system in place for emergency management (telephone, radio, and television) could not meet all demands for information (Jaeger, et al., 2007). Another lesson from the 9/11 terrorist attacks was the fact that mobile technology is not the ultimate, exclusive solution to all communication issues in a crisis situation. Instead, mobile technology is best viewed as an emerging medium added to the existing communication structures that raise new issues, challenges, and opportunities for communicating with others (Palen, 2002).

On December 26, 2004, an earthquake hit the Indian Ocean, creating a tsunami that caused extensive amount of damage and devastation in the region. The main areas that were impacted included Indonesia, Malaysia, Sri Lanka, India, and Thailand ("GIS and Emergency Management in Indian Ocean earthquake/tsunami disaster," 2006). The total amount of destruction left more than 250,000 people dead and millions homeless. According to the United Nations Foundations Report on Technology and Emergency Management (2010), the damage to the region reached about $7 billion. Photosharing capabilities and features were used to document events and to provide dramatic visual eyewitness accounts, including a poignant and frightening video of an incoming wave taken from the abandoned camera of one of the victims (Palen et al., 2010). After this traumatic event, the governments of Sri Lanka and other countries in the region established their own Disaster Management Center (DMC) to monitor potential natural disasters and create short messages to be delivered to their respective populations for updates on disasters ("New technologies in emergencies and conflicts report," 2010). This disaster also saw the initiation of the use of mobile technologies to solicit and receive donations for relief efforts ("New technologies in emergencies and conflicts report," 2010).

Mobile devices played key communication roles during the 2005 terrorist attacks in the London subways (Gordon, 2007). Gordon argues that in spite of some challenges, mobile devices are useful tools for coordinating the dissemination of information during this event to affected populations. In this particular case, the initial use of mobile devices was to communicate verbal information in the form of text (SMS), followed by visual information. Mobile devices soon forwarded pictures of the impact of the bombings on

train stations to the London community, the media, and to the rest of the world (Lui, et al., 2008; Palen, et al., 2010).

Shootings occurring on university campuses, including Virginia Tech and Northern Illinois University, provided further insight into the impact of mobile media use on disasters. People were beginning to use mobile media more extensively to communicate with others and give real-time accounts on what was going on during this traumatic event (Vieweg, et al., 2008). Palen and Vieweg (2007) analyzed online communication that was occurring during the Virginia Tech and Northern Illinois University (NIU) shootings, and found that people were using virtual communities (ex. Social networking sites) to interact with others, seek information regarding the crisis, share experiences, form online relationships with others, and build community and awareness of the tragic events. In the aftermath of these shootings, many colleges and universities instituted mobile telephone services used to communicate safety alerts to students, faculty, and staff.

One of the most devastating natural disasters events in recent history was Hurricane Katrina. On August 29, 2005, the Category 5 storm hit the levees of New Orleans, causing extensive flooding and resulting in mass evacuations and billions of damage to the city and community (Shklovski, et al., 2010). Crisis management experts view Hurricane Katrina not only as a natural disaster, but as an information disaster as well (Shklovski, et al., 2010). The entire communications systems of New Orleans and the state of Louisiana were overwhelmed. Messages that did get through targeted government agencies in the vicinity, but the information needs of victims of the disaster were not met (Procopio & Procopio, 2007). Not only were the community residents of New Orleans displaced during the disaster, but also their access to information online and through their mobile devices was disrupted. The existing communications infrastructure was not able to support the increased demand for bandwidth from emergency managers, concerned residents, government officials, and the media. As evidenced by interviews with members of the community, text messages often served as the only source of communication with family, friends, and the online community (Shklovski, et al., 2010).

Mobile phones also played a significant role in the Mumbai Terrorist attacks in 2008, by raising awareness through eyewitness accounts. On November 27, 2008, a series of coordinated terrorist attacks across the city of Mumbai hit several hotels, a café, train station, and a Jewish Center, resulting in the deaths of 195 people ("New technologies in emergencies and conflicts report," 2010). What was unique in this particular case was the fact that the traditional news media were obtaining most of their information from sources on the ground in Mumbai. "Citizen journalists" were reporting events during the 60-hour terrorist ordeal using tweets, Flickr pictures, and videos posted on YouTube from their mobile devices for the world to see ("New technologies in emergencies and conflicts report," 2010).

Most recently, the Haiti earthquake disaster of 2010 provided further insight into the power of communication via mobile devices during an emergency. On January, 12, 2010, a 7.0 magnitude earthquake hit Haiti, leaving millions of people without food, water, and shelter. The country's communications systems were impacted to the point where residents were almost completely isolated from the rest of the world ("Communications saves lives, brings hope after Haiti earthquake," n.d.). Following the earthquake, mobile devices were used to allow people from all over the world to donate to relief efforts using text messages, or SMS ("SMS text donations and the Haiti earthquake," January 12,

2010). This type of fundraising effort, first seen following the 2004 Tsunami disaster in Southeast Asia, increased the awareness of the power of non-profit organizations as a communication channel in a disaster situation ("SMS text donations and the Haiti earthquake," January 12, 2010).

The Haiti earthquake disaster highlighted a more mature use of SMS text messages to communicate first response aid to individuals needing immediate medical attention, or who were trapped under buildings and other fallen structures (Bulkely, June 18, 2010). Mobile phones were used to communicate first aid information and to provide information about where to go for shelter, food, water, and other health assistance (Bulkely, June 18, 2010). Examples of some of the messages that were being sent via these mobile devices included information for medical care ("Hospital Sacre-Coeur in Milot says it has capacity for patients and asks people to make their own way there"), search and rescue ("Though the government says the search and rescue phase is over, SAR teams are still available. If you know someone is trapped call + 870 764 130 944, email haiti.opc@gmail.com or contact MINUSTAH"), and general advisories on other issues of relevance ("Information in a crisis: text messages beamed to earthquake survivors in Haiti, June 18, 2010, ¶1-2). The growing prevalence of mobile phone ownership and use, even in very poor countries like Haiti, makes rescue efforts possible that would be unthinkable ten years ago.

Numerous additional anecdotal examples of using Web 2.0 technologies also exist, whether on static or mobile devices. For example, a downtown explosion in Bozeman, Montana, demonstrated the value of Twitter during a crisis. A media blogger and citizen journalist, upon hearing the explosion downtown but with little information available, created a hashtag (#bozexplod) and very quickly residents started using it; with at one point it was the second most popular trending topic on Twitter. Residents posted eyewitness reports, rumors, unconfirmed facts about casualties, phone numbers to call for help, phone numbers to call to volunteer to help, quotes from the press conference, links to photos, and links to news stories. Residents were responding and answering questions, and squelching rumors and thus self-regulating (Becker, 2009).

As a result of the Virginia Tech shootings, many state and local governments are now creating their own social networking sites. For example, in February 2008 the Virginia Department of Emergency Management launched a YouTube channel to reach state residents with emergency-related information and public service announcements. The site was developed in partnership with Google (Virginia Department of Emergency Management, 2007).

Thelwall and Stuart (2007) examined three crises (London attacks, Hurricane Katrina, Pakistan-Kashmir earthquake) and demonstrated that bloggers used Web 2.0 resources such as Wikinews, Wikipedia and Flickr picture sharing site for information, though these still played a minor role in comparison to mass media. All the newest technologies mentioned used were Web 2.0. "The precise mix of technologies seems to depend on the nature of the crisis" (p. 206).

Another example is the Department of Homeland Security (DHS) Virtual USA, an innovative information-sharing initiative—developed in collaboration with the emergency response community and state and local governments across the nation—that helps federal, state, local and tribal first responders communicate during emergencies. "Our

first responders need interoperable tools to make accurate and timely decisions during emergencies," said Secretary Napolitano. "Virtual USA makes it possible for new and existing technologies to work together seamlessly during disaster response and recovery and gives the public an opportunity to contribute information in real-time to support the efforts of police officers, firefighters and other emergency management officials." The announcement came as part of the White House Open Government Initiative. Related to this project is that it involves the public. Virtual USA allows Americans in their own communities to contribute information—in real-time—to support the efforts of police, fire and emergency management officials during disasters and recovery efforts (Homeland Security, 2009).

Last, the American Red Cross has started using Twitter to exchange real-time data about local disasters with those affected, and the U. S. Geological Survey operates a site called *Did You Feel It?* where people can report local earthquake activity. These case studies show a linear progression in the use of mobile technologies by both crisis managers and victims to obtain and share information. While these events have helped transform how disaster responders use mobile technology, progress towards maximizing the benefits of the technology has been somewhat slower than expected (Woodhall, 2007). Through further analysis of the opportunities and challenges provided by the use of mobile technologies in a disaster, proactive and well-designed best practices can be identified.

Opportunities provided by mobile devices in disaster situations

Mobile devices provide many opportunities for more effective communication in disaster situations. With their immediacy, nearly universal prevalence, and relative immunity from the failure of other types of infrastructure in an emergency, mobile technologies allow rapid and proactive disaster relief responses. Professionals operating in disasters have greatly improved remote access to information, along with the ability to communicate with their home base or others onsite (Chan, et al., 2004).

People have been very adaptive in using new forms of technologies, including mobile devices (Veinott, et al. 2009), and we can assume that user competencies will keep pace with the abilities offered by the technology. New mobile forms of technology "provide a broad, multi-faceted and interactive connection with the outside world. In fact, the very promise of being informed and connected seems to motivate high rates of communication technology adoption and appropriation in times of disaster," (Shklovoski, et al., 2010, p. 6).

The combination of mobile communication devices and access to the online community through the Internet allows emergency managers and risk communication professionals a gateway to handle a disaster more effectively (Jaeger, et al., 2007). Emergency center operators, police, military, and medical personnel have learned to actively use new forms of technology to communicate in a disaster or crisis situation (Shklovski, Palen, & Sutton, 2008). The ability of a single responder to disseminate information to large groups of people reduces the workload on emergency staff. Compare the information sent in text message form to Haiti mobile devices to previous methods, such as laboriously going door-to-door.

Mobile communication channels also serve as a valuable resource for the community, providing information, contributing to a sense of normal life, and supplying ways to pass

the time until the situation returns to normal (Shklovski et al., 2010). Prior to the advent of mobile devices, people experienced uncertainty and anxiety in addition to the challenges resulting from a particular disaster. Mobile devices help to reduce fear and anxiety by allowing people the means to obtain the information they need (Shklovski et al., 2010). Mobile devices have empowered people with the opportunity to establish connections with others during a disaster situation, while obtaining access to the information and knowledge they need in order to act themselves ("Information in a crisis: text messages beamed to earthquake survivors in Haiti," June 18, 2010). Stakeholders can collaborate and assist each other, enhancing their personal sense of control, and further reducing the load on official emergency responders.

The use of mobile technology has the potential to facilitate reciprocal communication between responders and large groups of people impacted by a disaster or crisis. Jaeger, et al. (2007) point out that the "combination of mobile telecommunications devices and the Internet, however, has the potential to provide higher capacity and more effective service, as well as create interactive communication mechanisms that can facilitate just-in-time communication and collaboration among large numbers of residents and responders" (p. 593).

Web 2.0 Media has provided not only an increased access to emergency response information, but also increased the ability of risk bearers to disseminate such information. Social media aids in people weighing conflicts of interest in risk and crisis communication, build networks among affinity groups related to a crisis, ability to witness debates, and ability to participate in chat rooms and other social media outlets. One example of using social media to relay crisis information is the use of MySpace with the Department of Homeland Security to spread news on hurricanes through users of the online network by the use of a software program that automatically feeds hurricane information from federal disaster agencies to MySpace users.

Another example is Twitter adoption and use during emergency events. A study conducted by Hughes and Palen (2009) suggested that Twitter messages sent during mass crisis events contain even more information broadcasting and brokerage than typical microblogs messages, and that Twitter is evolving to a more information-sharing purpose. Early evidence from their research also showed that Twitter users who joined during an emergency for information-sharing purposes are more likely to become long-term adopters of the technology, which could be beneficial to long-term risk communication campaigns, such as one related to IEDs utilized in the United States. Krimsky (2007) summed up well the quandary at hand with new media technologies. "At the same time that the availability and variety of information has expanded, the boundary between good quality and poor quality information has become blurred" (2007, p. 157).

Challenges raised by the use of mobile devices in disasters

In spite of the many advantages provided by mobile devices in an emergency, the history of responses to disasters in the era of new technologies demonstrates that this is a rapidly changing landscape requiring constant analysis and proactive planning. Recognizing the challenges to planners, responders, and victims posed by the use of mobile media during a disaster or crisis will allow crisis managers to anticipate problems and maximize performance.

Although personal use of mobile media is quite common, leading to relatively high levels of competence, emergency planners should not assume that all personnel have the knowledge and training to use the technology appropriately during a disaster situation. According to a Communications Capabilities survey, the majority of emergency management respondents (73 percent) said that their best means of communication with one other is one-to-one (Emergency Management, 2010). This implies that training might be needed for respondents using one-to-many or many-to-many features of mobile technology. Otherwise, these beneficial features could be mis-used or under-used. All personnel on the disaster scene (ex. Team leaders, dispatchers, etc) should be equally skilled in the use of technology, making the users of the devices interchangeable in the field (Yuan & Detlor, 2005). Training should also minimize the likelihood that unskilled users will consume the available bandwidth, which might be stretched very thin during an emergency (Veinott, et al., 2009). Although responders cannot control the bandwidth used by victims, informative messages suggesting ways victims should use their technology might be helpful.

Organizations need to provide training as well. Cloudman and Hallahan (2006) analyzed public relations practitioners training in crisis communication and found a lack of emphasis on overall training. Most crisis and risk communication training focused on briefings and spokesperson training, but did not take advantage of training with other techniques or technologies. The WIO Council (2009) argued for an increase in training since "users are almost always the weakest link in an information system, and may inadvertently divulge sensitive information through a social network" (p. 14). The United States Air Force New Media Guide provides some guidelines, but little guidelines and policies exist in relationship to crisis situations, which provides a stressed atmosphere that can often lead to increased pressure to divulge sensitive information.

Inadequate equipment will hinder efforts to use mobile technologies during an emergency. The Communications Capabilities survey found that 58 percent of emergency managers did not have cameras on their mobile devices, and fewer than 30 percent of the emergency managers surveyed could see the location of others on their dispatch screen (Emergency Management, 2010). A sound infrastructure for mobile devices supports all new features, allowing for the exchange of photos, videos, and data among responders on the disaster scene, as well as with others in relevant organizations (Woodhall, 2007). The information that is shared on these devices should be duplicated in both online and offline platforms. A critical aspect of a sound mobile infrastructure is the need to make security a top priority (Swartz, 2003).

Managing multiple communication channels, deciding what information should be disseminated to which audiences, and preparing the best strategies for rapidly changing emergency situations requires careful and extensive planning. Unfortunately, emergency management professionals appear to be lagging behind in the implementation of mobile media in their communication plans (Nichols, June 7, 2010). Although mobile technologies are improving rapidly and access to mobile devices is common, risk communication professionals and emergency managers need to remember that not everyone in the population will have access to one of these devices. Alternate means for reaching these individuals must be included in any crisis plan.

Among the challenges facing victims of a disaster is the risk of information overload, due to extensive coverage available in both traditional and mobile media (Cordner &

Scareborough, 2010). Crisis managers could benefit from taking the "need to know" approach, in which information designed to reduce victim's levels of uncertainty becomes a priority over general information that can be shared with others online or in person (Cordner & Scareborough, 2010). This aspect of mobile media is especially important to terrorist incidents, and should be an important part of security planning.

Mobile communication not only allows agencies to disseminate messages about a disaster, but it also allows stakeholders to communicate with each other while bypassing the information gatekeepers in agencies and traditional media. Today's stakeholder groups expect to be informed rather than controlled or commanded. While this aspect of mobile media is more compatible with democracies such as the United States than with more repressive governments, like Iran and China, it does raise significant challenges. Individuals supplying official messages must be completely transparent, operating with a 24/7 mentality and recognizing their role in the international digital business community. The reduced official control of information due to mobile media raises the likelihood that stakeholders might receive false information regarding the situation (Vieweg, et al., 2008). Digital information sent via mobile devices can spread virally in a matter of seconds, and receiving rumors or false information during a disaster can be catastrophic for all of those involved. Responders should also be aware that any "mistakes" or inappropriate behaviors will be communicated widely and instantaneously to the world audience. Also, news stories can spread incredibly fast and negative online comments can fan the flames, causing erroneous reputational damage (Aherton, 2009).

At the end of the day it's about balancing Web 2.0 and information control to leverage publicly disseminated information. Used thoughtfully, mobile devices can improve the communication efforts in a disaster situation greatly (Starbird et al., 2010). However, even with all of the technological advances and resources in the world, if people do not work together and help each other in these disaster situations, then it will be all for naught (Palen, et al., 2010).

Crisis communication and web 2.0: How technology is used as opposed to how much

A majority of research in crisis communication and Web 2.0 media focus on metrics, measuring such items as number of Twitter followers, hits on social media sites, number of friends following your organization's Facebook page. While those are important metrics, especially in relationship to marketing and reputation management, it's more important to understand how technology is being used, who are the influencers on social media, who is sharing what with whom, accuracy of information, and are there disadvantaged populations that are left out of risk communication campaigns.

Communities of risk can be considered a front line in the marketplace of attitudes, knowledge and perceptions over the distribution of resources. In this social arena, society is the collective enactment of that discussion via narratives (in harmony, in conflict, that build conflict) as shared meaning made public through voices in unified competition (Heath, 1994). The narrative used with Web 2.0 technologies may be even more important. For example, Twitter has often been criticized because of the limited value of narratives in 140 characters or less. The history and evolution of literature is all about writers shaping their work to exploit new technologies, and Twitter literature (Twitterature) is no different. For example, Poniewozik (2010, June 14) argued in his essay on the British Petroleum (BP) Deepwater Horizon oil-rig explosion how

@BPGlobalPR, an anonymous, satirical Twitter account, had more than 10 times as many followers within one week as the official BP site (@BP_America).

Web 2.0 mandates more transparency

Information transparency is the degree to which organizational actions and decisions are ascertainable and comprehensible by interested parties (Grunig & Hunt, 1984). Transparency is not just about information; it is a process whereby active participation in acquiring, distributing and creating knowledge (Grunig & Huang, 2000) with stakeholders is essential to effective relationships. According to Hon and Grunig (1999), transparency is another way of thinking about disclosure and it is an important part of relationship maintenance strategy. "[P]ublics want to understand the organizations that have consequences on their lives as well as the economy and health of their community. . . Failure to disclose breeds suspicion that an organization has something to hide" (Hon, 2006, p. 61). Organizations that adopt as part of its culture the concept of transparency improves a company's reputation and helps restore trust (Bowen, 2004). According to Reynolds, Galdo & Solker (2002) in their review of risk communication literature, empathy, caring, competence, commitment and accountability contribute to trust. A fundamental characteristic of Web 2.0 is transparency, but when it comes to risk communication efforts related to IED attacks in the United States, complete transparency might not be the best option and often can create more risk to citizens.

> "As the Internet grew, access to information by communities, public interest groups and ordinary citizens has been unprecedented up to this point in human history. Expertise on risk became secondary to the significance of trust and validity in the source of information. Public skepticism is fed and nurtured by new open forms of Internet communication. All risk websites are potentially equal in Cyberspace, constrained only by the skill of the web designer. It levels the playing field to a public that does not understand the hierarchy of expertise (meritocracy)" (Krimsky, 2007, p. 160).

Determine social media engagement as part of risk management policies and approaches

Every risk/crisis communication plan should have a section for communicating with stakeholders and working with the media. Social media can be used to both communicate directly with stakeholders and the media at the same time. More importantly, social media provides a built-in channel for stakeholders to communicate directly with the organization. Incorporating social media into the plan ensures the tools will be analyzed and tested before the crisis and requires continual updating of the plan as social media evolves.

At the same time there is a tremendous amount of research and planning that needs to be done to seamlessly integrate Web 2.0 risk communication procedures into county, local, city, state, tribal and federal emergency plans, and in particular crisis communication plans, as well as coordinating warnings and public information through the activation of the State's public communications strategy and the establishment of a JIC. Early efforts in policy and technical planning for Web2.0 has mostly focused on public information and awareness use of social media for dissemination and dialogue, such as the US Air Force New Media Guide, and not necessarily for use during a crisis. While there is

overlap, risk and crisis events provide unique situations that go beyond daily public information and awareness policies. In fact, social media and other variations of the term are not part of the National Response Framework. Many major areas of government, including the FTC, SEC, FDA and DOD have been meeting to examine, research and develop policies and guidelines for the use of social media, though they are mostly in their infancy stages and rarely related to risk communication. For example, the DOD Directive-Type Memorandum 09-026 – Responsible and Effective Use of Internet-based Capabilities addresses social networking services, and that "Internet-based capabilities are integral to operations across the Department of Defense" (2010, para. 1). Within these plans is the need to incorporate digital hand-held communication devices into traditional risk warning systems, but there is little evidence of this so far. FEMA is beginning to examine the use of social media as part of the Integrated Public Alert and Warning System (IPAWS).

Individuals may have information that is crucial to the mitigation of the crisis, but if they do not trust the organization or even know where to find it, that information will likely not be shared. In the midst of a crisis is not the time to suddenly try a hand at social media. To build partnerships and build trust, the discussion with publics should already be taking place. As Stephens and Malone (2009) identified in their research, if the organization wants to ensure that stakeholders go to their web site and new media technologies concerning new information, the organization must use the web prior to a crisis.

Incorporate social media tools in internal communication logistics and environmental scanning

Using social media like wikis on day-to-day projects can streamline communication and increase efficiency. Involving the crisis management team in the development of the crisis plan and document management site through social media, rather than handing the task off to a single individual, increases the potential for interactivity in the crisis response. In addition, tracking issues through social media and providing the crisis management team with the reports can increase the potential that a crisis will be addressed sooner and demonstrate to the team why social media needs to be embraced in the crisis response. At the very least environmental scanning of Web 2.0 media is critically important as indicated by the US intelligence community being very concerned that terrorists might use microblogging sites such as Twitter and other social media to coordinate attacks (Musil, 2008).

Recognize the traditional media is already using social media

The crisis will likely be discussed through social media. Traditional media will be part of that discussion. If the organization is not engaged, the media will find other sources through social media to comment on the crisis. Thus, when it comes to being accessible to the media, not engaging in social media can have the same effect as not returning a reporter's call. Utilization of social media in risk communication will also mean changing our definition of media to also include backpack journalists, bloggers, and key online influencers.

Organizations often promise to follow-up with the media and public as soon as they have new information, and yet, they wait to release that information until a press release can be

drafted, refined, and sent out or posted passively to the organization's website. Or, in order to convey the emotional concern required, wait until the next scheduled press conference. Using social media for updates in the crisis response and recovery allows the organization to humanize the response and continue to be a reliable source, without requiring all the exact details and time needed to fill a press release or hold another press conference.

Updates not only refer to media but also the use of digital hand-held devices for coordinating ad hoc search and rescue efforts and volunteer coordination among citizens. There has been anecdotal evidence of this already occurring during the 2007 southern California wildfires, shooting at Virginia Tech University and other universities, and the 2008 Mumbai bombings. Most of the use of Web 2.0 for such action has been organic and naturally occurring among risk bearers and near neighbors of such events, but the potential is there for a more organized infrastructure for the use of hand-held digital technology to be in place for informal and formal communication.

Web 2.0 and underserved, children, and hard-to-reach populations

One of the pressing issues with any advancement, including Web 2.0 and mobile communication technologies, is the challenge of integrating it with underserved populations, children, and in general hard-to-reach, thus hard-to-adapt, populations. New communication technology inequities plague vulnerable populations by age, income, education, race, as well as substantial differences between rural and urban living (National Telecommunications and Information Administration, 2010), which can compromise how quickly and how much risk information people receive during and IED attack. There is a need to identify the most effective channels (focus on mobile communication technology) and messages to engage in dialogue to adopt risk-reducing behaviors, with consideration of the feasibility and ethicality of using social media. Social media offer a variety of tools that may quickly reach broad audiences with risk information yet at the same time run the risk of broadening knowledge gaps and disparities among vulnerable populations. As social media are increasingly incorporated into the communication mix in risk and crisis campaigns, communication practitioners are charged with how to avail populations who may not have equal Internet access to the potential benefits of social media.

Regarding children, the National Commission on Children and Disasters *2010 Report to the President and Congress* found that the nation is unprepared to care for children in a disaster, including communication with children. Their report calls for funding to improve disaster planning for schools, child care, juvenile access and child welfare agencies, as well as creating a national evacuee tracking system to reunite children with families. "In light of the ongoing challenges, the Commission recommends that the Executive Branch and Congress invest greater resources to assist health care systems in regionalization, compliance with the national emergency care guidelines for children, and development of pediatric medical surge capacity for disasters" (p. 57). Social media, and mobile communication technologies, can play a role in improving this area of our national defense communication system. For example, families are going to use social media and cell phones to communicate, try to keep track of each other, and other everyday communication occurrences that are enhanced during a risk or crisis event. The question is what role DHS and other government agencies will have in supporting this information network. Even the national report recommends creating a system to "remain

in communication with caseworkers and other essential child welfare personnel who are displaced because of a disaster" (p. 104), which would at a minimum required mobile communication technology.

Web 2.0 could help overcome interoperability issues

The total planned US federal government spending on information technology in 2011 is $79.4 billion, a 1.2% increase from the 2010 Budget level of $78.4 billion. However, much of this technology is situated on thousands of different platforms, many of which don't integrate. Public Web 2.0 Media doesn't have this problem. However, it is questionable as to whether social media sites want to be responsible for fundamental communication during emergencies, and whether they can or will build the infrastructure required to operate during terrorist attacks, both from a capacity standpoint and a redundancy standpoint.

Another example of interoperability issues that has a direct issue related to mobile Web 2.0 technology for risk and crisis communication is that most emergency calls to 911 centers are coming from cell phones, which can be a problem for dispatchers who don't get the initial location information as quickly as opposed to landlines that immediately give a call-back number and address. Wireless phones give a call-back number and an approximate location, within a federal standard of 300 to 800 feet. There are new technologies that are addressing this issue. Most U.S. carriers have integrated technology to use global positioning system satellites or their own towers to help triangulate a cell phone's location. The Nation's current 9-1-1 system is designed around telephone technology and cannot handle the text, data, images and video that is increasingly common in personal communications and critical to future transportation safety and mobility advances. The Next Generation 9-1-1 (NG9-1-1) Initiative has established the foundation for public emergency communications services in a wireless mobile society. The new system will enable 9-1-1 calls from any networked device, and provide quicker delivery and more accurate information to responders and the public alike. Delivery will incorporate better and more useful forms of information: real-time text, images, video, and other data (U.S. Department of Transportation, n.d.).

INTERVIEW FEEDBACK

Seven general themes, plus one eclectic mix of issues, became evident during the interviews. These include: (1) different perspectives as to what social media is; (2) an eclectic range of policies and guidelines within the use of social media within crisis communication or general communication plans; (3) that social media should and will play an increasingly important role in risk and crisis communication but at the present time there is limited use, mostly on an information push role; (4) need for an increase in training and education for using social media for risk and crisis communication; (5) social media changes the focus of communication from the organization to the stakeholders/risk bearers during a crisis with numerous benefits, such as emotional support, identifying location of and health/safety status of friends and family during a disaster, as well as updates on property and return to "normal" activities; (6) mobile technology is considered the most probable next trend in risk and crisis communication; (7) social media's most beneficial aspect may be the opportunity to listen and conduct internal and external environmental scanning prior to, during and after a risk or crisis event; and (8) some additional general opportunities and constraints.

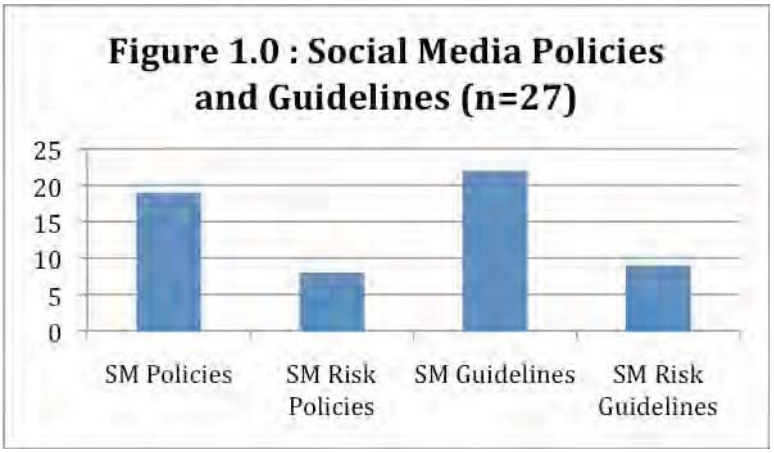
Social Media Confusion

There are inconsistencies to how practitioners, researchers, management and public information officers view social media. While not critically important, these inconsistencies demonstrate the ever-changing nature of new media technology, the range of experience and expertise in the use and management of social media, as well as to the disagreement within the academy as to what is social media. Lack of a consistent definition presents real-world challenges in developing, integrating, accessing resources to increase utilization, and measurement. The biggest difference was whether web sites, black sites, text messaging and instant messaging should be considered social media. In this regard, the differences relate to whether more "traditional" new media such as web sites and texting, which relies on information push and back and forth asymmetric communication, should be included.

Eclectic Range of Policies and Guidelines

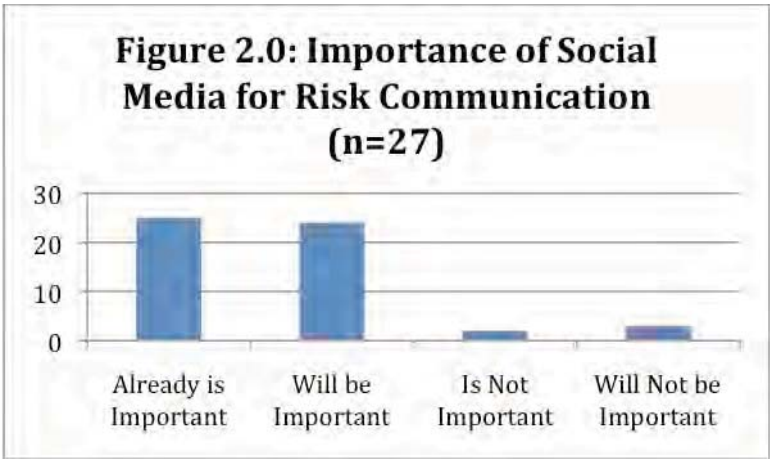
There is an eclectic range of policies and guidelines and within those ranges wild variations among the quality, measurement of, and expectations of the use of social media during a risk or crisis communication event. While keeping in mind that the interviewees are a purposeful sample working within organizations that are more likely to be early adapters of new technology, many of those interviewed had social media communication policies within their organization, less had policies for a crisis or risk event, while almost all the organizations had simplistic guidelines regarding the technical and communication use of social media within their public information/corporate communication offices (see Figure 1.0).

In addition there are numerous other concerns that were discussed regarding policies and guidelines. Issues such as clearance of policies across large organizations and government agencies, inconsistent policies, and lag time to create and approve policies. A recent roundtable discussion on the use of social media during disasters posed this question: "Should there be a common or central system that the public goes to for assistance? How do you get them to do that? Short answer: Yes. But there are many questions around the 'how.' Who established protocols? Who runs? Who funds? What about privacy issues? How to validate legitimate needs versus 'cranks?" (American Red Cross, 2010, "Anna's Roundtable Page).

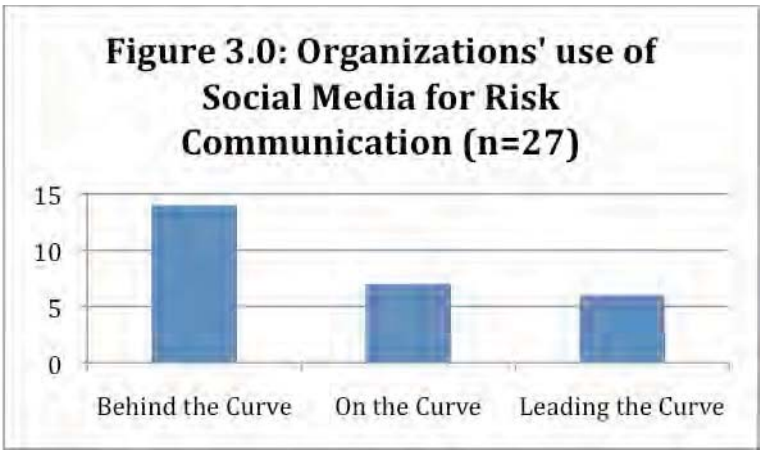


Key Role for Social Media during a Crisis Event

There is overwhelming consensus that social media is already to a limited degree, should be, and will be an important part of ongoing risk campaigns, crisis communication plans, and engaged crisis and disaster communication (see Figure 2.0). According to one federal agency public information officer, *"There is no question that social media is playing an increasingly important role in communicating with our stakeholders, they want it, we want to use it, and I can see its [social media] role increasing dramatically during the next 3-5 years."* There is ample anecdotal evidence to this. In the summer 2010 the Federal Emergency Management Agency (FEMA) announced a new widget entitled *Ready*, one of 11 available from the FEMA widget web site, as part of its efforts to use social media for emergency readiness and response. The widgets, small portable graphic interfaces offering Web links to key information, are for hurricanes, tornadoes, floods and even information relating to community volunteers. These are in addition to their efforts on Facebook, Twitter, RSS feeds, YouTube, and Google Books. According to FEMA's press release, FEMA's social media ventures function as supplemental outreach, and as appropriate channels for unofficial input" (Lipowicz, 2010, para. 6).



But what roles will that play and how does that come about? More than half of the people interviewed felt they were behind the curve in using social media, though these individuals were identified for the study as working for some of the more advance users or researchers in the use of social media during a risk or crisis event (see Figure 3.0). For most of the individuals interviewed, the use of social media within general communications and/or risk/crisis communication plans was the result of one person, one "techie" who strongly advocated the use of social media. As one senior industry corporate affairs officer stated, *"We are just getting into social media. At the beginning some of the staff had to push and shove us in that direction, but we are there. I see the obvious benefits but I just need some proof."*

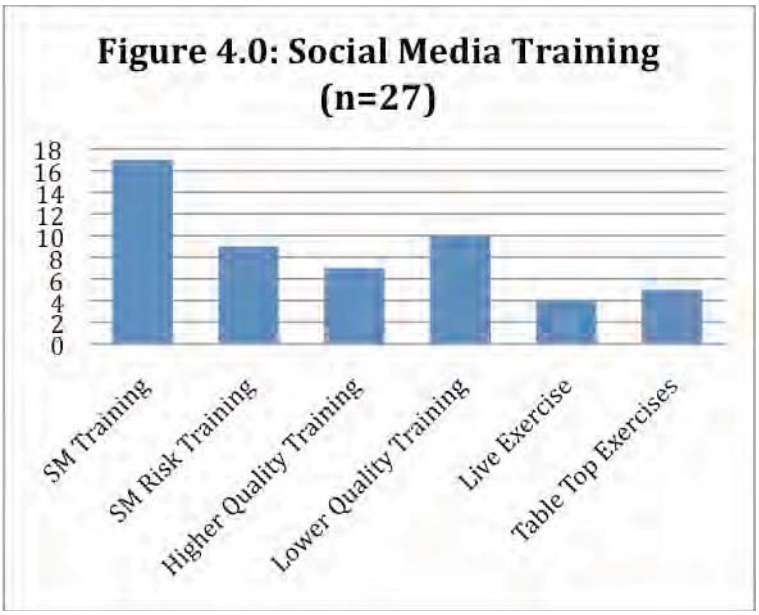


Institutional and Community Infrastructural Barriers of New Media Technology

The environmental justice literature clearly demonstrates the differential impact of minority and socioeconomic challenged communities related to health, safety and environmental issues, including the impact from disasters. According to Moore (2010), "the lack of a fully developed literature on the vulnerability of minority communities and institutions suggests that their critical role in the provisions of services to minority individuals is not well enough understood" (p. 5). Despite the uncertainty in this area, one thing from discussions is clear that new communication technology inequities plague vulnerable populations that can compromise how quickly and how much risk information they receive during an IED attack. Common points included the need to examine message strategies to engage in dialogue to adopt risk-reducing behaviors, with consideration of the feasibility and ethicality of using social media with vulnerable populations who may or may not have the technical resources, access nor education to use social media during a risk or crisis event.

Increased Education and Training

Overall there was a wide variety of the quality of the training, how often that training occurred, and no training. In addition, the use of tabletop or live exercises to practice social media during a crisis or risk event varied as well (see Figure 4.0). One public affairs officer described the high-end of social media and risk communication training: *"We are excited about how we are starting to use social media, whether in our daily communications or in our crisis response plans, and we train regularly – table top, full-scale response exercises – it's a great start, but I wish we could push how we are using and training with Web 2.0 and especially mobile devices."*



Leverage User-Generated Communication

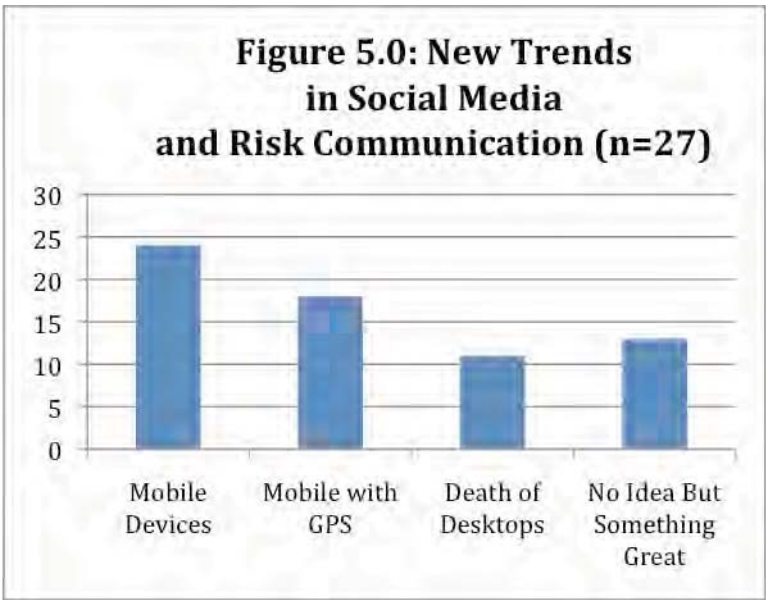
One of the most heavily talked about areas during the areas, leveraging user-generated communication is exactly what social media, including the use of mobile devices, is all about.
Leveraging stakeholders-generated communication to counter IED takes into consideration the fundamental role of social media, which combines "a wide range of online, word-of-mouth forums including blogs, company sponsored discussion boards and chat rooms, consumer-to-consumer e-mail, consumer product or service ratings websites and forums, Internet discussion boards and forums, microblogs" (Mangold & Faulds, 2009, p. 358). Lariscy, Avery, Sweetser, and Howes (2009) define social media in this leveraging perspective as "online practices that utilize technology and enable people to share content, opinions, experiences, insights, and media themselves" (p. 1). Leveraging communication to counter IED is about participation, openness, dialogue, community, and connectiveness – responsibility for finding, creating and disseminating information falling upon all parties involved and especially risk bearers in the community.

One interview example, from a nongovernmental organization's emergency management officer, summed up this approach. "Responding to disasters is so heavily dependent on good information communicated quickly to all the people who need it, whether it is to make decisions about yourself or others. Why not take advantage of social media during these times, using all the people in the community to get the word out… We are always lacking resources, including personnel. Social media adds thousands of people to a communication matrix during a disaster." In many ways, social media is revolutionary in its effects on how organizations and individuals communicate with each other (Solis, 2008). According to Solis, social media represent "an entirely new way to reach" (p. 5) people and connect with them directly. It adds an outbound channel that complements inbound communication, placing organizations and individuals on a level playing field to discuss things as peers. Social media in general is "much more than user-generated content. It's driven by people in the communities where they communicate and congregate. They create, share, and discover new content without our help right. They're

creating vibrant and rich cultures across online networks and using the social tools that we learn about each and every day to stay connected" (Solis, 2008, p. 5).

Digital Mobile Devices the Next Trend

One area of consensus is the idea of what would be the new trend in risk and crisis communication related to social media. An overwhelming majority saw the use of mobile digital devices as the next significant trend in social media, and specifically risk and crisis communication, followed by mobile devices that have GPS installed. The benefits of this relates to knowing where people are during an emergency, either from the risk generating/managing organization's perspective or for risk bearers to identify location of family, friends, the danger, and emergency services (see Figure 5.0). According to one researcher interviewed, *"We need to demonstrate, beyond anecdotal evidence, the value of using mobile devices during a disaster. The technology is there, abundant, and people are using their mobile devices not so much as a phone but a portable social computer – we need to examine the consequences of this in relation to better managing risk."*



Internal and External Environmental Scanning

Good risk communication practices include monitoring and planning for eventual crises. Social media can provide powerful tools for identifying crises at a very early stage, where intervention is likely to be more effective. For example, a relief agency could establish a set of Google alerts, search specifically for their organization or high profile incidents associated with their mission (e.g., tsunami) on social media search engines like Samepoint, or conduct focused searches of Twitter on a regular schedule to monitor "talk" about the organization and its services. In a recent example of how emerging crises might be detected early using social media, Google maintains a large monitor in its corporate lobby, refreshing regularly to show the most popular searches. One of the first hints that Mexico was entering its swine flu crisis, long before any news stories broke in the traditional media, was a flurry of searches from that country on "swine flu." Establishing best practices for these monitoring activities should be a priority for public relations researchers. According to one interview with an industry corporate communications officer, *"The best thing about social media, above all else, is the ability*

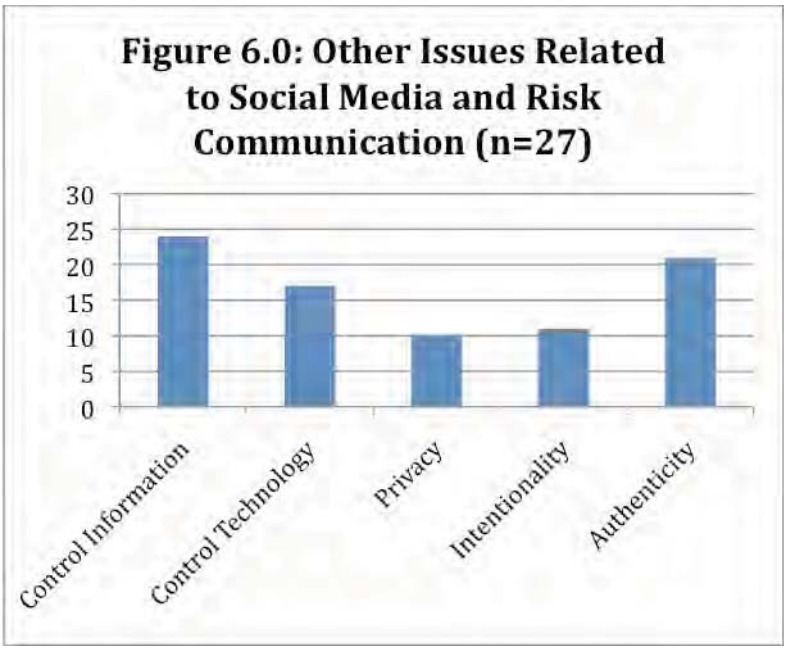
to listen to our customers, especially when there is a problem with our products or services, and especially when there is a product recall… And the amazing thing it's real-time research and incredibly cost-effective."

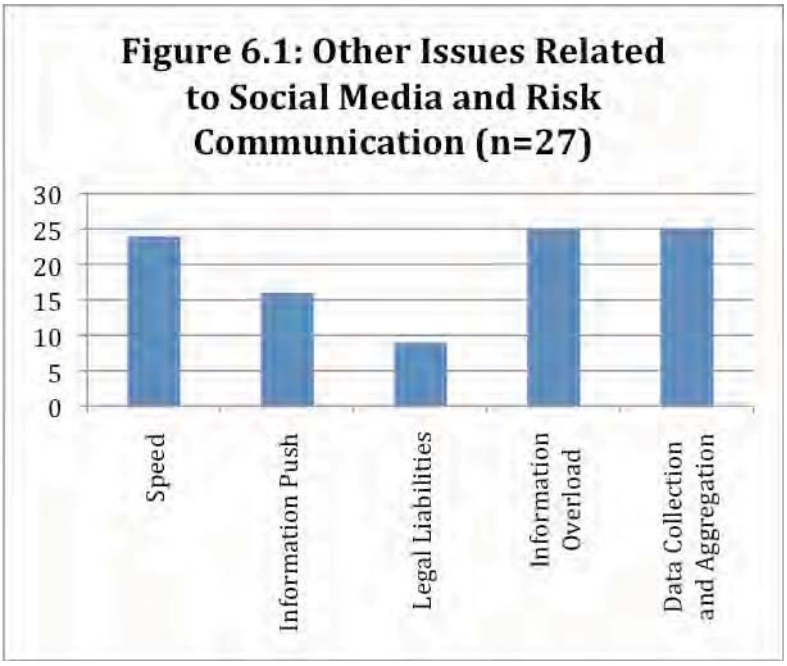
General Other Issues

There are numerous other issues that are right for discussion during the conference that were a part of numerous interviews and demonstrated narrative themes that deserve attention (see Figures 6.0 and 6.1). Issues such as who is in control of the information and technology are very important discussion points, which tie into policy and guideline issues. As one interviewee suggested, *"The challenge for us in social media is about letting go – or convincing others to let go – of control, like we ever had it in the first place."* Similarly concerns were expressed about who control the technology, and along with that data collection and aggregation.

Several of these issues relate more to residents' who would bear the risks and related issues, such as privacy and information overload. In a similar manner, there was plenty of concerns regarding issues such as intentionality (*"what happens when someone sends out wrong information that leads to someone's death, especially if it's the enemy"*), authenticity (*"one of the big challenges is relying on others not trained in emergency management to share information appropriately, accurately and with the right intentions"*), and legal liabilities (*"what's an organization's liability if they post information for the world to use, but it's spread by the online community incorrectly… are they responsible, am I responsible, is my company responsible"*).

Finally, two of the more information issues relate to information and speed. A majority of those interviewed talked enthusiastically about the advantages of social media, but at the same time had reservations that most organizations that use social media use it in a traditional information-push style of communication. According to one nongovernmental communications officer, *"We still mostly just push out communication, even when there is a problem. There are so many community dialogue advantages but it's hard to take advantage of that well."* Speed is another area of rigorous conversation. Speed is separated into several issues, including the speed to get authorization to use social media (*"I often have to follow the old adage, 'it's easier to ask for forgiveness than permission' when it comes to using social media on the job"*) and the speed with which information is shared among the online community and its related advantages and disadvantages (*"we can instantly get information out that took hours just a few years ago, but at the same time, man that is scary, that same speed works with good and bad information"*).





IMPLICATIONS FOR RISK COMMUNICATION PRACTICES

The primary issue facing emergency managers is a gap between expectations for the performance of new mobile technologies in a disaster, and the needs and expectations of those impacted by the disaster. There are certainly challenges that need to be taken into consideration based on previous disasters and acts of terrorism.

Taking full advantage of the opportunities provided by mobile devices while avoiding the potential pitfalls associated with these technologies requires careful, thoughtful analysis long before any disaster emerges. Emergency managers should monitor potential issues while establishing crises communication plans that reside on both static and mobile

devices. As issues are identified, research conducted on potential audiences should identify their trusted sources of information. Emergency managers and responders need to be proactive instead of reactive to take full advantage of the immediacy provided by mobile media.

The disaster communications and risk communications action plan should include policies specific to the use of mobile devices in a disaster situation. A thorough risk assessment needs to be implemented to determine the challenges and opportunities of using mobile devices in specific disaster situations and the appropriate action steps that need to be taken to address any identified risks. All employees should have thorough education on these devices. It is crucial that everyone involved understands the nature of these devices, how they are used, and expected behaviors by individuals using these devices in a disaster situation. Policies and measures for securing these devices should be in place. Potential issues arising in this area could be the loss of the device or a security breach on the communication channel by a third party. Security measures, new cyber attack protocols, and best practices in dealing with cyber terrorism must be addressed in relation to these new digital hand-held devices.

Information supplied by emergency managers and first responders should be consistent, providing individuals with the information that they need to reduce uncertainty and receive necessary help without producing overload. Emergency managers need to build a mobile communications and online community where stakeholders can engage with others and obtain contact information for media outlets and other crisis communication representatives. Empowering stakeholders in a crisis situation can work to everyone's advantage.

The CIO Council, in their September 2009 report entitled *Guidelines for Secure Use of Social Media by Federal Departments and Agencies* concisely summarized the decision to use Web 2.0 media based on costs and benefits (risk based on a strong business case) as opposed to making decisions on a technology-based decision. For example, the decision to authorize access to social media websites is a risk-based business decision with inputs from all involved parties (Walls, 2007). At the end of the day, "federal government information systems are targeted by persistent, pervasive, aggressive threats" (WIO Council, 2009, p. 6), and according to Walls (2007), risk to the individual, department or agency, and federal infrastructure needs to be considered. Any crisis communication systems that incorporate Web 2.0 media must fit into current and future government-wide policy for social media. In September 2009, the WIO Council put out a call for such a policy.

Beyond security, there are numerous other technical issues with using social media for risk and crisis communication. For example, the National Response Framework (2008) emphasizes the need for monitoring emergency communications carefully. "Throughout an emergency, critical information and direction will be released to the public via various media. By carefully following the directions provided, residents can reduce their risk of injury, keep emergency routes open to response personnel, and reduce demands on landline and cellular communication" (p. 17). While this is true, the proliferation of cellular phone technology, especially data transmission via cell phones and other portable devices, puts an added stress on that system. While we need to keep wireless systems operational for emergency services, risk communicators need to use wireless systems to

quickly share information with community residents, media, key stakeholders, and emergency responders.

There are other concerns with the use of hand-held digital devices as a fundamental communication infrastructure in risk and crisis situations. Traynor's (2008) research about the technical capabilities of emergency text messages as part of emergency alert systems (EAS) brings up issues with adopting technology without thinking about such risks. As university and other organizations have subscribed to more and more of these text messaging EAS systems, there are problems with technology, speed of information, systems overloads and blocking the delivery of critical information between emergency responders or the public to 911 services. "Such 'always on' connectivity may one day create new opportunities for the dissemination of critical information during an emergency. However, as demonstrated in this study, modern cellular networks are simply not capable of providing such a service, whether through voice calls or text messages" (p. 26).

Mobile devices implemented in emergency communications plans will allow a more even distribution and coordinated effort that will be beneficial for all parties involved in the disaster situation. Emergency managers can be actively communicating via text message or post other information (ex. videos, photos, etc.) to establish credibility and their authority as a primary source of information in the disaster situation for impacted communities. Connecting online and using these mobile devices effectively will establish a stronger virtual community that will be more informed and engaged in the disaster recovery and implementation process (Sutton, 2010). Technology is not always the answer, but the combination of sound online emergency management and communication practices integrated with the new technology is the ultimate communication goal for the next decade. Web 2.0 Media remains a channel despite its technology advancements, rapid access to information and large numbers of stakeholders, and low cost and ease of technology utilization. However, social media remains a communication vehicle, one with an ambitious agenda, but the power remains in the communicator or communicating organization, and their behaviors and narrative content, and not in the technology. "The real value of any communication – social media included – remains the quality of the content being disseminated around the actions a brand or company is taking, the empathy for affected stakeholders being displayed, and the appropriateness and relevance of the context and perspective being provided" (Aherton, 2009, 3). What is scary for many organizations and risk and crisis communicators is that social media speeds up communication, speeds up awareness, and often speeds up awareness of mistakes – the real question is whether it speeds up response and appropriate behavior?

Social Media Lessons Learned from Risk Communication Studies

Strategic Risk Communication: Ideas and Meaning Count

Strategic risk communication is about something: ideas and meaning count. Obvious and even trivial, risk communication researchers and communication campaign strategists often forget that their work can and do – positively or negatively – affect people's health, safety and environment, especially in relation to counter a domestic IED attack. Formative research prior to developing and implementing a risk communication campaign is essential, and strategic research via social media allows program planners to hear and learn from a myriad of stakeholders, including local residents, employees, health care providers, government officials, emergency personnel, and

vendors and contractors to name some major categories. With proactive dialogue, negotiated relationships and social identities as a starting point to examining the latest era of risk communication research and practices in relation to the use of social media, it is clear that strategic risk communication campaigns utilizing social media as another communication tool in the counter IED tool box of risk and crisis management can make a difference in communities; but only with the legitimate efforts of the government's prevention of terrorist attacks in the United States, political commitment, and the allocation of resources needed to carry out long-term risk communication.

Transparency

Transparency is not just about information; it is a process whereby active participation in acquiring, distributing and creating knowledge with stakeholders is essential to effective relationships. However, transparency and disclosure can facilitate communities to participate in environmental and development decision-making processes. One key aspect of risk communication consistently identified during ten years of research is to adhere to and improve voluntary protocols and laws improving the public's right of access to information and participation in organizational and governmental environment and economic decision making.

For example, technology enables organizations to communicate instantly and continually with stakeholders. Social media and other new communication technologies allow stakeholders the opportunity to unearth potentially unlimited amounts of information about risk generating organizations and related public policy debates. According to Gower (2006), the Internet has shaped the expectation of transparency and provided the facility to be transparent.

Build Trust over Time through Community Outreach and Collaborative Decision Making

Public distrust of industry and government officials is readily apparent. Research has demonstrated that industry and government regulatory officials are not considered the most trusted sources of risk information, including media and public relations spokespersons. For example, residents who demonstrated trust in industry and emergency response personnel were more likely to gather information, be knowledgeable and exhibit positive behavioral intentions regarding emergency response procedures (Palenchar & Heath, 2002). One part of the studies examined whether over a ten-year period increased awareness of industry's health and safety efforts increased support and trust for the industry. While residents were more supportive of the industry in relation to these efforts it did not necessarily translate into trust for the involved industry and government officials or awareness of specific communication efforts or sources of information (Palenchar & Heath, 2006b).

For effective risk communication, the source of information and advice needs to have a satisfactory level of trust in the judgment of each public (Renn & Levine, 1991). People tend to be less afraid of risks that come from places, people, corporations or other organizations that they trust, and are more afraid if the risk comes from a source they don't trust (Ropeik & Gray, 2002). If expert risk estimates conflict with one another, the decision to be made becomes more complex and requires greater amounts of trust.

Organizations that work to build trust over time through community outreach and collaborative decision making help to demonstrate an organization's efforts to achieve reasonable levels of health and safety. Such levels need to withstand the knowledgeable skepticism of the area residents that they could and should trust industry to exert reasonable amounts of security and

communicate in ways that increase rather than decrease citizens' security. Trust is ultimately demonstrated in word and dead. It is groomed and maintained, and can be lost or destroyed. If citizens cannot trust organizations or to be responsible, they will turn to other entries – activists and non-governmental organizations – to force appropriate operating standards.

Acknowledge the Uncertainty in Risk Assessments

The very nature of risk prohibits absolute definitions and knowledge. Driskill and Goldstein (1986) defined uncertainty "as the perceived lack of information, knowledge, beliefs and feeling necessary for accomplishing organizational tasks" (p. 41). In this vein, Albrecht (1988) defined uncertainty as the lack of attribution confidence about cause-effect patterns. Uncertainty motivates information seeking because it is uncomfortable. Using that principle, uncertainty reduction theory explains the human incentive to seek information (Berger & Calabrase, 1975). Publics want information to reduce their uncertainties about the subjects under consideration and about the people who are creating those uncertainties. As such, it would benefit both risk generating organizations and risk bearers if organizations acknowledge the uncertainty in risk assessments, and use it as an incentive for constantly seeking better answers to the questions raised.

Risk Communication is Carried out as Narrative Enactment

Communities of risk can be considered a front line in the marketplace of attitudes, knowledge and perceptions in relation to counter IED. In this social arena, society is the collective enactment of that discussion via narratives (in harmony, in conflict, that build conflict) as shared meaning made public through voices in unified competition (Heath, 1994).

Some communication scholars regard narrative as the paradigm of all communication (Fisher, 1985a). People think and act in terms of narratives, providing form and content to connect and give meaning to events. Narrative functions represent a universal medium of human consciousness (Lucaites & Condit, 1985) and a metacode for transactional transmission of messages about shared reality (White, 1981).

Within society discourse, the groups who are able to frame their interests as those of other groups exercise power. In the time of uncertainty – such as risk or crisis situations – the interpretations or narratives offered to frame and explain this uncertainty favor those of the empowered groups. Narratives are used to create, maintain and continue the interpretation and stabilizing the distribution of power within a society. In the marketplace of ideas there are many different stories interpreting any one event, and the use of social media to shape these ideas is critical. The acceptance of one narrative or interpretation leads to the elimination or muting of the alternatives.

Five Specific Gaps of Knowledge:

Specific gaps of knowledge identified include:

1. How is information being shared on social media sites, who are key influencers, and how do Internet memes (concepts that spread quickly via the Internet) develop, in addition to standard metrics of social media conversations on blogs, forums, social networks, and microblogging platforms (Twitter, Friendfeed) related to an IED event.

2. Monitoring and use of mobile technology during an IED event.

3. Better understanding the unique nature of information exchange among traditional and social media.

4. How are the properties of mediated publics like social networks sites different from unmediated publics in relation to risk communication message testing?

5. Discover and analyze what organization functions are engaged in social media and what business value is being realized.

Recommendations:

1. Despite an inconsistent understanding and incredibly diverse utilization of social media and digital mobile communication devices within risk and crisis communication, including whether or not they are part of an integrated crisis communication management plan and various federal government guidelines of its use, social media and especially digital mobile communication devices should immediately be integrated into risk and crisis communication plans to counter IEDs within the United States.

2. Despite the inability of organizational policy to strategically control and manage social media use due to the ever-changing nature of new media technologies, social media and especially digital mobile communication devices should immediately be integrated into risk and crisis communication plans to counter IEDs within the United States.

3. Local authorities and first responders for communication and coordination of civil populations in the immediate aftermath of terrorist attacks, local emergencies and disasters need considerable training and education in the use social media and especially digital mobile communication devices in relationship to risk communication plans to counter IEDs within the United States.

4. Digital hand-held communication devices should be used as an additional communication too, and not a replacement of traditional media and crisis communication tools, for transmitting hazard and risk warnings to members of the public who principally rely on these devices for news and communication, as well as for more communicating with traditional and new media communication outlets.

5. There are enormous implications of these devices on public risk perceptions of terrorism and the counter-terrorism efforts of authorities and government officials, given the prevalence of these devices among citizens, and the recent use of these devices for disseminating awareness of local disasters and emergencies. Such implications include variables of trust, dread, control, self-efficacy and other traditional risk communication psychometric variables analyzed in other sections of the overall project's reports.

6. Evidence suggests the clear potential that these devices hold for coordinating ad hoc search and rescue efforts and volunteer coordination among citizens and groups who do not have access to normal first responder channels.

In summary, government officials and agencies need to integrate social media, including the use of hand held digital devices, immediately into risk and crisis communication plans, provide the technology (hardware) and training resources necessary for proper utilization, develop the software and applications necessary for the community to generate and disseminate information during an IED attack, and essentially "get out of the way" of community residents and leverage their communication abilities to counter IED. At the same time, a short-term and long-term research agenda should be established to provide more research-based evidence that supports a return on investment in both capital costs and human and environmental health and safety, and address issues such as authenticity, misinformation campaigns, and privacy and liability concerns.

CONCLUSION

While there is strong anecdotal evidence that suggests that social media, and in particular mobile communication devices, can provide numerous opportunities to better manage risk and crisis communication during an IED attack in the United States, there is, unfortunately, little empirical research to validate social media's use during risk or crisis situations. As Fou (2010) recently argued, "the ROI [return on investment] of social media is still zero" (p. 1). In addition to the limited empirical research, since new media technology is rapidly advancing, it is difficult for any organization to develop policy that can catch up let alone keep pace with the uncertainty and ever-expanding use of social media platforms for risk and crisis communication.

This situation is changing rapidly however. Several significant projects have begun to examine and provide research into the use of social media during a risk or crisis situation, as well as the role of social media, and particularly mobile technology, on affecting behavior. While an exhaustive list is the not the purpose, several examples demonstrate the potential value of this new research. Lockheed Martin's Advanced Technology Lab and the University of Maryland, Baltimore County, have teamed up on a Department of Defense grant to create computerized simulations of how social media users react during disasters in order to test and possible create new communication tools. Stanford University's Persuasive Technology Lab creates insight into how computing products -- from websites to mobile phone software -- can be designed to change what people believe and what they do, including behavior related to safety. The National Center for Food Protection and Defense's Risk Communication Theme Group is working on social media to improve product recall, mobile technology, and industry reputation issues. Measurement of social media efforts are improving rapidly as well, as characterized by S4's Information Terrain Visualizer and Oak Ridge Lab's social media measuring projects, and social media efforts such as the Centers for Disease Control and Prevention during the H1N1 outbreak are positive signs for the advancement of the use of social media during risk and crisis events.

Yet, with social media, everyone has the potential to be watchdogs, citizen journalists, photojournalists and caring or nosy neighbors that can constantly survey the world around them and share what they find online, which can be used to improve risk and crisis

communication efforts if managed strategically and appropriate resources are injected to train and prepare government public information officers. The stakeholders on the ground of a risk or crisis event are generally the ones with first-hand knowledge of the event. These people may serve the role of information brokers or technical facilitators as they assist in connecting people and information via a number of technology media. They can provide and distribute information as well as create visuals to help organize relevant information. They may not intend to help crisis communicators but the information they provide inherently does.

References

Agenti, P. (2006). How technology has influenced the field of corporate communication. *Journal of Business and Technical Communication, 20*(3), 357-370.

Aherton, J. (2009, October). *Frontlineonline: Crisis planning in the digital age.* Surrey, United Kingdom: International Public Relations Association. Retrieved from http://www. ipra.org/archivefrontlinedetail.asp?articleid=1400

Aikin, A. (2009, November). *Communicating during a novel emergency: How to make your messages viral by using social media.* Washington, DC: Social media for crisis communications in government. Retrieved from http://www.aliconferences.com/conf /social_media_crisis1109/

Albrecht, T. L. (1988). Communication and personal control in empowering organizations. In J. A. Anderson (Ed.), *Communication yearbook* (Vol. 11, pp. 380-404). Newbury Park, CA: Sage.

Allen, K. J. (2007, March). *Speed to web: Web content report.* Retrieved from http://www. ragannewsletters.com

American Red Cross. (2010). *Safe and well list*. Retrieved from https://disastersafe.redcross.org

American Red Cross. (2010, August 9). *Web users increasingly rely on social media to seek help in a disaster.* Retrieved from http://www.redcross.org/portal/site/en/menuitem. 94aae335470 e233f6cf911df43181aa0/?vgnextoid=6bb5a96d0a94a210VgnVCM10000089f0870aRCRD

Andén-Papadopoulos, K. (2009, March). U. S. soldiers imaging the Iraq War on YouTube. *Popular Communication, 7*(1), 17-27.

Arthur W. Page Society. (n.d.). *Establishing principles for public relations on the Internet.* Retrieved from http://www.awpagesociety.com/site/resources/establishing_principles_for_pr

Baekel, T. (June 23, 2008). *The mobile internet revolution is here.* Retrieved from http://www.baekdal.com/trends/mobile-internet-revolution

Bargh, J. A., & McKenna, K. Y. A. (2004). The Internet and social life. *Annual Review of Psychology*, *55*, 573-590.

Beaubien, G. (2009, May). *Domino's YouTube* flap: A landmark event in crisis management. *Public Relations Tactics, 16*(5), p. 4.

Beaumont, C. (2008). *Mumbai attacks: Twitter and Flickr used to break news.* Retrieved from http://www.telegraph.co.uk/news/worldnews/asia/india/3530640/Mumbai-attacks-Twitter-and-Flickr-used-to-break-news-Bombay-India.html]

Beck, U. (1992). *Risk society: Towards a new modernity*, Translated from German by M. Ritter. London, Sage Publications, Newbury Park, CA.

Beck, U. (1999). *World risk society,* Polity Press, Cambridge, UK.

Becker, M. (2009, March 5). What Twitter did for crisis journalism today. *Hypercrit.* Retrieved from http://www.hypercrit.net/2009/03/05/what-twitter-did-for-crisis-journalism-today/

Beelinelabs. (2009a). *Emerging best practices: Social media monitoring, engagement, and measurement.* Retrieved from http://socialmediaanalysis.com/2009/06/

Beelinelabes. (2009b). *Social media 10x10: 10 things to know about 10 important social marketing topics.* Retrieved from http://socialmediaanalysis.com/2009/06/

Bellavita, C. (2010). Changing homeland security: Twelve questions from 2009. *Homeland Security Affairs, 6*(1), 1-30.

Berger, C. R., & Calabrese, R. J. (1975). Some explorations in initial interaction and beyond: Toward a developmental theory of interpersonal communication. *Human Communication Research, 1*(2), 99-112.

Berman, S. J., Abraham, S., Battino, B., Shipnuck L., & Neus, A. (2007). New business models for the new media world, *Strategy & Leadership, 35*(4), 23–30.

Bernoff, J., & Li, C. (2008). Harnessing the power of the oh-so social web. *MIT Sloan Management Review*. Retrieved from http://sloanreview.mit.edu

Bernstein, J. (2006, October). Who are these bloggers, and why are they saying these things? *Associations Now*, pp. 56–61.

Bostrom, A., & Lofstedt, R. E. (2003). Communicating risk: Wireless and hardwired. *Risk Analysis, 23*(2), 241-248.

Bowen, S. A. (2004). Expansion of ethics as the tenth generic principle of excellence: A Kantian theory and model for managing ethical issues. *Journal of Public Relations Research*, *16*(1), 65–92.

Boyd, D. M. (2007). Social network sites: Public, private, or what? *Knowledge Tree, 13.* Retrieved from http://kt.flexiblelearning.net.au/tkt2007/?page_id=28

Boyd, D. M., & Ellison, N. B. (2008). Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication, 13,* 210-230.

Buchwalter, C. (April 22, 2009). Online engagement deepens as social media and video sites reshape the Internet. Retrieved from http://www.nielsen-online.com/blog/2009/04/22/ online-engagement-deepens-as-social-media-and-video-sites-reshape-the-internet/

Bulkely, K. (2010, June 18). *Mobile technology takes centre stage in disaster relief.* Retrieved from http://www.guardian.co.uk/activate/mobile-technology-disaster-relief

Buzzlogic. (n.d.). *12 Essential tips for success in social media.* Retrieved from http://www.buzzlogic.com/case_study/12EssentialTipsWhitepaper_Yellow.pdf

Cardon, P. W. (2009). Online social networks. *Business Communication Quarterly, 72*(1), 96-119.

Cashmore, P. (2009, November 19). Next year's Twitter? It's Foursquare. *CNN.Com.* Retrieved from http://edition.cnn.com/2009/TECH/11/19/cashmore.foursquare/

Center for Social Media. (2009, February). *Public media 2.0: Dynamic, engaged publics.* Retrieved from http://www.centerforsocialmedia.org/ resources/publications/public_media_2_0_dynamic_engaged_publics

Chan, T. C., Killeen, J., & Griswold, W. (2004, November). Information technology and emergency medical care during disasters. *Academy of Emergency Medicine, 11*(11), 1229- 1236.

Cisco Systems Inc. (2009). *Annual security report: Highlighting global security threats and trends.* San Jose, CA.

Clark, J., & Aufderheide, P. (2009, February). *Public media 2.0: Dynamic, engaged publics.* Washington, DC: Future of Public Media Project.

Cloudman, R., & Hallahan, K. (2006). Crisis communication preparedness among U. S. organizations: Activities and assessments by public relations practitioners. *Public Relations Review, 32,* 367-376.

Colley, K. L., & Collier, A. (2009, Spring). An overlooked social media tool? Making a case for wikis. *Public Relations Strategist,* 34–35.

Coombs, W. T. (2008, April 2). *Crisis communication and social media.* Retrieved from http://www.instituteforpr.org/essential_knowledge/detail/crisis_communication_and_social_media/

Coombs, W.T. (2007). Protecting organization reputations during a crisis: The development and application of situational crisis communication theory. *Corporate Reputation Review, 10*, 163–176.

Cordner, G., & Scarborough, K. (2010, January). Information sharing: Exploring the intersection of policing with national and military intelligence. *Homeland Security Affairs, 6(1).*

Crush, P. (2006), Firefighting in the digital age: Crisis conference report. *PR Week,* pp. 24–26.

Currie, D. (n.d.). *Special report: Expert round table on social media and risk communication during times of crisis: Strategic challenges and opportunities.*

Digital Government: Technologies and practices. (2002). *Decision Support Systems, 34,* 223– 227.

Decker, K. C., & Holtermann, K. (2009). The role of exercise in senior policy pandemic influenza preparedness. *Journal of Homeland Security and Emergency Management, 6*(1), Article 32.

Deragon, J. (2008). *Leveraging social media for business purposes. White* paper. Retrieved from http://www.slideshare.net/jderagon/Leveraging-Social-Media-for-Business

Drapeau, M., & Wells, L. (2009). *Social software and security: An initial "net assessment."* Washington, DC: Center for Technology and National Security Policy, National Defense University.

Driskill, L. P., & Goldstein, J. R. (1986). Uncertainty: Theory and practice in organizational communication. *The Journal of Business Communication, 23*(3), 41-56.

Early Strategies Consulting. (2008). *The business impacts of social networking.* White paper. Retrieved from http://www.business.att.com/content/whitepaper/WP-soc_17172_v3_11-10-08.pdf

Ellison, N. B., Steinfield, C., & Lampe, C. (2007). The benefits of Facebook "friends": Social capital and college students' use of online social network sites. *Journal of Computer-Mediated Communication, 12*, 1143-1168.

Emergency Management. (2010, February). *Communication capabilities: Survey executive summary.*

Eyrich, N., Padman, M. L., & Sweetser, K. D. (2008). PR practitioners' use of social media tools and communication technology. *Public Relations Review, 34*, 412-414.

Facebook.com. (2010a). Hope for Haiti. Retrieved from http://www.facebook.com/search/?init=srp&sfxp=&o=65&q=hope+for+haiti

Facebook.com. (2010b). Home. Retrieved from http://www.facebook.com/search/?q=american+red+cross&init=quick

Federal CIO Council ISIMC NISSC Web 2.0 Security Working Group. (2009, September). *Guidelines for secure use of social media by federal departments and agencies.*

Fernando, A. (2007, January-February). Social media change the rules. *Communication World*, 9-10.

Festinger, L., Pepitone, A., & Newcomb, T. (1952). Some consequences of deindividuation in a group. *Journal of Abnormal and Social Psychology, 47*, 382-389.

Fisher, W. R. (1985). The narrative paradigm: An elaboration. *Communication Monographs, 52*(4)*,* 347-367.

Florini, A. (2007), *The right to know: Transparency for an open world* (Ed.).New York: Columbia University Press.

Fou, A. (2010, November 10). *The ROI of social media is still zero.* NY: Incisive Interactive Marketing.

Giddens, A. (1991), *Modernity and self-identity*. Palo Alto, CA: Stanford University Press.

Gillpin, D. (2008). Narrating the organizational self: Reframing the role of the news release. *Public Relations Review, 34,* 9-18.

GIS and emergency management in Indian Ocean earthquake / tsunami disaster. (2006, May). White paper.

Goldstein, B. D. (2005). Advances in risk assessment and communication. *Annual Review of Public Health, 26,* 141-163.

Gomez, E. A., Passerini, K., & Hare, K. (2006, May). Public health crisis management: Community level roles and communication options. In B. Van de Walle & M. Turoff (Eds.), *Proceedings of the 3rd International ISCRAM Conference* (pp. 435-443). Newark, New Jersey.

González-Herrero A., & Ruiz de Valbuena, M. (2006). Trends in online media relations: Web-based corporate press rooms in leading international companies. *Public Relations Review, 32*(3), 267–275.

González-Herrero, A., & Smith, S. (2008). Crisis communications management on the web: How internet-based technologies are changing the way public relations professionals handle business crises. *Journal of Contingencies and Crisis Management, 16*(3), 143–153.

Goolsby, R. (2009). Lifting elephants: Twitter and blogging in global perspective. In H. Liu, J. J. Salerno, & M. J. Young (Eds.), *Social computing and behavioral modeling* (pp. 2–7). New York: Springer.

Gordon, J. (2009). The coming change in social media business applications: Separating the biz from the buzz. Social Media Today.

Gordon, J. (2007a). The mobile phone and the public sphere. *The International Journal of Research into New Media Technologies*, *13*(3), 307–319.

Gordon, J. (2007b). The mobile phone and the public sphere: Mobile phone usage in three critical situations. *Convergence, 13*, 307-319.

Gower, K. K. (2006). Truth and transparency. In K. Fitzpatrick & C. Bronstein (Eds.), *Ethics in public relations: Responsible advocacy* (pp. 89-105). Thousand Oaks, CA: Sage.

Grunig, J. E., & Huang, Y. H. (2000). From organizational effectiveness to relationship indicators: Antecedents of relationships, public relations strategies, and relationship outcomes. In J. A. Ledingham & S. D. Bruning (Eds.), *Public relations as relationship management* (pp. 23–54). Mahwah, NJ: Erlbaum.

Grunig, J. E., & Hunt, T. (1984). *Managing public relations*. New York: Holt, Reinhart & Winston.

Guion, D. T., Scammon, D. L., & Borders, A. L. (2007). Weathering the storm: A social marketing perspective on disaster preparedness and response with lessons from Hurricane Katrina. *American Marketing Association, 26*(1), 20-32.

Guth, D. W., & Alloway, G. A. (2008). *Untapped potential: Evaluating state emergency management agency web sites 2008.* Retrieved June 29, 2009 from http://people.ku.edu/~dguth/ WebVersionEMA.pdf

Hallahan, K. (2009). Crises and risk in cyberspace. In R. L. Heath & H. D. O'Hair (Eds.), *Handbook of risk and crisis communication* (pp. 415–448). New York: Routledge.

Hamilton, J. T. (2005), *Regulation through revelation: The origins, politics, and impacts of the Toxic Release Inventory Program*. Massachusetts: Cambridge University Press.

Hare, B. (2009, October 14). *Does your social class determine your online network?* In CNN. Retrieved from http://www.cnn.com/2009/TECH/science/10/13/social. networking.class/index.html

Harris Interactive, Inc. (2009, April 16). *Just under half of Americans have a Facebook or MySpace account.* The Harris Poll.

Haythornthwaite, C., & Kendall, L. (2010). Internet and Community. *American Behavioral Scientist, 53*(8), 1083–1094.

Haythornthwaite, C., & Nielson, A.L. (2007). Revisiting computer-mediated communication for work, community, and learning. *Psychology and the Internet: Intrapersonal, Interpersonal and Transpersonal Implications*. Burlington, MA: Academic Press.

Heath, R. L. (1994). *Management of corporate communication: From interpersonal contacts to external affair*. Hillsdale, NJ: Erlbaum.

Heitmann, H., & Lott, B. (2008). Protecting corporate reputation in an ERA of instant transparency. In P. D. Alaleo & N. Pal (Eds.), *From strategy to execution: Turning accelerated global change into opportunity* (pp.237-257). Berlin: Springer.

Hinduja, S., & Patchin, J. W. (2008). Personal information of adolescents on the Internet: A quantitative content analysis of MySpace. *Journal of Adolescence, 31,* 125-146.

Homeland Security. (2009, December 9). Secretary Napolitano unveils "Virtual USA" information-sharing initiative. *Press Release.* Retrieved from http://www.dhs.gov/ ynews/releases/pr_1260375414161.shtm

Hon, L. (2006). Negotiating relationships with activist publics. In K. Fitzpatrick & C. Bronstein (Eds.), *Ethics in public relations: Responsible advocacy* (pp. 53–69). Thousand Oaks, CA: Sage.

Hon, L. C., & Grunig, J. E. (1999). *Guidelines for measuring relationships in public relations*. Gainesville, FL: Institute for Public Relations.

Hughes, A., & Palen, L. (2009). Twitter adoption and use in mass convergence and emergency events. *International Journal of Emergency Management, 6* (3/4), 248-260.

Hughes, A, Palen, L., Sutton, J., Liu, S., & Vieweg, S. (2008). "Site-seeing" in disaster: An examination of on-line social convergence. *Proceedings of the Information Systems for Crisis Response and Management Conference* (ISCRAM 2008).

Information in a crisis: text messages beamed to earthquake survivors in Haiti. (2010, June 18). Retrieved from http://www.guardian.co.uk/activate/information-in-a-crisis

Ingram, M. (April 12, 2010). *Mary meeker: Mobile internet will soon overtake fixed internet.* Retrieved from http://gigaom.com/2010/04/12/mary-meeker-mobile-internet-will-soon-overtake-fixed-internet/

Israel, S. (2009). *Twitterville: How businesses can thrive in the new global neighborhoods.* New York: Penguin Group.

Jacobs, I. (2009, June). The new interaction of social media. *Customer Relationship Management*, p. 12.

Jacques, A. (2009, Spring). Blog Council leaders discuss the importance of social media in corporate communications. *Public Relations Strategist,* 30–31.

Jaeger, P. T., Shneiderman, B., Fleischmann, K. R., Preece, J., Qu, Y., & Wu, P. F. (2007). Community response grids: E-government, social networks, and effective emergency management. *Telecommunications Policy, 31*, 592-604.

Java, A., Song, X., Finin, T., & Tseng, B. (2007, August 12). *Why we Twitter: Understanding microblogging usage and communities.* Conference paper presented at 9th WEBKDD and 1st SNA-KDD Workshop, San Jose, CA.

Johnson, C. (2009, Spring). Social media in a crisis: Blog and Tweet your way back to success. *Public Relations Strategist,* 23–24.

Karjaluoto, E. (March 1, 2008). *A primer in social media: Examining the phenomenon, its relevance, promise and risks.* White paper. SmashLAB. Retrieved from http://www.auburnmedia.com/wordpress/2008/10/13/prca-2008-state-conference-notes-links-and-observations/

Kelleher, T. (2008). Organizational contingencies, organizational blogs and public relations practitioner stance toward publics. *Public Relations Review, 34*, 300–302.

Kelleher, T. (2007). *Public relations online: Lasting concepts for changing media.* Thousand Oaks, CA: Sage.

Kim, P. (2009). Social media predictions for 2009. White paper. Retrieved from *beingpeterkim.typepad.com/files/Social%20Media%202009.pdf*

Klaassen, A. (2009, March 16). *How two Coke fans brought the brand to Facebook fame.* Retrieved from http://adage.com/abstract.php?article_id=135238.

Krämer, N. C., & Winter, S. (2008). Impression management 2.0: The relationship of self-esteem, extraversion, self-efficacy, and self-presentation within social networking sites. *Journal of Media Psychology, 20*(3), 106–116.

Krimsky, S. (2007). Risk communication in the internet age: The rise of disorganized skepticism. *Environmental Hazards, 7,* 157-164.

Lariscy, R. W., Avery, E. J., Sweetser, K. D., & Howes, P. (2009). An examination of the role of online social media in journalists' source mix. *Public Relations Review*, doi:10.1016/j.pubrev.2009.05.008.

Lefebvre, C. R. (2009, February 23). *Demographics of social network users (and other audience research).* [Web log message]. Retrieved from http://socialmarketing.blogs.com/r_craiig_lefebvres_social/2009/02/demographics-of-social-network-users.html

Leinhart, A. (2009, January 14). *Adults and social network websites.* Pew Internet & American Life Project. Retrieved from http://www.pewinternet.org/ Reports/2009/Adults-and-Social-Network-Websites.aspx

Leinhart, A., & Fox, A. (2009a, February 12). *Twitter and status updating.* Retrieved on June 23, 2009 from http://www.pewinternet.org/Reports/2009/Twitter-and-status-updating.aspx

Leinhart, A., & Fox, A. (2009b, February 12). *Twitterpated: Mobile Americans increasingly take to tweeting.* Retrieved from http://pewresearch.org/pubs/1117/twitter-tweet-users-demographics

Lipowicz, A. (2010, June 23). Widgets, Twitter to fuel FEMA emergency alerts. *Government Computer News.* Retrieved from http://gcn.com/articles/2010/06/23/fema-pushes-widgets-twitter-for-disaster-preparedness.aspx

Liu, S., & Palen, L. (2010). The new cartographers: Crisis map mashups and the emergence of neogeographic practice. *Cartography and Geographic Information Science (CaGIS) Journal*, *37*(1), 69-90.

Liu, S., Palen, L., Sutton, J., Hughes, A., & Vieweg, S. (2008). In search of the bigger picture: The emergent role of on-line photo-sharing in times of disaster. *Proceedings of the Information Systems for Crisis Response and Management Conference* (ISCRAM 2008).

Lucaites, J. L., & Condit, C. M. (1985). Re-constructing narrative theory: A functional perspective. *Journal of Communication, 35*(4), 90-108.

Lüders, M. (2008). Conceptualizing personal media. *New Media Society, 10*(5), 683-702.

Maltoni, V. (2009, January). *Marketing in 2009: 12 marketing professionals reveal their executive imperatives.* Conversation Agent.

Manfield, A. (2008). *What is social media?* E-book from iCrossing.

Mangold, W. G., & Faulds, D. J. (2009). Social media: The new hybrid element of the promotion mix. *Business Horizons, 52*, 357-365.

Marken, G.A. (2007) Social media...The hunted can become the hunter. *Public Relations Quarterly*, *52*(4), 9-12.

Market Content Flow Diagram. (n.d.). Retrieved from http://www.baekdal.com /articles/Management/market-of-information/

Mayfield, A. (2006). *What is social media?* Icrossing. Retrieved from http://www.spannerworks.com/fileadmin/uploads/eBooks/What_is_Social_Media.pdf

Mazer, J. P., Murphy, R. E., & Simonds, C. J. (2007). I'll see you on Facebook: The effects of computer-mediated teacher self-disclosure on student motivation, active learning, and classroom climate. *Communication Education, 56*, 1-17.

MC Marketing Charts. (n.d.). *Majority of Marketers Seek Email, Social Media Marriage.* Retrieved from http://www.marketingcharts.com/direct/majority-of-marketers-seek-email-social-media-marriage9637/?utm_campaign=newsletter&utm_ source=mc&utm_medium=textlink.

McDonald, D. D. (2007). *School implications & emergency response: What are the implications for social media.*

McKay, L. (June 2009). Everything's social (now). *Customer Relationship Management*, 24-28.

McLaughlin, S. (2009, Spring). Facing the Facebook nation: Will social networking sites help or hinder good business communications? *Public Relations Strategist,* 17–19.

Meisenbach, R. J., & Feldner, S. B. (in review). Adopting an attitude of wisdom in organizational rhetorical theory and practice: Contemplating the ideal and the real. *Management Communication Quarterly,* special issue on external organizational rhetoric.

Midkoff, S. F., & Bostian, C. W. (2002). Rapidly-deployable broadband wireless networks for disaster and emergency response. Presented at *The First IEEE Workshop on Disaster Recovery Networks (DIREN '02)*, New York City.

Moore, T. (2010, May). *Institutional barriers to resilience in minority communities.* Institute for Homeland Security Solutions.

Morgan, D. L. (1997). *Focus group as qualitative research.* Newburry Park, CA: Sage.

Musil, S. (October 26, 2008). *U.S. Army warns of twittering terrorists*. CNET News. Retrieved from http://news.cnet.com/8301-1009_3-10075487-83.html

National Commission on Children and Disasters. (2010). *2010 report to the president and congress.* Washington, DC: U.S. Department of Health and Human Services.

National Telecommunications and Information Administration. (2010, February). *Digital nation: 21st century Americas progress toward universal broadband internet access.* US Department of Commerce, Washington, DC. Retrieved from: http://www.ntia.doc.gov/reports/2010/NTIA_internet_use_report_Feb2010.pdf

Neff, J. (April 13, 2009). Study: ROI may be measurable in Facebook, MySpace after all. Retrieved from http://adage.com/abstract.php?article_id=135940.

Nichols, R. (June 7, 2010). *Emergency text messaging signals evolution in public safety communication.* Retrieved from http://www.emergencymgmt.com/safety/Emergency-Text-Messaging-Public-Safety-Communication.html

Number of US Facebook users over 35 nearly doubles in last 60 days. (2009, March 25). Retrieved from http://www.insidefacebook.com/2009/03/25/number-of-us-facebook-users-over-35-nearly-doubles-in-last-60-days/

Obama, B. (2009). *Transparency and open government: Memorandum for the heads of executive departments and agencies.* Washington, DC: The White House.

Ochman, B. L. (2009, April 13). *Amazon's silent mistake in the face of a social-media firestorm.* Retrieved from http://adage.com/digitalnext/post?article_id=135967

O'Dell, J. (April 2010). *New study shows the mobile web will rule by 2015.* Retrieved from http://mashable.com/2010/04/13/mobile-web-stats/

Owyang, J., & Toll, M. (2007). *Tracking the influence of conversations: A roundtable discussion on social media metrics and measurement.* A Dow Jones White Paper. Retrieved from http://www.web-strategist.com/blog/2007/08/20/social-media-white-paper-tracking-the-influence-factiva-of-dow-jones/

Paine, K. D. (2008, June 16). *KDPaine & Partners proposes new un-standard for social media measurement.* Retrieved from http://kdpaine.blogs.com/kdpaines_pr_m/ 2008/06/kdpaine-partner.html.

Palen, L. (2008). Online social media in crisis events. *Education Quarterly, 3, 76-78.*

Palen, L. (2002). Mobile telephony in a connected life. *Communications of the ACM*, *45* (3), 78-82.

Palen, L., Hiltz, R., & Liu, S. (2007). Online forums supporting grassroots participation in emergency preparedness and response. *Communications of the ACM*, *50*(3), 54–58.

Palen, L., & Liu, S. (2007). Citizen communications in crisis: Anticipating a future of ICT supported public participation. *Proceedings of the ACM 2007 Conference on Human Factors in Computing Systems (CHI 2007*), 727-736.

Palen, L., & Vieweg, S. (2008). Emergent, widescale online interaction in unexpected events: Assistance, alliance and retreat. *Proceedings of the ACM 2008 Conference on Computer Supported Cooperative Work (CSCW 2008),* 117-126.

Palen, L., Vieweg, S., Liu, S., & Hughes, A. (2009). Crisis in a networked world: Features of computer-mediated communication in the April 16, 2007 Virginia Tech Event. *Social Science Computing Review*, *27*(4), 467-480.

Palen, L., Vieweg, S., Sutton, J., Liu, S., & Hughes, A. (2007). Crisis informatics: Studying crisis in a networked world. *Proceedings of the Third International Conference on E-Social Science,* Ann Arbor, MI.

Palenchar, M. J., & Heath, R. L. (2002). Another part of the risk communication model: Analysis of communication processes and message content. *Journal of Public Relations Research, 14*(2), 127-158.

Palenchar, M. J., & Heath, R. L. (2006). *Strategic Risk Communication Campaigns: Some Insights from the Culmination of a Decade of Research.* Paper presented at the conference of the International Communication Association, Dresden, Germany.

Parr, B. (2010, March 29). Foursquare's growth not slowing down: 725,000 users, 22 million checkins. *Mashable Mobile.* Retrieved from http://mashable.com/2010/03/29/foursquare-growth-numbers/

Parr, B. (2009, June 17). Mindblowing #IranElection stats: 221,744 Tweets per hour at peak. *Mashable: The Social Media Guide.* Retrieved from http://mashable.com/2009/06/17/ iranelection-crisis-numbers

Pavlik, J. (June 4, 2008). *Mapping the consequences of technology on public relations.* Retrieved from http://www.instituteforpr.org/essential_knowledge/detail/ mapping_the_consequences_of_technology_on_public_relations/

Pew Research Center. (2010). *Government online: The internet gives citizens new paths to government services and information.* Washington, DC: Pew Internet & American Life Project.

Pew Research Center. (2008). *Key news audiences now blend online and traditional sources.* Retrieved from http://people-press.org/report/444/news-media

Pew Research Center. (2008, August). *Audience segments in a changing news environment: Key audiences now blend online and traditional sources.* Washington, DC: Pew Research Center Biennial News Consumption Survey.

Plotnick, L., White, C., & Plummer, M. (2009, August). The design of an online social network site for emergency management: A one-stop shop. *Proceedings of the 15th Americas Conference on Information Systems.* San Francisco, CA.

Pollack, M. (2007). Risk communication and the community response to a bioterrorist attack: The role of an internet-based early warning system A.K.A. "the informal sector". In M. S. Green at al. (Eds.), *Risk assessment and risk communication strategies in bioterrorism preparedness* (pp. 163-175). Springer.

Poniewozik, J. (2010, June 14). The soul of Twit. *Times,* p. 22.

Prentice, S., & Huffman, E. (2008, March). *Social media's new role in emergency management: Emergency management and robotics for hazardous environments.* Idaho National Laboratory: US Department of Energy. Retrieved January 31, 2010 from http://www.inl.gov/ technicalpublications/Documents/3931947.pdf

Present humanitarian information management. (n.d.). Harvard International Review. Retrieved from http://hir.harvard.edu/index.php?page=article&id=1923

Procopio, C. H., & Procopio, S. T. (2007). Do you know what it means to miss New Orleans? Internet communication, geographic community, and social capital in crisis. *Journal of Applied Communication Research, 35*(1), 67–87.

Rand, P. M., & Rodriguez, G. (2007). Relating to the public' the evolving role of public relations in the age of media. *The Council of Public Relations Firms*. White paper. Retrieved from http://www.prfirms.org/_data/n_0001/ resources/live/CPRF%20Social% 20Media%20White%20 Paper%20FINAL.pdf

Reddy, M. C., Paul, S. A., Abraham, J., McNeese, M., DeFlitch, C., & Yen J. (2009). Challenges to effective crisis management: Using information and communication technologies to coordinate emergency medical services and emergency department teams. *International Journal of Medical Informatics,78,* 259-269.

Renn, O., & Levine, D. (1991). Credibility and trust in risk communication. In R. E. Kasperson & P. J. Stallen (Eds.), *Communicating risks to the public* (pp. 175-218). Boston: Kluwer.

Ressler, S. (2006, July). Social network analysis as an approach to combat terrorism: Past, present, and future research. *Homeland Security Affairs, 2*(2). Retrieved from http://www.hsaj.orh

Reynolds, B. (2006). Response to best practices. *Journal of Applied Communication Research, 34*(3), 249-252.

Reynolds, B., Galdo, J., & Sokler, L. (2002). *Crisis and emergency risk communication.* Atlanta, GA: Centers for Disease Control and Prevention.

Reynolds, B., & Seeger, M. W. (2005). Crisis and emergency risk communication as an integrative model. *Journal of Health Communication, 10,* 43-55.

Robinson, E. (2010, January 13). Following the earthquake in Haiti on Twitter. *Washington Post.* Retrieved from http://voices.washingtonpost.com/postpartisan/2010/01/ following_the _earthquake_in_ha.html

Ropeik, D., & Gray, G. (2002). *Risk: A practical guide for deciding what's really safe and what's really dangerous in the world around you.* New York: Houghton Mifflin.

Ross, C., Orr, E. S., Sisic, M., Arseneault, J. M., Simmering, M. G., & Orr, R. R. (2008). Personality and motivations associated with Facebook use. *Computers in Human Behavior, 25*, 578-587.

Safko, L., & Brake, D. K. (2009). *The social media bible: Tactics, tools & strategies for business success.* Hoboken, NJ: John Wiley & Sons.

Sandman, P. (2006). Crisis communication best practices: Some quibbles and additions. *Journal of Applied Communication Research, 34*(3), 257-262.

Sanfilippo, A., Cowell, A. J., Malone, L., Riensche, R., Thomas, J., Unwin, S., Whitney, P., & Wong, P.C. (2009, June). Technosocial predictie analytics in support of naturalistic decision making. *Proceedings of NDM9, the 9th International Conference on Naturalistic Decision Making*.

Schulman, D. (2005, September). Their war. *Columbia Journalism Review, 44*(3), p. 13.

Scott, D. M. (2010). *The new rules of marketing and PR: How to use social media, blogs, news releases, online video, and viral marketing to reach buyers directly.* Hoboken, NJ: John Wiley & Sons.

Society for New Communications Research. (2008). *New media, new influencers and implications for public relations.* White paper. Retrieved from http://www.sncr.org/wp-content/uploads/2008/08/new-influencers-study.pdf

Scherp, A., Schwagereit, F., Ireson, N., Lanfranchi, V., Papadopoulos, S., Kritikos, A., Kopatsiaris, Y., & Smrs, P. (2009). Leveraging Web 2.0 communities in professional organizations. *W3C Workshop on the Future of Social Networking.* Barcelona, Spain. Retrieved from http://www.w3.org/2008/09/msnws/papers/ScherpEtAl LeveragingWeb2Communities.pdf

Seeger, M. W. (2006). Best practices in crisis communication: An expert panel process. *Journal of Applied Communication*, *34*(3), 232–244.

Sellnow, T. L., & Vidoloff, K. G. (2009, September). Getting communication right. *Food Technology, 63*(9), Retrieved from http://www.ift.org

Seo, H., Kim, J. Y., & Yang, S. U. (2009). Global activism and new media: A study of transnational NGO's online public relations. *Public Relations Review, 35*(2), 123–126.

Shankar, K. (2008). Wind, water, and Wi-Fi: New trends in community informatics and disaster management. *The Information Society, 24*(2), 116–120.

Shklovski, I., Burke, M., Kiesler, S., & Kraut, R. (2010). Technology adoption and use in the aftermath of Hurricane Katrina in New Orleans. *American Behavioral Scientist, 53,* 1228–1246.

Shklovski, I., Palen, L., & Sutton J. (2008). Finding community through information and communication technology in disaster events. *Proceedings of the ACM 2008 Conference on Computer Supported Cooperative Work (CSCW 2008)*.

Simon, S., & Stevenson, J. (2010, May 4). Combating simple, yet deadly, forms of terrorism. *Washington Post,* p. A23.

Slovik, P. (2002). Terrorism as hazard: A new species of trouble. *Risk Analysis, 22,* 425-426.

Smith, A. (2010, April). *Government online: The internet gives citizens new paths to government services and information.* Washington, DC: Pew Internet & American Life Project.

SMS text donations and the Haiti earthquake. (2010, January 14). Retrieved from http://mobileactive.org/mobile-giving-and-haiti-earthquake-relief-efforts.

Solis, B. (2009). *The state of PR, marketing, and communications: You are the future.* Retrieved from www.briansolis.com.

Solis, B. (2008a). *The essential guide to social media*. Retrieved from http://www.briansolis.com

Solis, B. (2008b, November 3). *Reinventing crisis communication for the social web.* Retrieved from http://www.briansolis.com/2008/11/reinventing-crisis-communications-for-the-social-web/.

Solis, B., & Breakenridge, D. (2009). *Putting the public back in Public Relations: How social media is reinventing the aging business of PR*. Upper Saddle River, NJ: Pearson Education.

Solis, B., & Carroll. B. (2008). *Customer service: The art of listening and engagement through social media*. 1-32. Retrieved from http://www.briansolis.com

Starbird, K., Palen, L., Hughes, A., & Vieweg, S. (2010). Chatter on the red: What hazards threat reveals about the social life of microblogged information. *Proceedings of the ACM 2010 Conference on Computer Supported Cooperative Work (CSCW 2010).*

Steinfield, C., Ellison, N. B., & Lampe, C. (2008). Social capital, self-esteem, and use of online social network sites: A longitudinal analysis. *Journal of Applied Developmental Psychology, 29,* 434-445.

Stelzner, M.A. (March 2009). *Social media marketing industry report: How marketers are using social media to grow their businesses.* White paper. Retrieved from http://www.marketingcharts.com/interactive/marketers-top-social-media-twitter-blogs-linkedin-facebook-8692/social-media-industry-report-stelzner-time-commitment-march-2009jpg/.

Stephens, K. K., & Malone, P. C. (2009). If organizations won't give us information…: The use of multiple new media in crisis technical translation and dialogue. *Journal of Public Relations Research, 21*(2), 229–239.

Stephenson, D. (2007). Networked Homeland Security: Transforming the public into full partners in terrorism and natural disaster preparation and response by capitalizing on personal communication devices and the science of emergency behavior. *Homeland Security Institute*. Retrieved from http://www.hsaj.org.

Stephenson, D., & Bonabeau, E. (2007, February). Expecting the unexpected: The need for a networked terrorism and disaster response strategy. *Homeland Security Affairs, 3*(1). Retrieved from http://www.hsaj.org.

Sutton, J., Palen, L., & Shklovski, I. (2008, March). Backchannels on the front lines: Emergent uses of social media in the 2007 southern California wildfires. In F. Fiedrich & B. Van de Walle (Eds.), *Proceedings of the 5th International ISCRAM Conference,* Washington, DC.

Swartz, J. (2003). Security systems for a mobile world. *Technology in Society, 25*, 5-25.

Sweetser, K. D., & Metzgar, E. (2007). Communicating during a crisis: Use of blogs as a relationship management tool. *Public Relations Review, 33,* 340–342.

Sydell, L. (2009, October 21). Facebook divide along social lines. [radio broadcast episode]. In *Morning edition.* Washington, DC: National Public Radio.

Terdiman, D. (2009, January 15). Photo of Hudson River plane crash downs TwitPic. *CNET.* Retrieved from http://www. news.cnet.com

Terrorist 'tweets'? US Army warns of Twitter dangers. (2008, October 25). Retrieved from http://www.breitbart.com/article.php?id=081025182242.js2g2op8

Thelwall, M., & Stuart, D. (2007). RUOK? Blogging communication technologies during crises. *Journal of Computer-Mediated Communication, 12,* 189-214.

Tong, S. T., Van Der Heide, B., Langwell, L., & Walther, J. B. (2008). Too much of a good thing? The relationship between number of friends and interpersonal impressions on Facebook. *Journal of Computer-Mediated Communication, 13*, 531–549.

Top seven mistakes new twitter users make. (n.d.). Retrieved from http://www.10000words.net /2009/03/top-7-mistakes-new-twitter-users make.html

Traynor, P. (2008, September). *Characterizing the limitations of third-party EAS over cellular text messaging services.* Atlanta: Georgia Institute of Technology.

Turner, K. (2009, March 9). Finding the right "brand voice" on Twitter. Retrieved on June 24, 2009 from http://mashable.com/2009/03/09/twitter-brand-voice/.

Twitter as a tool for college public relations students. (n.d). Retrieved from http://www.auburnmedia.com/wordpress/2008/09/28/twitter-as-a-tool-for-college-public-relations-students/

United Nations Foundation. (2010). *New technologies in emergencies and conflicts report: The role of information and social networks*. New York.

United Nations Foundation. (n.d). *Communications saves lives, brings hope after Haiti earthquake*. New York. Retrieved from http://www.unfoundation.org/our-impact/stories-of-impact/health-data-disaster-relief/communications-saves-lives-hope-haiti-earthquake.html

U. S. Department of Commerce. (2010, February). *Digital nation: 21st century America's progress toward universal broadband internet access.* Washington, DC: National Telecommunications and Information Administration.

U. S. Department of Defense. (2010, February 25). *Directive-type memorandum (DTM) 09-026 – Responsible and effective use of Internet-based Capabilities.* Washington, DC.

U. S. Department of Homeland Security. (2008). *National response framework.* Washington, DC.

U. S. Department of Transportation. (n. d.). Next Generation 9-1-1. *Research and Innovative Technology Administration.* Retrieved from http://www.its.dot.gov/ng911/index.htm

US mobile navigation on the rise. (2010, June 25). Retrieved from http://www.marketing charts.com/uncategorized/us-mobile-navigation-on-the-rise-13370/?utm_campaign =newsletter&utm_source=mc&utm_medium=textlink

Veil, S. R., & Sellnow, T. L. (2008). Organizational learning in a high-risk environment: Responding to an anthrax outbreak. *Journal of Applied Communications, 92*(1), 75-93.

Veinott, B., Cox, D., & Mueller, S. (2009, June). Social media supporting disaster response: Evaluation of a lightweight collaborative tool. *Proceedings of NDM9, the 9th International Conference on Naturalistic Decision Making*.

Vieweg, S., Palen, L. Liu, S., Hughes, A., & Sutton, S. (2008). Collective intelligence in disaster: An examination of the phenomenon in the aftermath of the 2007 Virginia Tech shootings. Proceedings of the *Information Systems for Crisis Response and Management Conference*. Washington, DC.

Vieweg, S., Hughes, A., Starbird, C., & Palen, L. (2010). A comparison of microblogging behavior in two natural hazards events: What Twitter may contribute to situational awareness. *Proceedings of the ACM 2010 Conference on Human Factors in Computing Systems (CHI 2010*).

Virginia Department of Emergency Management. VAEmergency. Richmond, VA: Virginia Department of Emergency Management;2007 [cited 2008 June 2]. Available from: http://www.youtube.com/user/VAEmergency

Wagner, M. (2008, December). Companies becoming more sociable. *Communication News*, p. 8. Retrieved from http://healthcareprojmgmt.com/category/social-media/

Walls, A. (2007). *Corporate use of social networks requires multilayered security control.* Gartner Research.

Walther, J. B. (2007). Selective self-presentation in computer-mediated communication: Hyperpersonal dimensions of technology, language, and cognition. *Computers in Human Behavior, 23*, 2538-2557.

Walther, J. B., Van Der Heide, B., Kim, S. Y., Westerman, D., & Tong, S. T. (2008). The role of friends' appearance and behavior on evaluations of on Facebook: Are we known by the company we keep? *Human Communication Research, 34*, 28-49.

Waters. R.D., Burnett, E., Lamm, A., & Lucas, J. (2009). Engaging stakeholders through social networking: How nonprofit organizations are using Facebook. *Public Relations Review, 35*, 102–106.

White, C., Plotnick, L., Kushma, J., Hiltz, S. R., & Turoff, M. (2009). An online social network for emergency management. *Proceedings from the 6th International ISCRAM Conference.* Gothenburg, Sweden. Retrieved January 31, 2010 from http://www.iscram.org/live/node/4644

White, H. (1981). The value of narrative in the representation of reality. In W. J. T. Mitchell (Ed.), *On narrative* (pp. 1-23). University of Chicago Press.

Williams, T., & Williams, B. (2008, July-August). Adopting social media: Are we leaders, managers or followers? *Communication World*, 34-37.

Wolport, S. (November 18, 2008). *Crafting your image for your 1,000 friends on Facebook or MySpace.* Retrieved from http://newsroom.ucla.edu/portal/ucla/crafting-your-image-for-your-1-71910.aspx

Woodhall, J. (2007, March). The future of emergency response: Need for technology enabled process transformation. *Presented at the National Science Foundation Conference: Educational programs or Emergency Response Technology*, 1-7.

Word of Mouth Marketing Association. (2010, February). *Social media marketing disclosure guide.*

Wortham, J. (2010, January 13). $2 million in donations for Haiti, via text message. *The New York Times.* Retrieved from http://bits.blogs.nytimes.com/2010/01/13/ 1-million-in-donations-for-haiti-via-text-message/

Wright, D. K. & Hinson, D. H. (2009a). An updated look at the impact of social media on public relations practice. *Public Relations Journal, 3*(2).

Wright, D. K., & Hinson, M. D. (2009b). Examining how public relations practitioners actually are using social media. *Public Relations Journal*, 3(3), 2–32.

Wright, D. K. & Hinson, D. H. (2008). How blogs and social media are changing: Public relations and the way it is practiced. *Public Relations Journal, 2*(2).

Wyatt, E. (2010, June 27). Broadband availability to expand. *NewYorkTimes.com.* Retrieved from www.nytimes.com/2010/06/28/.../28broadband.html

York, E. H. (2009, April 20). What Domino's did right -- and wrong -- in squelching hubbub over YouTube Video. Retrieved from http://adage.com/abstract.php?article_id=136086

York, E. H. (2009, June 29). How to make your employees the noise of your brand online. Retrieved from http://adage.com/digital/article?article_id=137595

Young, J. (2009, February 9). *How not to lose face on Facebook, for professors.* Retrieved from http://chronicle.com/temp/email2.php?id=cHdNCM5csszyMxw59fvFTgxdZkqmbp9c

Yuan, Y., & Detlor, B. (2005, February). Intelligent mobile crisis response systems. *Communications of the ACM, 48*(2), 95-98.

Zhao, S., Grasmuck, S., & Martin, J. (2008). Identity construction on Facebook: Digital empowerment in anchored relationships. *Computers in Human Behavior, 24,* 1816-1836.

Chapter 6

Guidance for Local Officials and Emergency Response Organizations on Developing an Emergency Risk Communication (ERC) and Joint Information Center (JIC) Plan for an Improvised Explosive Device (IED) Attack

Author: **Vincent Covello, Ph.D.**
Center for Risk Communication

Abstract

This chapter contains detailed guidance for local officials and emergency response organizations on developing an Emergency Risk Communication (ERC) and Joint Information Center (JIC) plan for an Improvised Explosive Device (IED) attack. The purpose of an ERC/JIC plan is to ensure the delivery of understandable, timely, accurate, consistent, and credible information to the public, the media, and other stakeholders. The plan can be adapted for other types of terrorist attacks and emergencies.

Table of Contents

Table of Contents -- continued

Appendices

1.0. Introduction

1.1 Objectives

This chapter provides guidance for local officials and emergency response organizations on developing an Emergency Risk Communication (ERC) and Joint Information Center (JIC) plan for an Improvised Explosive Device (IED) attack. The purpose of an ERC/JIC plan is to ensure the delivery of understandable, timely, accurate, consistent, and credible information to the public, the media, and other stakeholders. The plan can be adapted for other types of terrorist attacks and emergencies.

1.2 Background

Each locality in the United States is responsible for developing its own ERC/JIC plan for an emergency, including an IED attack. Unfortunately, there are no clear guidelines for such plans. This lack of clear guidelines has resulted in a lack of consistency from community to community in communication strategy, procedures, and messaging.

The need for localities to have a comprehensive ERC/JIC plan is greater than ever. For example, communication technologies have changed radically within the past decade. These new communication technologies, particularly mobility communication devices, have changed how information about an emergency shared.

2.0 Elements of the ERC/JIC Plan

The ERC/JIC plan should include a list of the elements contained in the plan. Section 2.1 provides a sample list of such elements.

2.1 Sample Statement Regarding Elements in an ERC/JIC Plan

The [insert name of organization] ERC/JIC plan contains the following elements:

- Letter of Endorsement by Senior Management
- Objectives and Assumptions
- Management Structure
  - Incident Command System
  - Joint Information Center
- Management Policies
  - Message Clearance and Approval
  - Disclosure of Identifiable Private Data about Individuals
  - Authorization for Media Interviews
  - Notifications
  - Communication Coordination
  - Emergency Risk Communication Preparedness
- Communication Tasks
  - Leadership Tasks
  - Media Relations Tasks
  - Message Development Tasks
  - Partner/Stakeholder Outreach Tasks
  - Web Site Tasks
  - Administrative and Technical Support Tasks
  - Studio/Broadcast Tasks
  - Media Monitoring/Research Tasks
  - Hotline Tasks
  - Community Education Tasks
  - Employee Communications Tasks
  - Subject Matter Expert (SME) Communications Tasks
  - Policymaker/Legislative Communications Tasks
  - Information Management Tasks
- Information Dissemination Methods
  - Emergency Broadcasts
  - News Conferences
  - Individual Media Interviews
  - News Releases
  - Web Site Updates
  - Call Centers/Hotline Services/Telephone Messaging
  - Social Media
  - Other Media
  - Communicating with Special Needs Populations
- Joint Information Center (JIC) Structure
  - Incident Joint Information Center (I-JIC)

- Virtual Joint Information Center (V-JIC)
- ERC/JIC Plan Maintenance

Each element is described in the plan.

2.2 Sample Checklist of Elements in a Comprehensive IED Risk Communication Plan

- ❑ Identify terrorist scenarios involving the use of an explosive-based Improvised Explosive Device (IED) and a "dirty bomb" (an explosive-based IED used to disperse chemical, biological, or radiological material).
- ❑ Describe emergency risk communication roles and responsibilities for each scenario.
- ❑ Designate staff who will assume emergency risk communication roles and responsibilities.
- ❑ Designate who will lead the emergency risk communication effort.
- ❑ Designate who within the organization will be responsible and accountable for implementing designated emergency communication actions and activities.
- ❑ Identify who will need to be consulted during the emergency risk communication process.
- ❑ Identify who will need to be informed about emergency risk communication actions and activities.
- ❑ Designate who will be the lead communication spokesperson and backup spokespersons for different emergency risk communication scenarios.
- ❑ Identify, train, and prepare second and/or third shift spokespersons – a necessity given 24/7 media coverage or a prolonged event.
- ❑ Identify procedures for information verification, clearance, and streamlined approval.
- ❑ Identify procedures for coordinating emergency risk communication efforts with partners (for example, with emergency response organizations, law enforcement, elected officials, non-governmental organizations (NGOs), special interest groups, and government agencies at the local, county, state, and federal level.
- ❑ Identify procedures to secure required human, financial, logistical, and physical support and resources (such as people, space, equipment, support services, and food) for emergency risk communication operations during a short, medium and prolonged event (24 hours a day, 7 days a week if needed).
- ❑ Identify agreements on when, how, and under what conditions information will be released.
- ❑ Identify the organization with primary responsibility for developing messages and communications regarding specific issues of concern or specific stakeholders; prepare and sign memorandums of agreement.
- ❑ Identify and maintain a list of stakeholders and partners who will receive emergency risk communication products in advance of mass distribution.
- ❑ Identify policies regarding employee contacts with the media.
- ❑ Include regularly checked and updated traditional media contact lists (including after-hours news desks).

- ❑ Include regularly checked and updated partner contact lists (day and night).
- ❑ Identify procedures for testing, on a regular basis, the accuracy of all information contained in contact lists.
- ❑ Identify the schedule for exercises and drills to test the emergency risk communication plan.
- ❑ Identify subject-matter and technical experts (for example, university professors, consultants, and practitioners) who can be called on to support emergency risk communication efforts; know in advance their perspectives, viewpoints, and ability to communication complex scientific or technical information in plain language.
- ❑ Identify key target audiences.
- ❑ Identify preferred emergency risk communication channels (for example, emergency radio broadcasts, telephone hotlines, radio and television announcements, news conferences, Web site updates, text messaging, social media postings, and faxes) to communicate with the public, the media, nearby residents, key stakeholders, and partners.
- ❑ Include message maps for all anticipated or frequently asked questions from key internal and external audiences.
- ❑ Check the consistency of all information contained in message maps, fact sheets, Web sites, question-and-answer documents, frequently asked question (FAQ) documents, media kits, audio-visual material, template press releases, media talking points, and other emergency risk communication products.
- ❑ Include maps, charts, graphics, video clips, and other supplementary emergency risk communication materials compatible with specific media formats and needs.
- ❑ Include a signed endorsement of the emergency risk communication plan by the organization's director.
- ❑ Identify a process for revising and updating previously approved messages and related emergency risk communication products.
- ❑ Include procedures for posting, revising, and updating emergency risk communication information on the organization's Web site.
- ❑ Include procedures for posting, revising, and updating information shared through social media networks.
- ❑ Include emergency risk communication task checklists for the first 2, 4, 8, 12, 16, 24, 48 hours, and 72 hours.
- ❑ Include procedures for evaluating, revising, and updating the emergency risk communication plan on a regular basis.
- ❑ Include procedures for tracking and analyzing media coverage (including social media and Web site traffic).

3.0 ERC/JIC Letter of Endorsement by Senior Management

An ERC/JIC plan should begin with a section containing an endorsement letter from senior management. A sample letter of endorsement is provided in Section 3.1.

3.1 Sample ERC/JIC Letter of Endorsement by Senior Management

[Insert Date]

The [insert organization name] recognizes the need to communicate understandable, timely, accurate, consistent, and credible information during and after an IED attack. Information is critical to an effective response. Heightened fear and misinformation can impede efforts to reach affected individuals and groups. Armed with factual information, affected individuals and groups can be a powerful ally in addressing the emergency.

An effective IED Risk Communication (ERC) and Joint Information Center (JIC) plan is a resource multiplier. Many of the potential adverse outcomes of the attack can be mitigated through the implementation of an effective ERC/JIC plan.

Affected individuals and groups must feel empowered to take protective actions in the event of an IED attack. For response efforts to be successful, local leaders and emergency response officials must be able to instill in people a sense of safety and trust. Communication strategies and messages focused on safety and trust allow people to take the steps needed to protect themselves and their families.

Implementation of the ERC/JIC plan will help the [Insert Organization Name] meet the communications needs and expectations of the media, public, and other stakeholders. We hope to never have an IED attack. However, if we do, it is essential we be prepared to communicate effectively.

Sincerely,

[Insert Senior Management Name]

4.0 ERC/JIC Objectives and Assumptions

An ERC/JIC plan should include a section describing ERC/JIC objectives and assumptions. A sample statement of objectives and assumptions is provided in Section 4.1.

Section 4.1 Sample Statement of ERC/JIC Objectives and Assumptions

Introduction

Effective emergency risk communication is an essential part of the response to an IED attack. Communicating effectively during an IED attack serves multiple purposes. These include:

- informing and instructing widely divergent audiences (e.g., the public, the media, employees, customers, emergency responders, public officials, and other stakeholders);
- minimizing stress, anxiety, and fear;
- encouraging the adoption of appropriate protective actions by individuals and organizations;
- building trust;
- minimizing or dispelling misinformation or rumors.

The [Insert Name] ERC/JIC plan provides the framework needed for understandable, timely, accurate, consistent, and credible communication during an IED attack. The plan provides a framework for a coordinated response by all those involved in emergency response.

The [Insert Name] ERC/JIC plan is intended to systematically address the roles, responsibilities, and resources needed to provide information to affected individuals, groups, and partner organizations during an IED attack. An effective, well thought out ERC/JIC plan will save precious time if an IED attack happens. Lines of authority and relationships with response partners need to be built before an IED attack occurs, not during the emergency.

[Insert Name]'s ERC/JIC plan is based on best practice and principles. The ERC/JIC plan is an integral part of [Insert Name]'s overall emergency response plan.

ERC/JIC Objectives

1. Ensure an efficient flow of understandable, timely, accurate, consistent, and credible information during and after an IED attack.
2. Facilitate communication among key internal and external partners.
3. Provide needed information to all involved parties through the media and other information channels.
4. Promote informed decision-making by involved parties.
5. Persuade all involved parties to engage in recommended protective actions.
6. Elicit cooperation among all involved parties.

ERC/JIC Assumptions

1. Dissemination of understandable, timely, accurate, consistent, and credible information among stakeholders (affected, interested, and influential target audiences) is critical to the effectiveness of the overall response to an IED attack.
2. Different types of information will need to be communicated to different target audiences.
3. It is highly likely that during an IED attack there will be widespread circulation of conflicting information, misinformation, and rumors.
4. Communication must be coordinated among all relevant response organizations to ensure consistent messages.
5. It is highly likely during an IED attack that particular individuals and groups will be hard to reach.
6. Affected and interested individuals and groups will have a high demand for information during an IED attack.
7. People who experience an IED attack may experience anxiety, depression, family disruption, violence, substance abuse, absenteeism, and other related physical and mental health symptom; every effort must be made to prevent such negative outcomes.
8. Local officials, in coordination emergency response organization, are responsible for keeping the media, the public, other stakeholders informed about protective actions during and after an IED attack.
9. Understandable, timely, accurate, consistent, and credible information is key to maintaining public trust and reducing possible health or safety consequences.
10. Verified information must be released as quickly as possible, even if all the details are not yet known.
11. Erroneous information must be corrected immediately; erroneous information can become “common knowledge” and difficult or impossible to refute later.
12. Monitoring the media and responding rapidly to correct mistakes is vital.
13. The concept of "people first" should motivate communication actions.
14. Leaders and emergency response officials must express appropriate levels of caring, concern, and empathy to be trusted.
15. Information about the emergency intended for stakeholders must often be repeated several times; people typically do not process (hear, understand, and remember) information under stress as well as they do under normal circumstances.
16. Panic is one of the many widespread myths about public response to emergency warnings; panic occurs in very particular circumstance that rarely, if ever, can be found in an actual emergency.
17. Information about the emergency must be communicated using multiple media (for example, through radio, television, newspapers, hotlines, and Web sites) to ensure messages are heard and understood.
18. Effective communication during and after an IED attack requires a coordinated response by the licensee and response partners, including federal, state, regional, county, and local government agencies; hospitals; educational institutions; and NGOs (Non-Governmental Organizations).
19. Emergency risk communications should serve to:
    - convey the status of the emergency and actions to protect people and the environment;
    - reduce uncertainty and dispel rumors in order to minimize counter-productive behaviors;

- exemplify professionalism;
- reassure the public, the media, employees, emergency responders, public officials, and other stakeholders that the emergency is being handled appropriately;
- provide people with messages that create a sense of hope, self- and group efficacy, safety, calm, and connectedness.

5.0 ERC/JIC Management Structure

An ERC/JIC plan should include a section describing the management structure for emergency risk communications. A sample statement regarding the management structure for emergency risk communications can be found in Section 5.1.

Section 5.1 Sample Statement Regarding the Management Structure for Emergency Risk Communications

1. Incident Command System

The [Insert Name] has adopted the Incident Command System (ICS) structure to respond to an IED attack. Under the ICS structure, the [Insert Name]'s Public Information Officer (PIO) is a member of the Command Staff and coordinates emergency risk communication and information dissemination activities. Such activities are conducted in concert with others in the emergency response network.

The PIO or designee reports to the leader in the ICS structure, the Incident Commander. Activities undertaken by the PIO and emergency risk communications team include:

- news conferences;
- media interviews;
- press releases;
- media advisories;
- postings to the organization's Web site;
- media monitoring;
- rumor control;
- other duties as needed or assigned.

2. Joint Information Center

In an IED attack, all emergency risk communication activities will be coordinated through a Joint Information Center (JIC). The JIC is described in greater detail in a later section of this document.

The JIC is designed to disseminate information and instructions to interested and affected parties through news conferences, press releases, media interviews, media advisories, and other means as needed. Public and news media inquiries are handled through the JIC.

The establishment of a JIC is based on the following assumptions.

- The media will come to a JIC only if they believe they will receive important information and will have their questions answered.
- The media will go where the story is.
- The JIC should be located as close as possible to the scene of the emergency but out of the way of harm.
- Every organization participating in the emergency response should be encouraged to send a representative to the JIC.

- Every participating emergency response organization should be encouraged to refer journalists to the JIC.
- At least one JIC representative should be available round-the-clock to respond to media and other inquiries.
- At least one JIC representative should be available round-the-clock to report to the Incident Commander or Unified Command.

6.0 ERC/JIC Management Policies

An ERC/JIC plan should include statements regarding ERC/JIC management policies. Sample statements regarding ERC/JIC management policies can be found in Sections 6.1 to 6.6.

Section 6.1 Sample Statement Regarding Message Clearance and Approval

All information released to the public, the media, employees, public officials, emergency response partners, and other stakeholders must be internally cleared in a timely manner. In an IED attack, it is important messages be identified as:

- pre-cleared;
- require clearance;
- questionable.

Only with the approval of the Pubic Information Officer or designee, in coordination with the emergency management team, will information be released.

Every effort should be made to obtain pre-event clearance of emergency risk communication messages. In an IED attack, information voids will be filled by others. Messages that might normally take several hours or days to get the proper clearances, cross clearances, and coordination may have to be released in minutes.

Section 6.2 Sample Statement Regarding the Disclosure of Identifiable Private Data about Individuals

Incident reports received by emergency response organizations may contain identifiable private data about individuals. Identifiable private data about individuals shall not be disclosed, except as noted below.

As used here:

- "Disclosure" or "disclose" means the communication of identifiable private data to any individual or organization outside the [Insert Name].
- "Private data" means information, recorded in any form or media that relates to the status of individuals or their use of resources and services.
- "Identifiable private data" means any item, collection, or grouping of data that makes the individual or organization supplying it, or described in it, identifiable.

The PIO or designee will evaluate identifiable private data about individuals and determine the minimum amount necessary for emergency response purposes. The PIO or designee will evaluate to whom it is necessary to share this information. The disclosure of identifiable private data about individuals will vary depending on the type of emergency, how the information is acquired, who may be affected, and how much interest there may be at the time in determining who the individual is. This information may require written approval from managers in the human resources and legal departments prior to being released.

Section 6.3 Sample Statement Regarding Authorization for Media Interviews

All decisions regarding media interviews will be made by the Public Information Officer or designee in consultation with designated spokespersons, subject matter experts, partner organizations, and other relevant parties. Authorization to participate in a media interview will be based on:

- appropriateness of the interview, topic and venue;
- availability of selected staff in light of primary responsibilities;
- potential for exacerbating versus calming public fear or anxiety;
- potential for relating information that cannot or should not be disclosed;
- the impact the information conveyed on other organizations;
- the assessed intent of journalist or other media representative.

Section 6.4 Sample Statement Regarding Notifications In an IED attack

Timely notifications of an emergency to all relevant stakeholders are critical to the effectiveness of the emergency response. Notification lists should be based on answers to the following types of questions:

- Which departments in your organization need to be notified?
- Which managers in your organization need to be notified?
- Which emergency response organizations need to be notified?
- Which elected or appointed officials need to be notified?
- Which government agencies need to be notified?
- Which non-governmental organizations need to be notified?
- Which media organizations need to be notified?
- Which additional stakeholder groups, based on the specific nature of the emergency, need to be notified?

The Public Information Officer or designee will ensure notifications have occurred by checking off names of pre-identified stakeholders on worksheets. Worksheets with complete contact information (day and night) will be developed for each pre-identified stakeholder to be notified (For a sample worksheet, see the "Worksheet for Notifications" in the Section).

Section 6.5 Sample Statement Regarding Coordination of Communications with Emergency Response Partners

Coordination of communications between the [Insert Name] and its emergency response partners is critical to the effectiveness of the response. Coordination helps ensure consistency in messaging.

To facilitate coordination, the Public Information Officer or designee will take all practical steps to share information with key partners in advance of the release of information to the media or other stakeholders.

Section 6.6 Sample Statement Regarding Emergency Risk Communication Preparedness

Emergency risk communications preparedness is an ongoing process that ensures the delivery of understandable, timely, accurate, consistent and credible communications in an IED attack. The following is a checklist of preparedness actions needed for effective emergency risk communications.

Checklist

- ❑ Assess the information needs of the public, the media, public officials, emergency responders, and other stakeholders and identify ways to meet these needs.
- ❑ Identify important stakeholders and subgroups within the audience as targets for your messages.
- ❑ Identify credible third parties who could support your messages.
- ❑ Train staff in emergency risk communication skills.
- ❑ Recruit spokespersons with effective presentation and personal interaction skills.
- ❑ Anticipate questions and issues that might be raised by stakeholders.
- ❑ Set up a system to monitor what appears in the media, on web sites, and in other online sources of information.
- ❑ Prepare and pre-test messages before offering them to stakeholders.
- ❑ Set up a system for practicing media interviews.
- ❑ Determine who will conduct news conferences.
- ❑ Set up a system to confirm facts.
- ❑ Establish an organizational protocol for all contacts with the media.
- ❑ Ensure all staff members are aware of the organizational protocol for contact with the media.
- ❑ Establish an efficient clearance and approval procedure and ensure all staff members are aware of the clearance and approval procedure for the release of messages to the public, the media, and other stakeholders.
- ❑ Determine the resources needed to carry out the emergency risk communication plan.
- ❑ Ensure all staff members are aware of policies regarding the disclosure of identifiable private information about individuals.
- ❑ Rehearse with your lead media spokesperson prior to media contact.
- ❑ Determine how you would greet, register and handle journalists who arrive at the site of the emergency.
- ❑ Develop a triage system for prioritizing and responding to media requests and inquiries.
- ❑ Develop media contact lists.
- ❑ Evaluate previous interactions with stakeholders and review lessons learned.
- ❑ Review what others have learned about communications during IED attack events or exercises.
- ❑ Determine the resources needed to carry out the emergency risk communication plan.
- ❑ Prepare, in advance, fact sheets, news release, answers to frequently asked questions, web site materials, audio visual materials (for example, graphs, maps, photographs, and video clips), biographical sketches, telephone hot line scripts, and other communication materials relevant for an IED attack; share these materials for vetting and possible use by emergency partner organizations.

7.0 ERC/JIC Communication Tasks

An ERC/JIC plan should include a section describing communication tasks. A sample description of communication tasks can be found in Section 7.1.

Section 7.1 Sample Statement Regarding Emergency Risk Communication Tasks

In a major IED attack, emergency response organizations may receive hundreds or thousands of inquiries each day from the media, the public, employees, response partners, public officials, and other interested parties. These inquiries must be managed in an organized fashion to avoid chaos. One device for accomplishing this is to organize emergency risk communication activities according to tasks. For example, communication teams can be organized around one or more of these communication tasks:

- leadership tasks;
- media relations tasks;
- message development tasks;
- partner/stakeholder outreach tasks;
- Web site tasks;
- administrative and technical support tasks;
- studio/broadcast tasks;
- media monitoring/research tasks;
- hotline/call center tasks;
- community education tasks;
- employee communications tasks;
- subject matter expert communications tasks;
- policymaker/legislative communications tasks;
- information management tasks.

Each task is described below. Many of these tasks are done rountinely during non-emergency times. One of the major differences between emergency and non-emergency risk communications is the stress placed on organizational staff and routine communictions systems caused by staff shortages, unfamiliar territory, large workloads, deadlines, and time pressure.

Leadership Tasks:

- arrange for the preparation and distribution of the written emergency risk communication plan;
- ensure all relevant individuals have copies of the ERC/JIC plan;
- ensure all relevant individuals are trained in how to implement the ERC/JIC plan;
- activate and implement the Emergency Risk Communication/Joint Information Center plan based on a careful assessment of the situation;

- meet with organization leadership shortly after emergency notification to review emergency risk communication strategies and activities;
- arrange to bring in needed resources—human and logistical—as specified in the ERC/JIC plan;
- assemble the emergency risk communication teams shortly after emergency notification, brief them on the event, consult with them on what needs to be done, and delegate tasks and assignments;
- contact other responding organizations to learn what emergency risk communication activities they are planning;
- distribute the predetermined policy guidance documents (for example, policy on information clearance and approval);
- contact and confirm availability of pre-determined lead spokespersons;
- review the strengths, weaknesses, and training of lead spokespersons;
- brief the lead spokespersons and review with them their responsibilities;
- remind all employees about organizational policies regarding contacts with the media;
- ensure notification of those in and outside the organization who should be informed when an emergency occurs (Note: given the importance of notifications, consider assigning at least one staff member responsibility for maintaining the notification lists and for confirming notifications have occurred);
- ensure coordination and dissemination of information with other organizations before its release;
- provide periodic briefings on emergency risk communication strategies with organization leaders;
- provide periodic briefings on emergency risk communication strategies with the emergency risk communications team;
- provide periodic briefings on emergency risk communication strategies with select stakeholders;
- arrange for the conduct of news conferences;
- implement the predetermined strategy for coordinating internal and external communication activities;
- determine operational hours for emergency communication activities, including shift changes (Note: reassess the shift change schedule every 12-24 hours);
- carry out all leadership responsibilities and tasks in a calm, professional manner;
- be aware of, and respond appropriately to, signs of stress among staff (including yourself). Signs of stress include:
  - mental signs (for example, difficulty concentrating, forgetfulness, exercising poor judgment, seeing only the negative, anxious or racing thoughts, constant worrying)
  - emotional signs (for example, moodiness, irritability, short temper, agitation, restlessness, inability to relax, depression)
  - physical signs (for example, dizziness, chest pain, rapid heartbeat, sensitivity to loud noises)
  - behavioral signs (for example, overeating, isolating oneself from others, procrastinating or neglecting responsibilities, using alcohol, cigarettes, or drugs to relax, nervous habits such as nail biting and pacing)

Media Relations Tasks:

- organize and conduct news conferences;
- produce and distribute timely news releases and other materials for the media;
- respond to media requests and inquiries;
- provide support for spokespersons;
- coordinate responses to media inquires.

Message Development Tasks:

- develop and distribute draft talking/message points
- implement predetermined procedures for information verification, approval, and clearance;
- create drafts of news releases, fact sheets, question and answer sheets (Q&As), speeches, video scripts, public service announcements, and other communication materials;
- create appropriate graphics and other visual material to support messages and other communication materials;
- ensure information contained in communication materials is accurate, current, and cleared for release;
- ensure coordination and consistency of messages internally and across other responding organizations.

Partner/Stakeholder Outreach Tasks:

- maintain open channels of communication with partners and stakeholders located in interested or affected governmental, non-governmental, not-for-profit, and private sector organizations;
- coordinate announcements and releases of information with partner organizations.

Web Site Tasks:

- post pre-developed Web page for use on the organization's Web site;
- establish and maintain links to other Web sites;
- post information about the event on the Web site;
- oversee prompt updating of materials to the Web site;
- develop, as needed, password protected Web sites to share information within the organization and among partner organizations;
- determine who needs to approve posting and updating of information on the Web site;
- review and assess Internet/Web site visits and use.

Administrative and Technical Support Tasks:

- manage essential administrative and technical tasks;
- distribute emergency risk communication materials.

Studio/Broadcast Tasks:

- activate equipment and support the broadcast of news conferences and other media events;
- record and log all news conferences and other media events.

Media Monitoring/Research Tasks:

- scan print and broadcast media for information that could help or hinder the response effort;
- scan Web sites for information that could help or hinder the response effort;
- scan blogs for information that could help or hinder the response effort;
- scan logs from hotlines for information that could help or hinder the response effort;
- scan social media (for example, Twitter, Facebook, and YouTube) for information that could help or hinder the response effort;
- analyze and summarize information on stakeholder knowledge, attitudes, and behavior;
- analyze and report feedback from other teams for patterns and crosscutting trends.

Hotline/Call Center Tasks:

- establish hotlines for all relevant stakeholders (for example, the public, the media, employees, employee families, elected officials, emergency response partners, etc.);
- respond to hotline requests for information;
- distribute requests for information by the public, the media, employees, employee; families, elected officials, emergency response partners, and other stakeholders to the appropriate person or organization;
- coordinate with other responding organizations the function and use of the hotlines.

Community Education Tasks:

- facilitate meetings of interested or affected communities or special populations
- identify public education needs;
- develop and ensure distribution of educational materials on IEDs, terrorism, and related issues to interested or affected communities and special populations;
- develop public information campaign materials if needed.

Employee Communications Tasks:

- identify and open predetermined channels for communicating with employees;
- work with other team members on message development and dissemination;
- arrange for regular briefings of employees and employee families;
- coordinate information dissemination efforts with other teams;
- provide feedback from employees to other communication team members.

Subject Matter Expert (SME) Communication Tasks:

- identify and open predetermined channels for communicating with subject matter experts;
- coordinate with subject matter experts in partner organizations;
- arrange and conduct regular briefings for subject matter experts;
- respond to requests and inquiries from subject matter experts;
- provide feedback from subject matter experts to other communication team members.

Policymaker/Legislative Communications Tasks:

- identify and open predetermined channels for communicating with policymakers;
- distribute communication materials and updates to elected officials/legislators/special interest groups;
- respond to requests from elected officials/legislators/special interest groups;
- arrange routine briefings for selected policymakers;
- work with other team members to evaluate materials for policymakers;
- provide feedback from policymakers to other team members.

Information Management Tasks:

- collect, review, and finalize informational materials;
- maintain a database/log of emergency risk communication materials;
- facilitate clearance of printed materials and messages;
- centralize and streamline information products to be released.

8.0 ERC/JIC Information Dissemination Methods

An ERC/JIC plan should include a section describing information dissemination methods. Sample statements describing information dissemination methods typically used in an IED attack can be found below.

Section 8.1 Sample Statement Regarding Information Dissemination Methods

In a major IED attack, all appropriate and available information dissemination methods should be used. The use of multiple communication channels (for example, radio, television, Web sites, and call centers) can substantially increase the reach and visibility of messages and recommendations.

Information dissemination methods include:

- **Emergency Broadcasts.** Used to provide information and instructions to the public through Emergency Alert System broadcast messages and follow up Special News Broadcasts.
- **News Conferences**. Used to simultaneously convey information to all interested news media.
- **News Releases**. Used to disseminate important information to the news media and through them to the public.
- **Individual Media Interviews**. Used to respond to individual media requests for information.
- **Web Site Updates**. Used as an efficient way for providing background information, updates, and responding to frequently asked questions.
- **Call Center/Hotline/Telephoning Messaging.** Used to respond to inquiries from stakeholders and the media and to provide recorded messages about the incident.
- **Social Media (**for example, Twitter, YouTube, and Facebook). Used to convey information to interested parties and subscribers.
- **Other Media for Disseminating Information**. Used to supplement other information dissemination methods. May include video news releases, audio news releases, blogs, and other information dissemination techniques.
- **Information Dissemination Methods for Communicating with Special Needs Populations.** Special needs populations include individuals who have disabilities, live in large group settings, are elderly, are children, are from diverse cultures and/or have limited English proficiency (or are non-English speaking), and are transportation disadvantaged

Sample statements for each information dissemination method can be found in Sections 8.2 – 8.9.

Section 8.2 Sample Statement Regarding Emergency Broadcasts

(Source: Adapted from "Emergency Broadcast Process and Instructions (2002). Federal Emergency Management Agency.

The careful preparation of information and instructions to be made available to the public through Emergency Alert System (EAS) broadcast messages and follow up Special News Broadcasts are an essential facet of preparedness. Typically, the EAS is used for this

purpose; however, other means, such as the National Oceanic and Atmospheric Administration (NOAA) weather service or other broadcast media, may be used.

Emergency broadcasts should be made promptly and be accompanied by an explanation of the existing situation and accurate statements of the protective action decisions (if any). When time constraints for the EAS message limits the inclusion of requisite information and instruction to the public, Special News Broadcasts should immediately follow the EAS message to include this necessary information and instruction. Emergency instructions and informational messages should be clear, succinct and complete; demonstrate authority; and be presented in an appropriate style or format.

Procedures for providing emergency information and instructions are discussed in FEMA-CPG-1-40, "Emergency Alert System," and FEMA-CPG-1-41, "Emergency Alert System, A Program Guide for State and Local Jurisdictions." In addition, pre-distributed emergency public information brochures are an important resource for citizens to use.

With all of these resources available, emergency broadcast messages should be developed with one objective: to provide information on the status of the emergency and inform the public about what actions (for example, evacuation or shelter) they should take to protect themselves. By focusing on this objective, emergency broadcast messages can be kept relatively short. Thus, broadcasts can provide important instructions quickly and instructions can be rebroadcast at periodic intervals.

1. Coordination

There should be clear and direct lines of communication between the protective action decision making authority, the preparer of emergency broadcast messages, and the person responsible for activation of the EAS or other broadcast media and actual delivery of the message. If possible, these individuals should be co-located at a Joint Information Center. If not, dedicated telephone lines, dedicated facsimile capabilities, and Internet connection capabilities should be available to allow both oral communication and transmission of hard copy information. Backup communication systems, such as encrypted VHR radios or cellular telephones, should be designated and available for this purpose. It is particularly important that the person making protective action decisions review emergency broadcast messages, preferably a hard copy, prior to broadcast. All parties involved in the alert and notification process should thoroughly coordinate their activities relative to the activation of the alerting system and development and dissemination of the EAS message.

This coordination should include information about the scheduled times for alerts and notifications, the essential text of the EAS message, including identification of the emergency status and authorized protective action decisions. When possible, hard copies of EAS messages should be transmitted to each of the relevant parties prior to broadcast.

When multiple jurisdictions have authority for emergency broadcast activation, it is important to coordinate both message content and the timing of the message delivery.

The coordination of messages cannot occur unless there is effective communication among all parties responsible for providing information to be used in the EAS messages. Ideally, there should be a dedicated capability for simultaneous, multiparty

communications. This can minimize critical time delays in reaching concurrence on EAS messages and in implementing activation procedures. In an actual emergency, many radio and television stations will be on the air continuously reporting on the status of the emergency and providing supplemental information to the public. Thus, the EAS message can be clearly differentiated from other messages and focus on pertinent protective actions to be taken by the affected person.

2. Content

Emergency broadcast messages should be developed to include the following content as appropriate:

2.1 Identification of the authority (e.g., governor, county executive, or mayor) issuing the emergency message.

2.2 Description of the emergency. The nature and extent of the emergency should be described in terms understandable to the public.

2.3 Subsequent EAS messages should include all new information.

2.4 Clear identification of the audience. The message should convey who is at risk and for whom protective actions are intended by using familiar landmark descriptions, e.g., rivers, railroad tracks, interstate highways, buildings, local government jurisdictions (counties, townships, villages, and towns) or zip codes specified in the plan. If appropriate, reassuring information may be provided to guide the actions of those who are not in the immediate area where protective actions are warranted.

2.5 Information on sheltering. Sheltering instructions should be provided. Instructions should be provided for transients as well as information regarding restricted access areas. Provisions for children in schools in affected areas should be described.

2.6 Information on evacuation. Evacuation instructions should include who is to go, where to go, and how to get there, i.e., the population at risk, evacuation routes, and the location of reception/congregate care centers. When appropriate, the EAS message should include information for:

- transportation-dependent persons;
- handicapped persons;
- institutionalized persons;
- parents regarding their children in school or day care centers;
- evacuees.

2.7 Emergency “hotline” telephone numbers should be provided for those needing special assistance and for public inquiries.

2.8 When early ingestion pathway protective measures are recommended, instructions for their implementation (e.g., wash fruits and vegetables gathered from gardens) should be provided.

2.9 Instructions to stay tuned to the emergency broadcast stations should include indications at the end of the broadcast on when additional information can be expected.

3. Comprehensibility

Information must be conveyed in an easy to understand way.

3.1 Language

EAS broadcast messages should be presented with clear language that adequately conveys the significance of the information while succinctly specifying the needed emergency actions. Geographical locations should be expressed in familiar terms, using well known references and landmarks. Legal descriptions or map coordinates should be avoided.

3.2 Brevity

Emergency broadcast messages should be as short as possible in order for the public to comprehend the content of the messages. While it may be possible to develop and broadcast short messages for natural hazards, it may be difficult to develop short EAS broadcast messages for a terrorist attack given the uncertainties of the event.

Thus, state and local governments involved in terrorist attack preparedness should attempt to develop pre-scripted emergency broadcast messages that are as short and succinct as possible, but sufficient in length to adequately address the most important questions and concerns. EAS messages are generally up to 2 minutes in length. If the emergency situation warrants, Special News Broadcasts may be used immediately following the relatively brief EAS message to provide additional information and instruction to the public.

3.3 Clarity and Coherence

Clarity and coherence of content presentation are essential in order to promote prompt and appropriate actions. The message should specify the site of the emergency, circumstances and other conditions related to the emergency. Emergency broadcast messages should provide a smooth flow and logical sequence of information.

3.4 Consistency and Comprehensiveness

The content of EAS broadcast messages should be consistent with the state or local plan, annually distributed public emergency information materials, and previously broadcasted messages. The message should reference public emergency information materials that provide reinforcement and non-vital information. When circumstances dictate that information relayed over the EAS broadcast stations differ from that included in previously distributed and broadcast emergency information materials, such differences should be clearly identified to avoid confusion.

3.5 Repetition

Repetition is an element in an effective EAS broadcast system. Effective messages should include repetition of the key information, as well as a regularly scheduled repeating of all messages until new information is available and messages are updated. Repetitions serve to confirm important information about purpose, context, source and emergency actions expected of the public. It is possible that during the emergency a radio or television station may provide continuous reporting on the response to the emergency.

4. Format

Pre-scripted EAS broadcast messages can contribute to important time savings when the rapid flow of information is essential. Several things should be considered in selecting a format for pre-scripted messages. The chosen format should enable the development of clear, accurate and complete messages in a minimum amount of time.

A decision should be made as to the number of pre-scripted messages that should be prepared. Procedures should be established for reviewing messages prior to broadcast to ensure that:

- the newest or most vital information is presented near the beginning of the message;
- the message is organized so that all similar information is presented together;
- any changes in emergency status or protective action decisions are delineated;
- information no longer applicable is deleted;
- information contained in the message is consistent;
- all protective action decisions are contained in the message, including those from earlier broadcasts;
- the status of all affected areas, including any areas where protective actions identified in previous broadcasts have been lifted, is presented;
- message content is clear and concise;
- both new and critical information is repeated within the message.

5. Delivery

The person having the responsibility for physically activating the EAS broadcast station should act only after receiving instruction from the designated emergency response official vested with the decision-making authority to issue protective action decisions and authorize activation.

Timing of alert signals and media message broadcasts should be closely coordinated. Procedures should be established to ensure that there is close coordination with parties responsible for siren activation (or other alerting mechanisms) and EAS broadcast activation and to ensure that all parties are aware of the scheduled time for both events. These procedures should ensure that emergency messages are broadcast immediately following cessation of the siren, or at least within five minutes after siren activation.

It is important that all designated radio and television stations broadcast the message at the designated time. The local population should have a listing of EAS broadcast stations in pre-distributed brochures, calendars, telephone books, or other means. The listing should include instructions to immediately tune to one of these stations when alerted. A capability should exist for monitoring these stations to ensure that correct messages are

broadcast at the designated time and repeated with the designated frequency, e.g., every 15 minutes.

A well-coordinated emergency broadcast program requires 24-hour-staffing capability with competent and knowledgeable personnel. Individuals tasked with preparation of instructional messages and with activation of the EAS broadcast system should be properly trained. They should know how, and by whom, they will be notified to initiate the EAS broadcast message and activate the EAS broadcast stations. They should be familiar with procedures for: message development, coordination of message content and delivery with participating jurisdictions, establishment of communication with primary and backup EAS stations and completion of the authentication process. Personnel should be properly trained in the operation of their primary and backup equipment. This primary and backup equipment, especially equipment necessary for emergency broadcast activation, should be checked periodically to make sure that it is operational. Substitute personnel should be identified and trained in the event that primary personnel are unavailable to perform these tasks.

In summary, EAS broadcast messages are the primary vehicles for transmitting important emergency instructions and information to the public. They should be clear, concise, simply stated, and authoritative if they are to be effective. With careful planning and a flexible, imaginative approach to the form and content of EAS broadcast messages, this goal can be achieved

Addendum: Comprehensibility, Language, and Readability

Clear language for an emergency broadcast, as well as all emergency communications, refers to the ease with which a given passage of text can be read and understood. As indicated by the National Incident Management System Integration Center of the Federal Emergency Management Agency,

> "The use of plain language in emergency response is matter of public safety, especially the safety of first responders and those affected by the incident. It is critical that all local responders, as well as those coming into the impacted area from other jurisdictions and other states as well as the federal government, know and utilize commonly established operational structures, terminology, policies and procedures."[1]

In determining comprehensibility and readability[2], two basic factors should be considered: sentence length and vocabulary difficulty.

---

[1] NIMS Integration Center, NIMS Alert, "NIMS and the Use of Plain Language," December 19, 2006
NA: 023-06

[2] Several formulae have been developed to predict comprehensibility and readability. These include the Dale-Chall Formula, the Flesch Reading Ease Formula, the Flesch-Kincaid Grade Level Formula, the FOG Readability Formula, and the SMOG Readability Formula. The Dale-Chall formula is a vocabulary-based formula. The Flesch Reading Ease Formula and the Flesch-Kincaid Grade Level Formula base their readability scores on the average number of syllables per word and number of words per sentence.

The longer the average sentence length, the more difficult the information is to understand. More complex and more difficult language usually is associated with longer sentence length. Sentence length is also related to the complexity of the sentence structure. For example, as the number of dependent clauses in a given sentence increases, so does the intellectual sophistication needed to comprehend the material.

Language that can be described as "bureaucratic" should be avoided. Language that is overly technical or legalistic should be avoided. Everyday terms and expressions should be used wherever possible.

The higher the proportion of words classified as "difficult", the higher, or more difficult, the passage rating will be. Word difficulty affects readability in the following ways:

(a) Over-reliance on words with three or more syllables increases the difficulty rating of the passage.

(b) Over-reliance on words not found in lists of familiar words increases the difficulty rating of the passage. Several Web sites contain lists of familiar words, including the Dale-Chall list.

Section 8.3 Sample Statement Regarding News Conferences

During an IED attack, it is important to get factual and appropriate information to the public as quickly as possible via the news media. Getting this information to the media during an emergency will typically require several news conferences.

News conferences provide reporters with the facts of the event as known and what is not known. They provide information on steps being taken to respond to the emergency. They provide opportunities for reporters to ask questions.

The two basic elements of a news conference agenda are listed below.

1. **Opening/Introductory Remarks and Speaker Presentations**

The opening/introductory remarks and speaker presentations at a news conference provide confirmed and appropriate facts. Opening/introductory remarks and speaker presentations are typically given by speakers from the represented organizations. Speakers typically provide information about:

- the who, what, where, why, when, and how of the emergency;
- what is being done by emergency response organizations;
- what people should be doing.

2. **Questions and Answers**

Microsoft Word, as part of its spelling and grammar checker, can display readability scores for a document using the Flesch Reading Ease Formula and the Flesch-Kincaid Grade Level Formula.

The opening/introductory remarks and speaker presentations are typically followed by a question and answer session. The person moderating the news conference should:

- allow time for questions from journalists;
  (Note: Failure to allow time for questions may encourage journalists to go elsewhere for information. It may also result in journalists deciding not to attend the news conference.)
- direct questions from journalists to the appropriate person;
- consider closing the Q&A with a repetition of key messages.

Section 8.4 Sample Statement Regarding the Logistics of a News Conference

Effective news conferences can be major undertakings. They require hard work, attention to detail, and preparation to be successful. Staff responsible for organizing news conferences should use the following checklists to ensure all appropriate actions are taken.

1. Checklist Regarding Location of the News Conference

- ❑ Consider holding the news conference at a hotel or public building in a central location if you don't have access to a convenient and appropriate off-site location.
- ❑ Make sure the room is not too large as otherwise there may be lots of empty seats, giving the impression that few journalists attended.
- ❑ Make sure there is sufficient room and places for all the speakers to stand or sit (for example, a long table or sufficient space behind the podium for the speakers to stand).
- ❑ Ensure there is adequate open space for television cameras, lights and microphones.
- ❑ Provide technical support and seating convenient for different media (such as forward seating for radio and open space in the front for photographers).
- ❑ Provide access to the internet (for example, through wireless connections or dedicated computers).
- ❑ Ensure there are an adequate number of electrical outlets.

2. Checklist Regarding Timing of the News Conference

- ❑ Accommodate local and national media deadlines.
- ❑ Remember journalists have busy schedules.
- ❑ Because of deadlines, often the best time to hold a news conference is from 9:00 A.M .–10:30 A.M. on a weekday morning or 3 P.M. – 4 P.M . on a weekday afternoon, although this may vary by locality.
- ❑ Consider when to end the news conference. If you want to make the 12 noon, 6 P.M. or 11 P.M. television or radio news programs, keep in mind some news crews may need time to travel or edit tape.
- ❑ If you are going to set restrictions, such as limited photo access or limits on the number of seats available, put the restrictions in writing and communicate them to the media in advance.

- ❑ Plan around competing events and other activities that may prevent journalists from attending the news conference.
- ❑ In fast-breaking emergencies, consider holding at least two news conferences per day
  (thereby allowing the spokesperson to gather more information, to come back the same day to give more in-depth information, and to say: "I don't know the answer to that now but I will try to have more information for you later today).
- ❑ Quickly release critical information.

3. Checklist Regarding Notifications of the News Conference

- ❑ Send a notice of the news conference by email, fax, or other means.
- ❑ Include in the notice of the news conference:

  - the location;
  - the start and finish times;
  - the date;
  - the agenda or brief description of what will be covered;
  - names and titles of speakers.

- ❑ Bear in mind that newsrooms are often swamped with releases, faxes, and invitations to events.
- ❑ Don't call unnecessary news conferences; if it's not worth their time, the media will only be angered.
- ❑ Ensure all emergency response partners have been notified of the news conference with sufficient time for feedback.
- ❑ Be considerate of the time of reporters and others when scheduling a news conference. If no new information is to be reported, let the reporters know ahead of time.

4. Checklist Regarding Materials for the News Conference

- ❑ Put together a media kit or media packet for journalists attending the news conference. Include in the kit or packet:

  - the agenda or brief description of what will be covered;
  - press releases;
  - fact sheets;
  - the names and titles of speakers;
  - biographical information (including photographs, if possible) of speakers, subject-matter experts, and others as appropriate;
  - contact numbers;
  - copies of any reports or documents that would be useful to reporters covering the event;

- visual material (such as maps, charts, timelines, diagrams, drawings, photographs of the facility);
- information sheets containing locations of local hotels, restaurants, coffee shops, etc.;
- other materials as appropriate.

- ❑ Consider handing out a page at the outset of the session with the names, titles and responsibilities of the presenters.
- ❑ Decide in advance whether handouts are needed
- ❑ Make sure you have plenty of copies of media packets or information materials in case more people attend than expected.
- ❑ If the speaker is giving a presentation for which there is a text, you may want to wait and hand out the text after the talk so reporters will stay and listen. However, it's advisable to tell the media you will provide a text of the presentation so they are not irritated by having to take unnecessary notes.
- ❑ Have a sign-in sheet for journalists attending.
- ❑ Use the sign-in sheet to update your media contact list.

5. Checklist Regarding Preparations for the News Conference

- ❑ Set up the room for the number of people you expect.
- ❑ Set up a podium or front table, if appropriate.
- ❑ Provide water for the speakers.
- ❑ Make sure microphones, chairs, lighting and water are in place at least 30 minutes prior to the event.
- ❑ Notify all partner organizations you are having a news conference.
- ❑ Decide what partner organizations to invite to attend or participate in the news conference.
- ❑ Don't be disappointed if fewer people show up than expected – attendance is hard to predict.
- ❑ Try to limit the length of the news conference to less than 30 to 45 minutes, but be flexible.
- ❑ Have staff available to assist journalists before, during and after the event.
- ❑ Arrange for assistants to be on hand to help distributing media kits or packets, managing the sign-in sheet, directing journalists to telephones, and handling any last-minute details.
- ❑ Select a moderator for the news conference who will set the ground rules.
- ❑ Consider setting the following ground rules:

  -- all reporters asking a question must first be recognized by the moderator;

-- each reporter recognized by the moderator will be allowed to ask one question and one follow-up question;

-- all questions should be directed to the moderator who in turn will direct the question to the appropriate speaker;

-- all reporters should, if possible, indicate which speaker they would like to direct their question.

- ❑ Determine beforehand which speaker will make the opening remarks.
- ❑ Introduce each speaker, and decide when the question/answer period ends.
- ❑ Discuss camera placement with camera crews and movement during the event.
- ❑ Supply the necessary hook-ups for electronic media, including lighting and audio (microphone).
- ❑ Develop anticipated questions and answers for speakers.
- ❑ Rehearse the speakers if time allows, asking them basic challenging questions.
- ❑ Make your formal opening statement brief – around three to seven minutes
- ❑ Make sure you mention all pertinent information (for example, who, what, where, when, why and how) in your opening statement.
- ❑ Allow time for questions (typically at least 10 to15 minutes).
- ❑ As a general rule, limit the number of speakers to no more than three and limit speaking time to no more than 5 minutes.
- ❑ If additional people are available to answer questions, have them sit in the front row or off to the side, where they can easily be called on and be seen by the audience when speaking.
- ❑ Start on time – journalists work to deadlines and need time to complete their story on time.
- ❑ Remember: a news conference is held primarily to allow the media to ask questions, not attend a lecture.

6. Checklist Regarding Follow-Up to a News Conference

- ❑ Thank reporters for attending.
- ❑ Allow time at the conclusion of the news conference to arrange photographs.
- ❑ Tell reporters how unanswered questions raised in the news conference will be handled and provide call-in number or web-site information.
- ❑ Tell reporters when the next news conference will be held, if one is scheduled.
- ❑ Offer to fax, email, or post to the Web site materials for those journalists who were unable to attend.
- ❑ Consider following the news conference with a media availability session where all the partners are available as a panel to talk to media one at a time but can hear each partner's comments.
- ❑ Make sure your staff knows where to direct telephone calls from journalists calling after the event.
- ❑ Monitor media coverage following the news conference.
- ❑ Recognize reporters often pay attention to comments (both positive and negative) about news stories and may integrate the comments into future stories.
- ❑ If requested, set up one-on-one interviews with subject matter experts or speakers.

Section 8.5 Sample Statement Regarding Guidelines for the News Conference Moderator

Checklist

- ❑ Ensure the lead spokesperson has a predetermined message for the news conference (If they do not have a message or something new or interesting to say, you may not need to hold a news conference.)
- ❑ Set a time limit for each speaker prior to starting the news conference
- ❑ Introduce yourself, including your name, title, spelling of your name, and pronunciation of your name
- ❑ Explain the format of the news conference
- ❑ Provide the time frame (usually no more than 30 to 45 minutes)
- ❑ Read all or the most important part of the most recent news release if changes have been made
- ❑ Refer the reporters to any handout materials
- ❑ Introduce the speakers, including their titles
- ❑ Provide the correct spellings and pronunciation for the names of all speakers (especially for speakers with names having an unusual spelling or pronunciation)
- ❑ Refer reporters to the biographical sketches of the speakers in the media packet
- ❑ Invite the speakers to present, indicating the approximate amount of time they will be speaking
- ❑ Begin the presentations by the speakers
- ❑ Begin the question and answer period
- ❑ Lay out the ground rules for the question and answer period, such as:
  -- one question and one follow up question per reporter;
  -- being recognized by the moderator before asking a question;
  -- stating your name and what media organization you represent
- ❑ Always allow time for a few questions from reporters
- ❑ Avoid letting one reporter dominate the time available for questions and answers
- ❑ End the news conference, announcing the time for the next scheduled news conference
- ❑ If there is no scheduled news conferences to follow, let the reporters know how they can find about where and when the next news conference will occur
- ❑ Inform the reporters if news conferences are scheduled by partner organizations
- ❑ Consider making one or more of the speakers available at the end of the news conference

Section 8.6 Sample Statement Regarding the Opening of a News Conference

Welcome, ladies and gentlemen to [insert time: today's; this morning's; this afternoon's; tonight's] news conference.

My name is[insert name and title].

We will be presenting information at this news conference on [insert topic].

I will briefly read the latest news release.

With us today are [insert names and titles].

Biographical information for each person presenting at this news conference can be found in the media packet at the back of the room or given to you when you entered.

We will begin the news conference with a brief statement from [name the individual; indicate the spelling and pronunciation of the person's name; state their organizational title].

We will also have statements from [name the individuals; indicate the spelling and pronunciation of the person's name; state their organizational title].

We will then open the floor to your questions. We will be available for [insert number] minutes today.

Please allow me to recognize you before asking a question.

Please restrict yourself to one question and one follow up question.

Please identify who you are and what media organization you represent

(at the end of the Q&A)

Because of ongoing emergency operations, we will have time for two more questions.

Thank you for your questions.

We will now adjourn.

The next scheduled news conference will be in this same room at [insert time].

Following the news conference, staff will be available to help you with any further needs.

Section 8.7 Sample Statement Regarding Media Interviews

A media interview is a question-and-answer session usually done on a one-to-one basis between an organizational spokesperson and a reporter. Media interviews are typically initiated by the reporter. The purpose of the media interview is to relay information from the organization to the reporter and to respond to questions from the reporter.

The Public Information Officer or designee will select spokespersons from a pre-approved list for media interviews. Once a media interview is completed, the interviewed staff member must promptly send a summary of the interview to the Public Information Officer or designee. The summary should provide, at a minimum, the reporter's name, the name of media organization, the questions asked, the topics covered, and any concerns resulting from the interview. The interviewed staff member should immediately contact the Public Information Officer or designee if questions or concerns raised during the interview need an urgent response. If staff members are contacted directly by a reporter for a media interview, the staff person should direct the reporter to the Public Information Officer or designee at [Insert telephone number].

Section 8.8 Sample Statement Regarding Pitfalls in a Media Interview

- **Don't assume you are the right person to be interviewed**. Discuss with the reporter the specific topic of the interview before the interview to ensure you are the right person to be interviewed.
- **Don't assume you know what the first question from the reporter will be**. Consider asking the reporter in advance what the first question will be.
- **Don't allow the interview to stray from the topic**. Offer (1) to cover additional topics during a separate interview or (2) put the reporter in touch with someone who is better able to respond than you.
- **Don't let a reporter put words in your mouth**. The reporter may use inflammatory or emotionally laden words. Do not repeat them.
- **Don't accept a question that is improperly framed**. Rephrase a question if it contains leading or loaded language, and then answer the question.
- **Don't assume the reporter is correct about facts**. Be on guard for claims that someone has made an allegation or has shared damaging information. Instead of reacting to such information, say: "I have not heard that" or "I would have to verify that before I could respond". Do not allow the reporter to start a fight.
- **Don't volunteer more than you want to say**. If a reporter persists after you've answered a question by asking the question again, then stop. Wait for the next question or say: "That was my answer. Do you have another question you would like me to address?" Say it without sarcasm, defensiveness or annoyance.
- **Don't go "off the record."** There is no absolute assurance that what is said "off the record" will not be reported.
- **Don't assume your knowledge or position alone qualifies you to answer questions**. Work with your colleagues to anticipate as many questions as possible. Determine if you are the best person to answer the question. If you are, draft the answers to as many as time permits. Nuances count. A word change here or there may make the difference as to how well your answer is received. Write your first draft of the answers then edit them or have them edited. Identify the key words in the answer. Identify the main points you want to make and put them first. Put the "bottom line" up front. Does it ring true?
- **Don't go into an interview without at least three key messages**. Have prepared message points and make them at the very start of the interview. Try to get across your key message points in sound-bite format in fewer than 27 words and less than nine seconds. Be prepared to elaborate on your prepared message points.

- **Don't guess or fake it when responding to questions.** If you do not know the answer or cannot answer, say so. Give the reason why you do not know or can't answer. For example, if it's not in your area of expertise, say so and then bridge to what you do know.
- **Don't speak disparagingly of others, not even in jest**.
- **Don't assign blame or point fingers.** Stick to what you know and what your organization is doing.
- **Don't fight your battles using the media**. Remind the journalist that professionals often have legitimate differences of opinion.
- **Don't buy into extreme or baseless "what if" questions**. Rephrase the question in a way that addresses the legitimate and warranted concerns.
- **Don't depend on the reporter to remember what was said**. Use a tape recorder to record sensitive interviews, if necessary. Be sure the reporter knows you are doing this before the interview.
- **Don't ask journalists to allow you review their articles or interviews**. Offer to clarify information for the reporter as they prepare their story. If a reporter shows you the story, understand he or she expects you to correct errors of fact not viewpoints that may differ from yours.
- **Don't try to answer all parts of a multiple-part question**. Break down multiple-part questions and answer each part separately.
- **Don't raise issues you do not want to see in print or on the news**.
- **Don't say "no comment" to a reporter's question**. People often interpret "no comment" statements as showing guilt, hiding something, lying or covering up. Instead, state why you cannot answer the question. For example, say the matter is under investigation, the organization has not yet made a decision, or simply that you are not the right person to answer the question. If appropriate, indicate follow-up actions you are willing to take, including providing referrals or providing further information by the reporter's deadline.
- **Don't assume you have been quoted correctly**. Have someone monitor media coverage and check whether your statements were edited incorrectly or out of context. If significant errors are discovered, seek further coverage to correct mistakes and get your points across.
- **Don't miss the reporter's deadline for the interview**. If you miss the reporter's deadline, your perspective may go unrepresented in the reporter's story.
- **Don't assume facts speak for themselves.**
- **Don't assume the interview will be easy.**

Section 8.9 Sample Statement Regarding Methods for Responding Effectively to Challenging Questions in a Media Interview

Responding to sensational, negative or unrelated questions

Answer the question in as few words as possible, without repeating the sensational or negative elements, then return to one or all of the three key messages – recommended "bridging phrases" to help do this include the following.

- Let me emphasize again what I said before…

- The overall issue on the table, from my perspective, is…
- What's important to remember about this issue is…
- What I can tell you about this issue that might be helpful is…
- What I'm really here to discuss is the critical importance of…
- What all these issues boil down to is…
- What is really important for your [readers/viewers/listeners] to know is….

Responding to character attacks

Do not attack the character of an adversary. It may be necessary to question the science, issues or goals, but not someone's character. For example, say, "I can't speak for Dr X. You'll have to ask him/her. What I can address is…."

Responding to machine-gun questioning

Be aware that a reporter might ask questions rapidly, quicken the pace, or frequently interrupt your responses. One response to this is to say, "Please let me answer this question". Control the pace and take time to think.

Responding to microphone feeding and pausing

Be aware of situations in which a good answer has been given to a controversial question, and the reporter says nothing while the cameras continue to roll. Silence on air does not make for interesting viewing unless the spokesperson is reacting nervously or uncomfortably so be aware of non-verbal cues. Avoid a "deer-in-the-headlights" appearance, fidgeting, wiping of the brow and shifting frequently in the seat. It is the reporter's job to fill the airtime so relax and wait for their next question.

Responding to a hot microphone

Assume the microphone is always on – including during "testing" and chatting before and after the interview.

Responding to a sensational question with an A or B dilemma

Reject both A or B if neither is valid. Explain by saying "there's actually another alternative you should consider", and give the message point. Use positive words and correct inaccuracies without repeating the negative.

Responding to a surprise prop

The reporter attempts to hand over a report, a document, a prop, a videotape or a supposedly contaminated item (such as a glass of "contaminated" water). Avoid taking "ownership" and refuse to take or touch the item. Alternatively, accept it but quickly set it aside and out of view of cameras. React by saying, "I'm familiar with that specific report, and what I can say about the issue is…" or "I'm not familiar with that report, but what is important to keep in mind is…" and then return to your key messages.

Section 8.10 Sample Statement Regarding Non-Verbal Communication Skills

People are often highly attentive to non-verbal cues, especially in high-stress emergency situations. Non-verbal cues can be even more important than verbal communication. A list of non-verbal cues and their possible meanings is provided below. The exact meaning of the non-verbal communication will depend upon on the situation and the culture in which it occurs.

Ways of minimizing the effects of negative non-verbal messages include:

- practicing the presentation or interview with colleagues;
- asking communication experts within or outside the organization to critique non-verbal
- communication displayed in a simulated interview or news conference;
- critiquing yourself based on a videotaped practice interview.

Non-Verbal Behavior	Possible Negative Perceptions
Poor eye contact	dishonest, closed, unconcerned, nervous, lying
Sitting back in chair	not interested, unenthusiastic, unconcerned, withdrawn, distancing oneself, uncooperative
Arms crossed on chest	not interested, uncaring, not listening, arrogant, impatient, defensive, angry, stubborn, not accepting
Infrequent hand gestures/body movements	dishonest, deceitful, nervous, lack of self-confidence
Rocking movements	nervous, lack of self-confidence
Pacing back and forth	nervous, lack of self-confidence, cornered, angry, upset
Frequent hand-to-face contact/ resting your head in your hands	dishonest, deceitful, nervous, tired, bored
Hidden hands	deceptive, guilty, insincere
Speaking from behind barriers (podiums, lecterns, tables)	dishonest, deceitful, withdrawn, distancing oneself, unconcerned, not interested, superior
Speaking from an elevated position	superiority, dominant, judgmental
Speaking indoors behind a desk	bureaucratic, uncaring, removed, distant, uninvolved
Touching and/or rubbing nose	doubt, disagreement, nervous, deceitful
Touching and/or rubbing eyes	doubt, disagreement, nervous, deceitful
Pencil chewing/hand pinching	Lack of self-confidence, doubt
Jingling money in pockets	nervous, lack of self-confidence, lack of self-control, deceitful (hint: empty change from your pockets beforehand)
Constant throat clearing	nervous, lack of self-confidence
Drumming on table, tapping feet, twitching	nervous, hostile, anxious, impatient, bored
Head in hand	bored, tired, frustrated
Clenched hands	anger, hostile, uncooperative
Locked ankles/squeezed hands	deceitful, apprehensive, nervous, tense, aggressive
Palm to back of neck	frustration, anger, irritation, hostility
Tight-lipped	nervous, deceitful, angry, hostile
Licking lips	nervous, deceitful
Frequent blinking	nervous, deceitful, inattentive
Slumping posture	nervousness, poor self-control
Raising voice/high-pitched tone of voice	nervous, hostile, deceitful
Shrugging shoulders	unconcerned, indifferent

Non-Verbal Behavior	**Possible Positive Perceptions**
Excellent eye contact	honest, open, competent, caring, empathetic sincere, dedicated, confident, knowledgeable, interested
Sitting slightly forward in chair	interested, enthusiastic, concerned, cooperative
Open hands	open, sincere
Speaking outdoors in low-wind conditions	dedicated, hardworking, involved, concerned
Hand to chest/heart region	open, honest, dedicated, sincere
Erect posture	self-confident, self-controlled, assertive, determined
Lowering voice	self-assured, honest, caring

Section 8.11 Sample Statement Regarding Methods for Responding to Anticipated Questions in a Media Interview

Consider using this five step model for responding to anticipated questions in a media interview.

In your answer, you should…	**by…**
1. Express empathy and caring in your first statement	-- using words and gestures conveying authentic listening, caring, or empathy -- using a personal story -- using the pronoun "I"
2. State your key messages	-- limiting the total number of messages to no more than three messages -- limiting the total number of words used (typically less than 30 words or 9 to 15 seconds) -- using positive words -- setting the messages apart by using words, pauses, or inflections
3. Provide supporting information for your messages	-- using at least two to three supporting facts -- using analogies -- using a personal story -- citing credible third parties
4. Repeat your key messages	-- using approximately the same words used in step 2
5. State future actions	-- listing specific next steps -- providing information about where to get additional information

Section 8.12 Sample Statement Regarding Guidelines for Correcting Errors by Journalists

- Remain calm and composed when speaking to reporters or editors about errors and mistakes.
- Contact the reporter directly and point out errors only if the errors are significant. (Do not complain about trivial mistakes or omissions.)
- Ask the reporter to amend the office file copy of the story.
- Consider asking the reporter to make an appropriate change in their next story. (Note: this can be controversial and may lead to a difficult discussion with the journalist.)
- Avoid embarrassing the reporter who made an error by naming him/her during a news or press conference or briefing.
- Avoid, if possible, going to the reporter's editor or producer – this should only be done if there is a major mistake, and if the reporter will not acknowledge the mistake and make the requested correction. By going over the reporter's head you may ruin any working relationship you have developed.
- If the error occurs in the stories of several different reporters, or if the story is picked up by a wire service, and if the error is deemed major, then correct the error during the next media interview, news release, or news conference without naming the individuals responsible for the error.
- Recognize the difference between errors and differences in points of view – differences in points of view will generally not be corrected.

Section 8.13 Sample Statement Regarding News Releases

The news release is a short, written summation detailing facts and viewpoints. It is nearly always written by the organization involved with, or affected by, the event. The news release's primary intended audience is reporters covering the incident who will use the information to write a story. Once received by reporters, the news release may be printed, broadcast, or uploaded verbatim or nearly verbatim, used only as a reference by the reporter, or ignored completely.

News releases should follow the following guidelines

1. Format your news release using the standard format for producing a news release (see Section 8.14). Reporters and editors are more likely to read the release if it uses the standard news release format and contains information about who, what, where, when, why, and how.

2. Your release should go on your organization's letterhead, preferably with your logo.

3. At the top left hand side of the page, or in the top center, write in bold-face the words "**PRESS RELEASE**" or "**NEWS RELEASE**" in all capital letters or with the first letter of each word in capital letters.

4. Move down two lines. Write in bold-face "**For Immediate Release:**" in all capital letters or with the first letter of each word in capital letters.

5. Next to, or immediately below the words, "**For Immediate Release:**" put the date of the release.

6. Immediately below, or to the right of, "**For Immediate Release:**" write the word "**Contact:**" or "**Contact Information:"** in bold-face. Next to this write a contact phone number that reporters may call for additional information. Some organizations add the name of a contact person, the name of a department, and an email address. If this option is chosen, the contact person should be your organization's public information officer or spokesperson.

7. Two lines below the date and contact information put your headline. Your headline should be bold, in a larger font, with the first letter of each word capitalized. Some organizations prefer to center the headline. The headline should be a brief summary (no more than two to three lines) of what your news release is about. It needs to be informative and grab the attention of the reporter or editor. Keep in mind journalists receive many news releases each day. The headline should be clear, to the point, and encourage the reader to read the rest of the release. You can include a subheading to provide more information and entice the reader to read on.

8. Two lines below your headline insert the name of the town or city where the release is coming from, followed by a dash. This is called the dateline. You can boldface the city if you choose. (for example, **Washington, DC -**)

9. After the dateline is where your text begins. The first paragraph of your release should be brief and include information pertaining to who, what, where, when, why, and how. Everything you want the reader to know quickly should be in this paragraph.

10. You should double-space your text and use a 12 point font, such as Times New Roman or Arial. Some organizations indent paragraphs. Others do not. Leave plenty of white space in your press release. Use ample margins around your page.

11. The remaining paragraphs of the release should provide information you believe will interest the reader.

12. Your next to last paragraph should be similar to your first paragraph.

13. Your last paragraph should state: "For more information, call..." or "Visit our Web site at www… for information materials." You should direct the reader to a place where they can get more information on the issue.

14. A couple of spaces below your final paragraph, centered on the page, put "###".This signifies the end of your release.

15. At the end of the release (after your last paragraph and before the ###), consider including a couple of sentences about your organization. This can include what your

organization's mission is or what your organization is tasked to do. At the end of the description, refer the reader to your organization's Web site.

16. If the news release goes beyond one page, then include the word "- **MORE -**" or "-more -" under the last line on the first page. Some organizations write this word in capital letters and use bold-face. Others do not.

17. If the news release goes on to a second page, write the headline, or a shortened version of the headline, and "Page 2."

18. Keep your sentences short with an occasional longer sentence to break the monotony.

19. Keep the news release brief. Keep it to no more than two pages and to the point. Refer readers to a phone number or Web site they can go to for additional information.

20. Present only facts; leave out editorializing.

21. Avoid using acronyms, jargon, and technical language.

22. **Have a least one communicator and one subject matter expert proofread the news release.** A pair of "fresh" eyes may catch mistakes you missed. A major typo or mistake can discredit your release. Most people have trouble proofreading their own writing. Ask a colleague to proofread it for you.

23. If it's a local event or topic, indicate the name of the town or city in the headline. This will increase the likelihood the local media will pick up the story.

24. Include in the news release authentic statements of empathy, caring, and compassion, especially when there is high concern, high stress, or harm to people, property, or the environment. It is typically best for these statements to come from a senior leader of the organization. The statements should be set off with quote marks. For example, "Our thoughts and prayers go out to the employees injured in this accident and to their families" stated [insert name of senior official]. Or, "I know many people are worried and concerned about events happening at the facility. As a community, I believe we can make it through this difficult time," stated [insert name of senior leader].

25. Make sure your release is clear and simple.

26. Perform a readability test to ensure the news release is between the sixth and eighth grade reading-level.

27. Some online news services require a summary of your news release. This is because some media outlets will distribute only your headline, summary, and a link to your news release.

28. Make sure your release gets all of the organizational clearances and approvals needed.

29. Make sure you share your release with partners for vetting before releasing to the media.

Section 8.14 Sample Statement Regarding the News Release Format

The news release should following the format provided below.

[Organization's name on letterhead with logo]

News Release

For Immediate Release: [Insert date]
Contact: [Insert name of media representative]
[Insert name of organization]
[Insert telephone number]
[Insert fax number]
[Insert email address]
[Insert after-hours telephone number]
[Insert Web site]

[**Insert headline here, bold-faced, with the initial letter of each word in capital letters]**

[**City, State**] – [Insert Date] – [Text goes here, often double-spaced with indented paragraphs]

[First paragraph: short (less than 30 words), containing the most important information]

[Second, third, fourth …paragraphs: short, containing supplemental information. Try to include a quote from leadership within the first few paragraphs]

If the news release is more than one page long, insert the following:

– more –

Center the word at the bottom of the page, then continue onto the next page with a shortened headline and page number as follows:

[Insert shortened headline] – Page 2

[Next to last paragraph: similar to your first paragraph]

[Last paragraph: put "For more information, call..." or "Visit our Web site at www….for information materials."]

Put at the end of the release:

End

Alternatively, put at the end of the release:

###

Place "End" or "###" on the left or centered. This lets the reporter or reader know they are at the end of the news release.

==========

Section 8.15 Sample Statement Regarding the Content of a News Release

The purpose of the news release is to answer the basic questions: who, what, where, when, why, and how. This requires the news release to be at least several paragraphs in length.

First paragraph: Provide two to three short sentences describing the current situation. This paragraph addresses questions relating to who, what, where, why, when, and how.

_____
_____
_____

Next paragraph (optional): Provide a quote from an official or senior manager demonstrating leadership and expressing caring. This paragraph should address the question, "Why is this issue or event important?"

_____
_____
_____

Next paragraph (Optional): Provide information on actions that are being taken.

_____
_____
_____

Next paragraph (Optional): Provide information on actions that will be taken.

_____
_____
_____

Next paragraph (Optional): Describe coordination activities with your emergency response partners.

_____
_____
_____

Section 8.16 Sample Statement Regarding the Organizational Web Site

The [Insert Name] will maintain a Web site for the public and an internal Web site for employees http://. The [Insert Name] may also establish specialized Web sites for specific groups (for example, for the media, health care professionals, or emergency responders). The Web site will include a page with updated emergency risk information. The Web site team will post on the Web site press releases, fact sheets, advisories, and other information in a timely fashion.

Section 8.17 Sample Statement Regarding Call Center/Hotline Services/Telephone Messaging

The [Insert Name] will establish call centers/hotlines for public and employee inquiries. The [Insert Name] may also establish specialized call centers/hotlines for specific groups (for example, for the media, health care professionals, public officials, reception centers, or first responders). The call centers will have the capacity to handle a large number of inquiries. The [Insert Name] call centers will have a toll free number.

The public and employee call centers/hotlines operating out of the Joint Information Center will have the capacity to handle approximately [insert number] incoming telephone calls. In case of a surge, pre-established agreements or contracts to increase capacity will be implemented.

The call centers/hotlines will supplement the public access telephone line [insert telephone number] and employee access telephone line [insert telephone number]. Calls to these numbers during an IED attack will be screened (via an automated phone system or staff who cover the line) and transferred to the call centers/hotlines if needed.

Section 8.18 Sample Statement Regarding the Use of Other Media, Including Social Media

People immediately affected by an IED attack will use a variety of sources to obtain information. In an addition to friends, neighbors, relatives, and traditional media outlets (radio, television, newspapers, and magazines), people will use many other sources of information. Several examples are provided below. (Additional information regarding sources of information can be obtained in the document "Emergency Support Function 15: External Affairs Standard Operating Procedures." Department of Homeland Security. January 2009. Annex R.)

1. Text Messaging

Text messaging, or texting, is a colloquial term referring to the exchange of brief written messages between mobile phones, over cellular networks. While the term most often refers to messages sent using the Short Message Service (SMS), it has been extended to include messages containing image, video, and sound content. Individual messages are referred to as "text messages" or "texts". Text messaging is available on most digital mobile phones and many personal digital assistants (PDAs).

The most common application of text messaging is person-to-person messaging. However, text messages can also be sent to and from automated systems.

2. Twitter

Twitter is a free social networking service that allows users to send information or updates to others with short messages, not exceeding 140 characters. Twitter requires an account be established.

Twitter is similar to text messaging. What makes Twitter different is it allows users to follow comments made by another person or organization. Whenever a person signs up

"to follow" somebody on Twitter, they are able to instantly receive updates from that person, or organization. It is this feature of Twitter that makes Twitter and similar social networking systems potentially useful for emergency risk communications. For example, the technology allows users to send status updates via their cell phone, laptop, PDA (personal digital assistant), smart phone, or other mobile devices.

Messages sent through Twitter are broadcast in "real time" to followers. Twitter can be accessed from anywhere electronic signals can be received.

Twitter is capable of handling a large amount of traffic. "Followers" can be targeted, such as residents within the 10 mile Emergency Planning Zone. Use is initiated by entering a url (Web page address) in the Twitter profile or by sending the url to followers. Messages are called "Tweets." The number of Tweets person receives from Twitter is directly proportional to number of followers a person has. An additional feature of Twitter is TwitterFeed. TwitterFeed can automatically send titles of updates to users.

One potential use of Twitter, and similar technologies, is that they allow users to access help quickly by posting questions or requests. For example, a Twitter user can post an urgent request such as, "I need urgent help on …". In a matter of minutes, help can be offered. Twitter users can also post the latest news related to an event or answer questions from concerned co-workers, families and friends.

Twitter has the potential to assist communicators in performing a variety of other emergency communications tasks. For example, it can be used as a tool for collecting live feedback from people engaged in emergency response activities. Twitter messages can also be monitored for rumors.

As with any new technology, Twitter has the potential for abuse and misuse, including possible security concerns. However, Twitter has communication features that can add substantial value to emergency risk communications.

3. Wikipedia

Wikipedia is a free, web-based, collaborative, multilingual encyclopedia project supported by the non-profit Wikimedia Foundation. Wikipedia contains over 13 million articles (three million in the English Wikipedia). The articles have been written collaboratively by volunteers around the world. Almost all of its articles can be edited by anyone with access to the site. It was launched in 2001 and is currently the largest and most popular general reference work on the Internet.

Critics of Wikipedia have questioned (1) its reliability and accuracy; (2) its susceptibility to vandalism; (3) its susceptibility to the addition of spurious or unverified information; and (4) its departure from the expert-driven model of encyclopedia building. Wikipedia currently serves both as a popular Internet encyclopedia and as a source of updated news about events.

4. Social Networking

Social networking such as Facebook, MySpace, and LinkedIn are internet sites that allow users to connect online to one other. Most social networking sites require members to be

invited or accepted into the network. The power of these sites during an emergency was vividly demonstrated during the shootings at Virginia Tech. For example, student Facebook users posted real-time updates on victims more rapidly than information communicated through traditional communications channels.

5. Video and Photo Sharing

Sites such as YouTube (video sharing), Flickr and Picassa (photo sharing) allow users to send video or still images during an emergency.

6. Podcasts

Pod casts are video or audio clips that are made available to users. The audio or video file is uploaded to a server and made available to users. Users can download the file to their personal computer or audio device. Podcasts can be used for the broadcast or rebroadcast of news conferences, speeches, instructions, or other information.

7. Blogs

Blogs offer opportunities for an organization to give stakeholders a place to go to hear commentary by the organization on particular news stories or to check facts being reported by the media. A blog is a type of Web site maintained by an individual or organization with regular entries of commentary, descriptions of events, or other material such as graphics or video. There are currently millions of blogs. Entries are commonly displayed in reverse-chronological order. The ability for readers to leave comments in an interactive format is an important part of many blogs.

8. Other Media

Other media that should to be considered include video news releases, audio news releases, virtual worlds (a computer-based, simulated environment, such as Second Life, in which users interact with each other through virtual representations of themselves), internet forums, message boards, and any other source of information people may use in an emergency. Holding constant all other variables, the more channels for delivering messages to users, the more effective the emergency risk communication will be.

Section 8.19 Sample Statement Regarding Communicating with Special Needs Populations

(Source: Emergency Support Function 15, External Affairs Standard Operating Procedures, Section 1 to Annex E. Department of Homeland Security. January 2009.)

A special team should be activated in an IED attack to communicate with audiences who are not likely to receive messages through mass media channels. Based on the nature of the IED attack, the team should identify the most effective method for reaching out to these special populations. The team should work closely with partner organizations to communicate effectively with these populations. The team should also, if needed, identify vendors who can provide special specialized services, such as translation or sign language services.

Individuals with special communication needs make up a sizeable portion of the U.S. population. Before, during, and after an IED attack, members of these populations may need additional information related to topics such as transportation, supervision, and medical care.

Special needs populations include, at a minimum, individuals who:

- have disabilities;
- live in large group settings;
- are elderly;
- are children;
- are from diverse cultures and/or have limited English proficiency (or are non-English speaking;
- are transportation disadvantaged.

The provision of timely and potentially lifesaving information to members of these populations before, during, and after an IED attack must be ensured.

1. Planning Assumptions for Communicating to Special Needs Populations

To effectively communicate to special needs populations, members of the special populations team should:

- have a sound working knowledge of accessibility and nondiscrimination requirements applicable under Federal disability and civil rights laws;
- be familiar with the demographics of the population of people with special needs who live in their community;
- engage in efforts to remove communication barriers faced by members of the special needs populations within the affected area;
- involve a variety of people from the special needs population in identifying communication needs during an emergency;
- identify existing, and develop new, resources within the community.

2. **Strategies for Communicating with Special Needs Populations**

The needs of each special population must be considered. For example, Federal civil rights laws require equal access for, and prohibit discrimination against, people with disabilities in all aspects of emergency planning, response, and recovery. Equal access applies to emergency information pertaining to:

- preparedness;
- notification of emergencies;
- sheltering in place;
- evacuation;
- transportation;
- communication;
- shelters;
- distribution of supplies;

- food;
- first aid;
- medical care;
- housing;
- application for and distribution of benefits.

Preparations need to be made for individuals with a variety of limitations, including individuals who are deaf, hard of hearing, have speech impairments, or need information presented in a visual format. Auxiliary aids and services may be needed to ensure effective communication. These may include closed captioning, pen and paper, or sign language interpreters through on-site or video interpreting.

Individuals who are blind, have low vision, or have cognitive disabilities may need information presented in an audio format, materials in large print, or people to assist with reading and filling out forms.

Service animals have access to the same facilities and evacuation assets as the humans they service, under the Americans with Disabilities Act of 1990.

Additionally, steps need to be taken to ensure persons with limited English proficiency have meaningful access to communication regarding programs, services, and information provided to the general public. Individuals who do not speak English or have limited English proficiency may need information in a language other than English, or an interpreter who can relay information to them.

Given these considerations, it is essential when communicating information before, during, and after an IED attack to ensure:

- respect for the civil rights of ethnically diverse populations;
- coordination and collaboration with experts on Civil Rights;
- use of communication methods reflecting cultural competence;
- use of specialists in cultural competence to assist in disseminating information;
- use of communication staff, whenever possible, familiar with the culture of the affected special needs population.

9.0. JIC Structure

An ERC/JIC plan should include a section describing the Joint Information Center. Samples statements regarding the structure of a Joint Information Center can be found in the following Sections.

Section 9.1 Sample Statement Regarding Establishing a Joint Information Center (JIC)

A Joint Information Center (JIC) is:

> a central point for coordination of incident information, public affairs activities, and media access to information regarding the latest developments. In the event of incidents requiring a coordinated Federal response, JICs are established to coordinate Federal, State, tribal, local, and private-sector incident communications with the public.
>
> (Public Affairs Support Annex PUB-1, Department of Homeland Security, January 2008, http://www.fema.gov/pdf/emergency/nrf/nrf-support-pa.pdf)

The Joint Information Center concept evolved with the Incident Command System (ICS). ICS established a clearly defined management scheme for responding to disasters and emergencies. After the Department of Homeland Security was created, it became a requirement that all first responder organizations implement the ICS in all security-related incidents.

Two types of Joint Information Centers should ideally be established to effectively deal with the communication challenges posed by an IED attack: an Incident Joint Information Center, or I-JIC, and a Virtual Joint Information Center, or V-JIC.*

---

* Other types of JICs include:

- **Satellite JIC**: A Satellite JIC is typically smaller in scale than an Incident JIC. A Satellite JIC is established to provide flexible capability for timely release of information. A Satellite JIC may also be established to support a specific news event.
- **Area JICs**: Area JICs are established when multiple JICs are operating in support of the same or related incidents and jurisdictions. Area JICs are typically used when there are multiple field offices supporting the Incident Command System structure. Coordination between the Area JICs is important to ensure mutual awareness and consistency in messaging and public instructions among all participants.
- **National JIC**: A National JIC is activated when an incident requires a coordinated Federal response. Incidents of great magnitude with high media interest may require Federal coordination, especially incidents of long duration or that affect a large area of the country.

Section 9.2 Sample Statement Regarding Establishing an Incident Joint Information Center (I-JIC)

An Incident Joint Information Center (I-JIC) is a physical location where public affairs representative from organizations involved in the response work together to respond to media inquiries and perform other public affairs functions. The I-JIC serves as a focal point for the coordination and dissemination of emergency risk information to the public, media, employees, pubic officials, response organizations, and other stakeholders during an IED attack.

The I-JIC should be located close to the site of the emergency but not so close as to pose a risk to the participants. It is typically located outside the 10 mile Emergency Planning Zone (EPZ). The location may change depending on the requirements of the emergency. In most cases, the I-JIC is established at, or is virtually connected to, the Emergency Operations Center.

Section 9.3 Sample Statement Regarding Functions of an Incident Joint Information Center (I-JIC)

In an IED attack, the I-JIC serves as the focal point for all public affairs activities and media access. The I-JIC remains in operation for as long as the situation warrants. The I-JIC is designed to handle communication on a larger scale than could be effectively managed by a single organization. The I-JIC can be expanded or contracted to meet the needs of the emergency.

All emergency response and partner organizations are encouraged to participate in, and share the resources of, the I-JIC. If participation is not feasible, the non-participating organization is encouraged to coordinate all communication activities with the I-JIC.

Through the I-JIC, (1) information can be provided to the media, the public, and other stakeholders in a timely and consistent fashion; and (2) organizations involved in managing and responding to the emergency can work together in a cohesive manner and respond with coordinated messages. By maintaining a centralized communication link, the I-JIC helps ensure communication resources are managed well and duplication of effort is minimized. The use of an I-JIC also allows for tracking and maintaining records. These records can later be analyzed and evaluated to improve performance.

All participating organizations in an I-JIC may continue to use their own mechanisms for releasing emergency risk information. However, all releases of information should be coordinated with the I-JIC

The I-JIC should be led by the lead organization's Public Information Officer (PIO). The lead organization's PIO must ensure that these primary I-JIC functions are effectively performed:

- gather incident data;
- obtain verified, up-to-date information from appropriate sources;
- inform the media and the public about the event and about personal protective actions;

- serve as the primary source of understandable, timely, accurate, consistent, and credible information about the incident, the response, and the recovery effort;
- identify potential issues or problems that could have an impact on the response and recovery effort;
- employ techniques for obtaining feedback from the media, the public, and selected target audiences regarding response and recovery efforts.

The primary emergency risk communication activities of the I-JIC are:

- hold news conferences;
- issue news releases;
- respond to media requests for interviews;
- respond to inquires from the media, the public, and other interested parties;
- produce emergency risk communication materials.

Other I-JIC activities include:

- notify the media that the JIC has been activated;
- hold briefings for JIC staff members;
- hold briefings for partner organizations;
- establish mechanisms to ensure coordinated information;
- develop approved fact sheets, core messages, message maps, talking points, media kits, and other background material;
- identify trends in media reporting;
- identify and responding to rumors and misinformation;
- monitor the physical and mental wellbeing of the JIC staff and the JIC staff's family members;
- monitor media and public interest in the situation;
- write situation assessment reports.

Section 9.4 Sample Statement Regarding Logistics of an Incident Joint Information Center (I-JIC)

A typical I-JIC includes the following work areas.

- I-JIC staff work area
- Media briefing area/news conference room
- Media monitoring area
- Media registration area and security
- Work area for journalists, including break room and restroom facilities
- Work area for spokesperson(s)
- Storage area
- Work area for telephone hotline/call center teams
- Break room and restroom facilities for JIC staff

Sufficient workspace should be reserved for staff and equipment.

- Staff members responsible for handling inquires from the media, the public, and key stakeholders
- News release writers
- Supervisors
- Staff members who to collect, collate, and review news releases, fact sheets, and other emergency risk communication materials
- Staff members who conduct media monitoring activities
- Status boards
- Maps
- Copiers, computers, projectors, flip charts, white boards, printers, and fax machines

Additional space that is separate but convenient to the other workspaces is needed at an I-JIC for (1) news conferences and (2) a work area for reporters. The news conference room needs to be large enough to accommodate a large number of newspaper, television and radio reporters, as well as photographers, and camera crews.

I-JIC personnel arriving at the facility should enter through a designated entrance. Each I-JIC staff member should be required to sign a log sheet at the I-JIC staff registration desk and get an I.D. badge or name tag. The I-JIC operations manager should provide a copy of the roster to the facility security for subsequent check-ins.

Equipment and supplies needed at an I-JIC may vary with location. At a minimum, computers, fax machines, and adequate power outlets and telephone lines should be available. Provided below is a checklist of I-JIC equipment and supplies. The I-JIC should have secure internet access and secure wireless routers to serve staff and the media.

9.4.1 Checklist of Equipment and Supplies for I-JIC Staff Work Areas

Equipment

- ❑ Fax machine (with pre-programmed numbers for fax releases to media and partners)
- ❑ Telephones
- ❑ Computers (with internet capability and loaded with e-mail distribution lists and other communication materials)
- ❑ Laptop computers (with internet capability and loaded with e-mail distribution lists and other communication materials)
- ❑ Printers for every computer
- ❑ Copiers
- ❑ Tables and chairs
- ❑ Cell phones/pagers/personal data devices
- ❑ Visible calendars
- ❑ Message boards
- ❑ Refrigerator and microwave
- ❑ Conference tables
- ❑ Color copier

- ❑ A/V equipment
- ❑ Flow charts, bulletin boards, status boards
- ❑ Area maps
- ❑ Flip charts and easels
- ❑ Podium for news conference rehearsals
- ❑ TVs with cable hookup
- ❑ Portable microphone
- ❑ Extension cords
- ❑ VHS VCR Player
- ❑ CD–ROM/DVD Player
- ❑ Secure wireless router(s)
- ❑ Secure network access devices(s)
- ❑ Thumb (Flash) drives
- ❑ **Other**

Supplies

- ❑ Paper shredder
- ❑ Badges for JIC staff members and sign in log sheet
- ❑ Copier toner
- ❑ Printer ink
- ❑ Paper
- ❑ Pens and pencils
- ❑ Markers
- ❑ Highlighters
- ❑ Erasable markers
- ❑ Overnight mail supplies
- ❑ Sticky notes
- ❑ Tape
- ❑ Notebooks
- ❑ Poster boards
- ❑ Standard press kit folders
- ❑ Organized B-roll in beta format (keep VHS copies available for meetings)
- ❑ Formatted computer disks
- ❑ Telephone directories
- ❑ Color-coded everything (folders, inks, etc.)
- ❑ Baskets (to contain items you're not ready to throw away)
- ❑ Organizers to support your clearance and release system
- ❑ Expandable folders (with alphabet or days of the month)
- ❑ Staplers (lots of them)
- ❑ Paper punch
- ❑ Paper cutter
- ❑ Three-ring binders
- ❑ Organization's logo on a sticker
- ❑ Colored copier paper

- ❑ Paper clips (all sizes)
- ❑ Other

9.4.2 Checklist of Equipment and Supplies Checklist List for I-JIC News Conference and Media Work Areas

News Conference Room

- ❑ Projector
- ❑ Back up projector and/or extra projector bulb
- ❑ Computers
- ❑ Easels
- ❑ Flip Charts
- ❑ Emergency status signs
- ❑ I-JIC podium sign
- ❑ Public address system (podium microphone, portable microphones, microphone feed box)
- ❑ Lectern
- ❑ Lighting
- ❑ Table and chairs for speakers
- ❑ Printers
- ❑ Table for computer
- ❑ Area maps
- ❑ Name plates for speakers
- ❑ **Other**

Media Registration Area

- ❑ Desks with chairs
- ❑ Media directories
- ❑ Badges for media representatives
- ❑ Sign-in log/registration sheets
- ❑ **Other**

Work Area for the Media

- ❑ Telephones
- ❑ Telephone directories
- ❑ Multiple electrical outlets
- ❑ Extension cords
- ❑ Desks/chairs or tables/benches to accommodate several reporters
- ❑ Internet access
- ❑ Copiers
- ❑ Fax machines
- ❑ Printers
- ❑ Break room and restroom facilities

- ❑ **Other**

Section 9.5 Sample Statement Regarding Staffing of an Incident Joint Information Center (I-JIC)

Under normal operations, the I-JIC typically uses two 12-hour shifts or three eight-hour shifts. Depending upon the level of the emergency and the extent of media interest, the I-JIC lead Public Information Officer and operations manager may elect to suspend most I-JIC operations during non-business hours, typically overnight. However, a duty officer and support staff should be available 24/7 to respond to calls, monitor media reporting, and perform other duties as needed. A telephone based menu with information updates can also be used to receive calls.

The I-JIC operations manager is responsible for determining shift changes. The administrative support supervisor is responsible for informing staff of the time for shift changes and ensuring shift changes take place.

During a shift change, incoming JIC members should:

- Arrive 30 minutes prior to shift change;
- Sign in and receive badges;
- Participate in a briefing by the Public Information Officer or designee.

Outgoing shift members should:

- Brief incoming shift members;
- Turn over logs, notes and other pertinent data;
- Sign out and turn in badges.

At maximum capacity, an I-JIC can be very large. As shown in the following checklist, many job positions may need to be filled.

<u>I-JIC Staffing: Checklist of Positions</u>

- ❑ Administrative Support Coordinator
- ❑ Administrative Support Staff
- ❑ Assistant Lead Public Information Officer
- ❑ Audiovisual Production and Support Team Leader and Members
- ❑ Elected Officials Hotline/Call Center Team Leader and Members
- ❑ Emergency Responders Hotline/Call Center Team Leader and Members
- ❑ Employee Liaison Officer
- ❑ Employee Family Liaison Officer
- ❑ Facility Operations Manager
- ❑ Facility Operations Deputy Manager
- ❑ Government Liaison Officer
- ❑ Lead Public Information Officer
- ❑ Legal Counsel
- ❑ Media Hotline/Call Center Team Leader and Members

- ❑ Media Monitor Team Leader and Members
- ❑ Media Registration Coordinator
- ❑ Medical Professional Hotline/Call Center Team Leader and Members
- ❑ Mental Health Advisor
- ❑ News Conference Room Manager
- ❑ News Conference Room Manager Assistant
- ❑ Non-Lead Public Information Officers
- ❑ Partner Organizations Liaison Officers
- ❑ Public Hotline/Call Center Team Leader and Members
- ❑ Reception Centers/Congregate Care Centers Liaison Officers/Coordinators
- ❑ Researchers
- ❑ Security Team Leader and Officers
- ❑ Special Needs Population Liaison
- ❑ Spokespersons
- ❑ Staff Support Team Members
- ❑ Technical Advisors
- ❑ Technical Hotline/Call Center Team Leader and Members
- ❑ Web Site Manager/Webmaster
- ❑ Writers

Every position does not to be filled. Positions can be combined or eliminated depending on the needs of the situation.

Position assignments should be made in advance with people trained in performing the task. Because of shift work and absenteeism, ideally at least two to three persons should be available to perform the functions associated with each position.

Section 9.6 Sample Statement Regarding News Conferences Conducted at an Incident Joint Information Center (I-JIC)

One of the primary means for the I-JIC to communicate with the media during an IED attack is the regularly scheduled news conference. The lead Public Information Officer, in coordination with partner organizations, should establish the schedule of news conferences.

During a major IED attack, there should be a minimum of two to three news conferences each day. News conferences should continue to be held for as long as the size of the media contingent covering the event warrants. News conferences should be scheduled to help reporters meet news deadlines. Many deadlines have become shorter due to modern communications technology. In some cases, reporters ask questions or ask for comment seconds or minutes after the event has occurred.

Although the specific times for news conferences vary by situation and location, a typical daily news availability schedule may be as follows:

- morning news conference;
- afternoon news conference;

- evening news conference.

If an IED attack occurs during the evening or early morning, every effort should be made to hold the first news conference before noon to meet media deadlines. If the emergency happens in the late morning or early afternoon, every effort should be made to conduct the first news conference before 3 p.m. It should be noted, however, that the time needed by the media for preparation and editing has decreased due to digital connections, internet streaming video, and other technologies.

News conferences should be scheduled to fill media voids. Frequent media briefings or news conferences are highly recommended. If there is no new information on the emergency to report, the briefing or news conference can be used to present information or provide answers to more detailed questions about science, technology, a process, or a procedure being used by response teams. Alternatively, the news briefing or conference can be used to present information or answer questions about the activities, processes, and technologies being used by partner organizations.

If there is no new news to report, it is useful to alert the media to this fact and inform them about the agenda in advance. The reporter can then decide to attend or not.

Prior to each news conference, the news conference room manager should advise the media of the briefing protocol. The room manager should also provide information on facilities and services available to reporters.

At the news conference, spokespersons from the involved organizations should provide statements, update information, and be available to respond to questions. Presentations, if made, should be kept brief – typically no more than three to seven minutes each. Selected experts should be available during each news conference to respond to questions or provide additional details as needed.

A summary of each news conference should be prepared by a designated staff member. This summary should be provided to all I-JIC members and all spokespersons.

At least 30 minutes before each news conference, the lead Public Information Officer should meet with those who will participate in the news conference. The following agenda items should be discussed at the pre-meeting:

- the opening statement;
- the order of presenters;
- time allocated for each presenter;
- anticipated questions;
- handling of questions;
- the use of visual material;
- the closing statement.

Between news conferences, a list of anticipated questions should be developed by the I-JIC communications staff. Responses to the questions should be reviewed, discussed, and rehearsed before the news conference.

Additional guidelines for conducting a news conference can be found in previous sections of this document.

Section 9.7 Sample Statement Regarding I-JIC Media Advisories and News Releases

One of the primary means for the I-JIC to communicate to the media during an IED attack is through news releases. News releases are described earlier in this document. Samples of I-JIC news releases and related materials can be found in the appendices. The lead Public Information Officer or designee, in coordination with partner organizations, should review and approve all news releases.

Section 9.8 Sample Statement Regarding Personal and Professional Characteristics of the Lead Spokesperson

In almost all emergencies, a designated lead spokesperson is a necessity. The public and media tend to like and trust a familiar face and voice. The image or voice of the lead spokesperson is often the first message an organization sends out during an emergency. Having a lead spokesperson also simplifies information flow and promotes consistency in message content.

To be effective, the lead spokesperson must:

- possess excellent media skills;
- have sufficient authority or expertise to be accepted as speaking on behalf of the organization;
- possess or work to develop good professional relationships with important members of the media and other important partners and stakeholders;
- be able to learn quickly;
- respond to sensitive questions within his/her area(s) of expertise in a professional and sensitive manner;
- effectively respond to hostile questions;
- stay on message yet remain flexible and able to make decisions quickly offer examples, anecdotes and stories;
- provide effective on-the-spot responses to media enquiries;
- express technical knowledge or complex information in a way that can be easily understood by journalists and by the average person;
- remain calm and composed at all times;
- express caring, listening, empathy and compassion;
- work well under pressure or high emotional strain;
- accept constructive feedback;
- share the spotlight;
- call on the expertise of others;
- express thanks to others and share praise;
- take responsibility for things that go wrong;
- present the appropriate tone for the audience;
- defer, delegate, and redirect questions to others as needed;
- be
    - perceived as authoritative and credible by stakeholders, partners and the public;

- at ease with the media;
- knowledgeable (generally and specifically) about the emergency, its dynamics and its management;
- a subject-matter expert on the event or able to delegate to subject-matter experts;
- resourceful.

- Even while under intense pressure and stress, the lead spokesperson must be able to:
  - stay on message;
  - avoid straying intentionally or inadvertently from prepared points;
  - use bridging techniques, if needed, to re-direct the conversation.
  - Only those things appropriate for quotes should be expressed, even in jest. There is no such thing as "off the record". The lead spokespersons must be continually aware of the potential media pitfalls outlined in the section on media interviews in this guidance document.

Section 9.9 Sample Statement of Skills Needed by the Lead and Other Spokespersons

During an emergency, the lead spokesperson and other spokespersons are the public face of the organization. In order to deal effectively with the media during an IED attack, the following skills are needed.

Listening Skills

- Listen to, acknowledge and respect fears and anxieties.
- Remain calm and in control, even in the face of fear, anxiety and uncertainty.
- Offer authentic statements and actions that communicate compassion, conviction and optimism.
- Provide people with ways to participate, protect themselves, and gain or regain a sense of personal control.

Presentation Skills

- Focus on what is known.
- If a question cannot be answered immediately, share information about what follow-up actions will be taken and where to get additional information.
- Be honest, candid, transparent, ethical, frank and open.
- Remember first impressions are lasting impressions – they matter.
- Avoid humor because it can be interpreted as uncaring or trivializing the issue.

Messaging Skills

- Be extremely careful in saying anything that could be interpreted as an unqualified absolute, for example, "never" or "always". It only takes one exception to disprove an absolute.
- Balance bad news with three or more positive, constructive, or solution-oriented messages.

- Avoid mixed or inconsistent verbal and non-verbal messages.
- Demonstrate media communication skills (verbal and non-verbal) including avoidance of major traps and pitfalls – for example, speculating about extreme worst-case scenarios, saying "there are no guarantees," repeating negative words used in allegations or accusations, or saying "no comment."
- Develop and offer three concise key messages in response to each major concern.
- Continually look for opportunities to repeat the prepared key messages.
- Use clear non-technical language free of jargon and acronyms.
- Make extensive but appropriate use of visual material, personal and human-interest stories, quotes, analogies and anecdotes.
- Find out who else is being interviewed and make appropriate adjustments.
- Monitor what is being said by others.
- Avoid attacking the credibility of those with higher perceived credibility.
- When possible, use research to help determine responses to messages.
- Acknowledge uncertainties and challenges.

Organization Skills

- Plan emergency risk communications programs well in advance, conduct scenario planning, identify important stakeholders, anticipate questions and concerns, train spokespersons, prepare messages, test messages, anticipate follow-up questions and rehearse responses.
- Provide information on a continuous or frequent basis.
- Ensure partners (internal and external) respond with coordinated messages.
- Have a contingency plan for when partners (internal and external) disagree.
- Plan public meetings carefully – unless they are carefully controlled and skillfully implemented they can backfire and result in increased public outrage and frustration.
- Encourage the use of face-to-face communication methods, including sessions with experts, workshops, and poster-based information exchanges.
- Ensure facts offered have gone through the appropriate clearance process.

Leadership Skills

- Be the first to share bad or good news.
- Be highly visible.
- Be readily available to speak.
- Take the first day of an emergency very seriously – drop other obligations.
- Take ownership of the issue or problem; avoid blaming others.
- Avoid guessing – check and double-check the accuracy of facts.
- Be able to cite other credible sources of information.
- Admit when mistakes have been made – be accountable and responsible.
- Seek, engage and make extensive use of support from credible third parties.
- Lead the way by example.

Section 9.10 Guidelines for Establishing a Virtual Joint Information Center (V-JIC) for an IED attack.

The primary purpose of a Virtual Joint Information Center (V-JIC) is to link participants who cannot physically come to the physical Joint Information Center because of geographical restrictions, transportation problems, incident management requirements, or other limitations. The Virtual Joint Information Center (V-JIC) links participants through technological and electronic means. Depending on the type of information being shared, links among participants in the V-JIC can be set up to be secure or non-secure.

The V-JIC allows participants to coordinate messages. It can be used to improve upon, add to, or replace most of the activities that take place at an Incident Joint Information Center.

As many authors have observed, we now live in an era of instant news. Audiences want, and are receiving, news about what is happening almost immediately. Even traditional printed news sources, such as newspapers, are now maintaining Web sites and blogs. Stories appearing on newspaper Web sites are now competing with radio and television outlets and other Web sites for immediacy. The Internet means that media organizations can now put out information quickly in a variety of formats for a global audience.

In almost every major event, audiences go directly to the source of the news if they have a high interest. Examples of organizations experiencing this phenomenon are frequent. For example, on September 11, 2001, CNN's Web site registered 11 million hits. In the years since, the number of users accessing Web sites for news has increased significantly.

In the US there are millions of Internet users who connect with the Internet every day to get news. When a major event occurs, such as an IED attack, the Web sites of emergency response organizations will likely be inundated with millions of hits. The Web sites of emergency response organizations will likely serve as a primary source of information for reporters, members of the public, family members of those involved, key government officials, and others. Users will expect the information provided on the web site to be complete, accurate and up-to-the-minute. Users can also now witness first-hand what is happening as it happens.

As Gerald Baronet, an expert in emergency management has noted on his web site, a V-JIC addresses the four primary problems identified with the traditional JIC:

1. Assembly of responders
2. Participation of those not present
3. Lack of infrastructure
4. Web site management and infrastructure

1. Assembly of Responders

Members of the V-JIC can become operational in the time it takes to get to a computer with an Internet connection. That means their office, their car, or a hotel room. After signing in with a pre-authorized password, team members can immediately participate in information preparation and approvals, response to inquiries, tracking news reports and

scheduling upcoming news conferences. Any authorized user can distribute approved information via email, fax or using text-to-voice telephone messaging.

It is essential in a V-JIC operation that several members of the V-JIC be physically present at the Joint Information Center. For example, the Public Information Officer should be present to work and confer directly with the Incident Commander/Unified Command. JIC staff members need to be available to respond to and escort members of the media who may arrive on scene.

Use of the V-JIC can reduce the number of reporter inquiries. When reporters find they can get the information they need delivered directly to their computers or digital devices, their need to visit the scene or the I-JIC is lessened. The option of submitting questions via the Web site further reduces the need for calls or visits, providing the inquiries receive a fast response.

2. Participation of Those Not Present

Barone, Atkins, and other experts in Joint Information Centers have pointed out that V-JIC membership is not limited to those physically present. Membership is given to all those with access. Access levels are controllable. Different members can be given access to different functions and information. Also, the system can be designed to facilitate both internal communication and external communication with individuals and groups who are not formal members of the V-JIC. For example, individuals and groups can be given access to selected information via the Web site that is not available to the general public. This capability can be used, for example, to communicate with leaders who cannot be physically present but who wish to be kept fully informed.

The inquiry management function of a virtual communications center is especially useful when operated in a V-JIC setting. All inquiries are logged into the system regardless of whether they came in via the inquiry function on the external Web site, through phone calls, through traditional email, or through newer media such as Texting, Facebook, and Twitter. Even with a widely dispersed communication team, the PIO or task leaders can review all inquiries and see who has asked which questions, what the responses have been, and how quickly the JIC members have responded. Rumors can be quickly identified and addressed in new information updates and quality control issues quickly spotted, including violations of pre-release of changing information. This ability to review real-time communication activity can be extended to agency and executive leadership who are not on scene, provided they are given the appropriate security access.

3. Lack of Infrastructure

The infrastructure needed to operate a virtual JIC consists of computers with Internet access—preferably high speed access. Cell phones are also essential, particularly for responding to reporters and other stakeholders. Cell phone numbers of responders can be provided on the Web site and in information releases. Care should be taken to distribute the call load if volume is heavy.

Given current technology, even with a V-JIC, a place to hold a news conference is still required.

4. Web site Management and Infrastructure

In a V-JIC, users have full control of the entire Web site including the ability to launch entirely new Web sites for specific information purposes. All content is managed not as a separate communication function but fully integrated within the normal information development and distribution process. When a news release is drafted, edited, and approved, the PIO or designee can release it by going through two basic steps: (1) posting the information to the Web site, and (2) distributing it to contact lists by email, fax, or text-to-voice telephone messaging. All this is accomplished in seconds by selecting options within V-JIC system.

One significant advantage of this is the ability to have a continuous flow of updates. Media representatives or stakeholders coming to the V-JIC Web site can add their name to the mailing list so future updates can automatically be emailed to them. This can greatly diminish incoming phone calls.

A V-JIC Web site should be able to withstand millions of hits per day. The cost of providing this capability can be distributed across multiple users making it feasible for even smaller organizations to have full access to this capability. The V-JIC can be continually updated and modified, which increases usefulness.

Another important benefit is documentation. As Barone (2010) notes, documentation is a critical element of I-JIC operations. A V-JIC eliminates the need for most documentation staff. The V-JIC system itself tracks and records all activities including the participation of every member. This documentation capability is highly valuable for post-incident briefings and after-action reports.

Section 9.11 Sample Statement Regarding the Needed Capabilities of a Virtual Joint Information Center (V-JIC)

The following is a checklist of needed V-JIC capabilities.

- ❑ Capability to provide Web access by team members (users)
- ❑ Capability to provide 24/7 high capacity throughput/bandwidth that can handle millions of requests for data (text, images and video)
- ❑ Capability to store data from the primary data center in a geographically separated back-up data center
- ❑ Capability of being used for communications with internal, external, and guest groups
- ❑ Capability to scale to a virtually unlimited number of users, guests, and contacts
- ❑ Capability to monitor media and online communication activity
- ❑ Capability to contact media and online sources such as bloggers
- ❑ Capability of a virtually unlimited amount of storage for content, including images and video
- ❑ Capability to provide secure access by users for pre-approved functions
- ❑ Capability to provide application and security controls for guests to pre-approved documents
- ❑ Capability to change the status of the site between private, protected, and public

- ❑ Capability for drafting, storing, and archiving documents, including message maps, with draft/version control
- ❑ Capability for built-in approval process by document type
- ❑ Capability to store and archive pre-approved message maps and other communication materials, such as fact sheets and maps
- ❑ Capability to reduce the response time to inquiries and frequently asked questions
- ❑ Capability to easily post approved documents to the web site without information technology support staff intervention
- ❑ Capability to notify the media, the public, and other stakeholders via: email, text messaging (with two-way acknowledgement), fax, automated text-to-voice calling (with acknowledgement tracking)
- ❑ Capability to feed to Web sites
- ❑ Capability to feed to Social Media (such as Twitter, YouTube, Facebook, MySpace, etc.);
- ❑ Capability to handle inquires directly via e-mail or by phone
- ❑ Capability to track and archive responses with each inquirer for subsequent follow up and research
- ❑ Capability to efficiently solicit feedback from stakeholder
- ❑ Capability to be used with minimal training (less than two hours)

There are many technologies that can perform these capabilities. Ideally, all of these capabilities should reside in one system. Having them all in one system can significantly enhance the efficiency and effectiveness of team members who may be working remotely.

10. ERC/JIC Plan Maintenance

The ERC/JIC plan must be maintained. A sample statement regarding plan maintenance is provided in Section 10.1.

Section 10.1 Sample Statement Regarding ERC/JIC Plan Maintenance

The ERC/JIC plan must be consistently and continuously reviewed, practiced, and modified to stay current. In addition, training exercises should be scheduled so everyone with an identified role and responsibility under the plan and protocol can practice carrying out their function.

As part of plan maintenance, the following activities should be conducted.

- Each emergency risk communication task leader should annually review his/her strategy
- Each emergency risk communication task leader should annually incorporate changes to his/her strategy based on feedback received from other task leaders.
- The ERC/JIC plan should be revised annually and distributed to all members of the emergency risk communications team.
- All details in the ERC/JIC plan related to contacts with the media and other stakeholders (for example, telephone, email, fax, Web sites) should be reviewed, at a minimum, on a quarterly basis.
- All staff identified in the ERC/JIC plan (for example, spokespersons, news conference moderators, Web site managers, call center/hotline operators) should receive specialized training in their emergency risk communication tasks.
- Tests, drills, and exercises should be carried out regularly on the elements of ERC/JIC plan to confirm participants are prepared to respond effectively to an emergency.

Section 1:

Worksheet for Media Contacts

Site Name_____ Date_____

Use this worksheet to plan your communications with the media in the event of an IED attack. Be sure to consider the media's coverage in the past during the planning process.

Media	Contact Information	Past Coverage History of the Organization
Newspapers		
Radio Stations		
Television Stations		
Other Media		

Section 2:

Worksheet for Subject Matter Experts (SMEs)

Subject Matter Expertise	Name of Expert	Contact Information
		(0ffice tel.)
		(Home tel.)
		(Cell)/Mobile)
		(Fax.)
		(Email)

Section 3:

Worksheet for Notifications

Notifications

Use this worksheet to identify organizations and individuals who need to be notified in the event of an IED attack. Be sure to include both day and evening contact information.

Group	Notifications (check those that apply)	Contact	
		Who	How (Day/Evening)
	1.		
	2.		
	3.		
	4.		
	5.		
	6.		
	7.		
	8.		
	9.		
	10.		
	11.		
	12.		
	13.		

Notifications

Use this worksheet to identify organizations and individuals who need to be notified in the event of an IED attack. Be sure to include both day and evening contact information.

Group	Notifications (check those that apply)	Contact	
		Who	How (Day/Evening)
	14.		
	15.		
	16.		
	17.		
	18.		
	19.		
	20.		
	21.		
	22.		
	23.		
	24.		
	25.		
	26.		
	27.		
	28.		

Notifications

Use this worksheet to identify organizations and individuals who need to be notified in the event of an IED attack. Be sure to include both day and evening contact information.

Group	Notifications (check those that apply)	Contact	
		Who	How (Day/Evening)
	29.		
	30.		
	31.		
	32.		
	33.		
	34.		
	35.		
	36.		
	37.		

Notifications

Use this worksheet to identify organizations and individuals who need to be notified in the event of an IED attack. Be sure to include both day and evening contact information.

Group	Notifications (check those that apply)	Contact	
		Who	How (Day/Evening)
	38.		
	39.		
	40.		
	41.		
	42.		
	43.		
	44.		
	45.		
	46.		
	47.		
	48.		

Notifications

Use this worksheet to identify organizations and individuals who need to be notified in the event of an IED attack. Be sure to include both day and evening contact information.

Group	Notifications (check those that apply)	Contact	
		Who	How (Day/Evening)
	49.		
	50.		
	51.		
	52.		
	53.		
	54.		
Other	55.		
	56.		
	57.		
	58.		
	59.		
	60.		
	61.		
	62.		
	63.		
	64.		

Notifications

Use this worksheet to identify organizations and individuals who need to be notified in the event of an IED attack. Be sure to include both day and evening contact information.

Group	Notifications (check those that apply)	Contact	
		Who	How (Day/Evening)

]

Section 4:

Call Center/Hotline Tracking Form

Time of Call:_____ a.m. p.m.

Nature of call: Information Requested or Provided

- ❑ Clarify recommendations
- ❑ Current status of the incident
- ❑ Topic 1_____
- ❑ Hot topic 2_____

Request for referral:

- ❑ For more information
- ❑ For follow up
- ❑ Other _____

Feedback:

- ❑ Information regarding a specific contact with the organization
- ❑ Information about recommended actions
- ❑ Information about ability to carry out recommended actions
- ❑ Information about other topics (specify)

❑ Rumor or misinformation verification (briefly describe)

Outcome of call:

❑ Appeared to satisfy caller based on scripted information

❑ Referred caller to:

- ❑ Expert
- ❑
- ❑
- ❑
- ❑

Action needed:

❑ None

Return Call urgency*:*

- ❑ Critical (respond immediately)
- ❑ Urgent (respond within 24 hours)

❑ Routine

_____

Call taken by: _____ Date: _____

Section 5:

Principles and Techniques for Effective Media Communication

Listed below is a summary of the principles and techniques of effective media communication. This summary is based upon a review of the scientific and practitioner literature.

1. Demonstrate respect for the media by keeping them well informed of decisions and actions.

- Establish good working relationships with the media before an emergency arises.
- Include journalists in emergency response training exercises.
- Be polite and courteous at all times, even if the reporter is not.
- Avoid embarrassing journalists.
- Provide information for on-site journalists on the location of electrical outlets, public telephones, rest rooms, hotels, restaurants and other amenities.
- Avoid being defensive or argumentative during interviews.
- Include elements in interviews that make a story interesting to the media, including examples, stories and other aspects that influence public perceptions of risk, concern and outrage.
- Use a wide range of communication techniques to engage and involve people.
- Adhere to the highest ethical standards – recognize that people hold you professionally and ethically accountable.
- Strive to inform editors and journalists of preparedness plans for an IED attack.
- Offer to follow-up on questions that cannot be addressed immediately.
- Strive for "win-win" media outcomes.

2. Plan thoroughly and carefully for all media interactions

- Assess the cultural diversity and socioeconomic level of the target populations.
- Assess internal media-relations capabilities.
- Recognize that all communication activities and materials should reflect the diverse nature of societies in a fair, representative and inclusive manner.

- Begin all communication planning efforts with clear and explicit goals – such as:
  -- informing and educating;
  -- improving knowledge and understanding;
  -- building, maintaining or restoring trust;
  -- guiding and encouraging appropriate attitudes, decisions, actions and behaviors; and
  -- encouraging dialogue, collaboration and cooperation.
- Develop a written communication plan.
- Develop a partner communication strategy.
- Establish coordination in situations involving multiple agencies.
- Identify important stakeholders and subgroups within the audience as targets for your messages.
- Prepare a limited number of key messages in advance of potential emergencies.
- Post the key messages and supporting information on your own well-publicized web site.
- Pre-test messages before using them during an interview.
- Respect diversity and multiculturalism while developing messages.
- Train key personnel – including technical staff – in basic, intermediate and advanced media communication skills.
- Practice media communication skills regularly.
- Never say anything "off-the-record" that you would not want to see quoted and attributed to you.
- Recruit media spokespersons that have effective presentation and personal interaction skills.
- Provide training for high-ranking government officials who play a major role in communication with the media.
- Provide well-developed talking points for those who play a leading role in communication with the media.
- Recognize and reward spokespersons who are successful in getting their key messages included in media stories.
- Anticipate questions and issues that might be raised during an interview.
- Train spokespersons in how to redirect an interview (or get it back on track) using bridging phrases such as "what is really important to know is...".
- Agree with the reporter in advance on logistics and topic – for example, the length, location, and specific topic of the interview – but realize that the reporter may attempt to stray from the agreed topic.
- Make needed changes in strategy and messages based on monitoring activities, evaluation efforts and feedback.
- Work proactively to frame stories rather than waiting until others have defined the story and then reacting.
- Carefully evaluate media communication efforts and learn from mistakes.
- Share with others what you have learned from working with the media.

3. Meet the functional needs of the media

- Assess the needs of the media.
- Be accessible to journalists.
- Respect their deadlines.
- Accept that news reports will simplify and abbreviate your messages.
- Devise a schedule to brief the media regularly during an emergency, even if updates are not "newsworthy" by their standards – open and regular

---

communication helps to build trust and fill information voids.

- Refer journalists to your web site for further information.
- Share a limited number of key messages for media interviews.
- Repeat your key messages several times during news conferences and media interviews.
- Provide accurate, appropriate and useful information tailored to the needs of each type of media, such as sound bites, background videotape, and other visual materials for television.
- Provide background material for journalists on basic and complex issues on your web site and as part of media information packets and kits.
- Provide explanations and interpretations for numbers: can easily be misinterpreted or misunderstood.
- Stick to the agreed topic during the interview – do not digress.
- If you do not know the answer to a question, focus on what you do know, tell the reporter what actions you will take to get an answer, and follow up in a timely manner.
- If asked for information that is the responsibility of another individual or organization, refer the reporter to that individual or organization.
- Offer journalists the opportunity to do follow-up interviews with subject-matter experts.
- Strive for brevity, but respect the reporter's desire for information.
- Hold media availability sessions where partners in the response effort are available for questioning in one place at one time.
- Remember that it benefits the reporter and the organization when a story is accurate.
- Before an emergency occurs, meet with editors and with journalists who would cover the story.
- Work to establish durable relationships with journalists and editors.
- Promise only that which can be delivered, then follow through.

4. Be candid and open with journalists

- Be first to share bad news about an issue or your organization, but be sure to put it into context.

- If the answer to a question is unknown or uncertain, and if the reporter is not reporting in real time, express a willingness to get back to the reporter with a response by an agreed deadline.
- Be first and proactive in disclosing information about an emergency, emphasizing appropriate reservations about data and information reliability.
- Recognize that most journalists maintain a "healthy skepticism" of sources, and trust by the media is earned – do not ask to be trusted.
- Ask the reporter to restate a question if you do not understand it.
- Hold frequent media events to fill information voids.
- Do not minimize or exaggerate the level of risk.
- Acknowledge uncertainty.
- Be careful about comparing the risk of one event to another.
- Do not offer unreasonable reassurances (i.e. unwarranted by the available information).
- Make corrections quickly if errors are made or if the facts change.
- Discuss data and information uncertainties, strengths and weaknesses – including those identified by other credible sources.
- Cite ranges of risk estimates when appropriate.
- If credible authorities disagree on the best course of action, be prepared to disclose the rationale for those disagreements, and why your organization has decided to take one particular course of action over another.
- Be especially careful when asked to speculate or answer extreme or baseless "what if" questions, especially on worst-case scenarios.
- Avoid using absolutes (for example, the words "never" or "always."
- Tell the truth.

---

5. Listen to the target audience

- Do not make assumptions about what viewers, listeners and readers know, think or want done about risks.
- If time and resources allow, prior to a media interview, review the available data and information on public perceptions, attitudes, opinions, beliefs and likely responses regarding an event or risk. Such information may have been obtained through interviews, facilitated discussion groups, information exchanges, expert availability sessions, public hearings, advisory group meetings, hotline call-in logs, and surveys.
- Monitor and analyze information about the event appearing in media outlets, including the internet.
- Identify with the target audience of the media interview, and present information in a format that aids understanding and helps people to act accordingly.

- During interviews and news conferences, acknowledge the validity of people's emotions
  and fears.
- Be empathetic.
- Target media channels that encourage listening, feedback, participation and dialogue.
- Recognize that competing agendas, symbolic meanings, and broader social, cultural,
  economic or political considerations often complicate the task of effective media communication.
- Recognize that some audiences will be primarily concerned about whether people are being treated fairly in terms of access to information, care, and resources.

6. Coordinate, collaborate and act in partnership with other credible sources

- Develop procedures for coordinating the activities of media spokespersons from multiple agencies and organizations.
- Establish links to the web sites of partner organizations.
- Recognize that every organization has its own culture and this culture impacts upon how and what it tries to communicate.
- To the extent possible, act in partnership with other organizations in preparing messages in advance of potential emergencies.
- Share and coordinate messages with partner organizations prior to media interviews or news conferences.
- Encourage partner organizations to repeat or echo the same key messages – such repetition
  and echoing by many voices helps to reinforce the key messages for target audiences.
- In situations involving multiple agencies, determine information clearance and approval
  procedures in advance when possible.
- Aim for consistency of key messages across agencies – if real differences in opinion do exist be inclined to disclose the areas of disagreement and explain why your organization is choosing one course of action over another.
- Develop a contingency plan for when partners cannot engage in consistent messaging – be prepared to make an extra effort to listen to their concerns, understand their point of view, negotiate differences, and apply pressure if required and appropriate.
- Devote effort and resources to building bridges, partnerships and alliances with other
  organizations (including potential or established critics) before an emergency occurs.
- Consult with internal and external partners to determine which organization should take the lead in responding to media enquiries, and document the agreements reached.
- Discuss ownership of specific topics or issues in advance to avoid one partner treading upon the perceived territory of another.

- Identify credible and authoritative sources of information that can be used to support messages in potential emergencies.
- Develop a plan for using information from other organizations in potential emergencies.
- Develop contact lists of external subject-matter experts able and willing to speak to the media on issues associated with potential emergencies.
- Cite as part of your message credible and authoritative sources that believe what you believe.
- Issue media communications together with, or through, individuals or organizations believed to be credible and trustworthy by the target audience.

7. Speak clearly and with compassion

- Be aware that people want to know that you care before they care what you know.
- Use clear, non-technical language.
- Explain medical or technical terms in clear language when they are used.
- Use graphics or other pictorial material to clarify and strengthen messages.
- Respect the unique information needs of special and diverse audiences.
- Express genuine empathy when responding to questions about loss – acknowledge the tragedy of illness, injury or death.
- Personalize risk data by using stories, narratives, examples and anecdotes that make technical data easier to understand.
- Avoid distant, abstract and unfeeling language about harm, deaths, injuries and illnesses.
- Acknowledge and respond (in words, gestures and actions) to the emotions people express, such as anxiety, fear, worry, anger, outrage and helplessness.
- Acknowledge and respond to the distinctions people view as important in evaluating risks, such as perceived benefits, control, fairness, dread, whether the risk is natural or man-made, and effects on children.
- Be careful to use risk comparisons only to help put risks in perspective and context, and not to suggest that one risk is like another – avoid comparisons that trivialize the problem, that attempt to minimize anxiety, or that appear to be trying to settle the question of whether a risk is acceptable.
- Give people a sense of control by identifying specific actions they can take to protect themselves.
- Identify significant misinformation, being aware that repeating it may give it unwanted attention.
- Recognize that saying “no comment” without explanation or qualification is often perceived as guilt or hiding something – consider saying instead “I wish I could answer that. However...”.
- Be sensitive to local norms, such as those relating to speech and dress.
- Always try to include in a media interview a discussion of actions under way by the organization and actions that can be taken by the public.

Section 6:

Sample News Release Announcing the Opening of a Joint Information Center

==========

NEWS RELEASE

CONTACT: [name of contact] PHONE: [number of contact]

Date:

Joint Information Center Opened

[Insert location of JIC] At [insert time] today, the [insert organization name] received reports of [insert information on nature of the incident]. Due to this situation, a Joint Information Center (JIC) is being opened at the [insert location]. See attached map. A JIC is a centralized communications facility that serves as a central point for public affairs activities, media access, and coordination of emergency information.

[Insert actions being taken]

Spokespersons from the [insert organization name] and [insert names of other organizations and partners] will be available in the JIC to provide immediate updates on the situation and developments that may occur as a result of the situation. News conferences, background information, and opportunities to conduct interviews with public officials and subject matter experts will be available at the JIC.

Note to Reporters, Editors, and Assignment Desks

Reporters should enter the [insert description] entrance of the building. All reporters must sign in. All reporters must have credentials. A media workroom, equipped with telephones and other supplies, is available at the JIC. A JIC representative will be present to meet with media representatives. All news briefings will be held in the JIC news conference room.

For information updates by telephone, a media telephone bank has been installed at the JIC. The following telephone number is FOR MEDIA USE ONLY: [insert telephone number]

Please do not release this number to the public. This is for media use only. The public will be given a different number for information.

[Insert address, phone number for media and directions or a map to JIC]

Section 7:

Sample Joint Information Center News Releases

CONTACT: [insert name of contact] PHONE: [insert telephone number of contact]

Date: [insert date]

JOINT INFORMATION CENTER NEWS RELEASE

(Note: Items in brackets below are to be filled in)

At [insert time] today, the [insert name of organization] received reports of [insert information on the nature of the incident];

We have a [insert information on the existing plan, procedure, operations] in place for just such an [insert emergency or event]. We are being assisted by [insert names of partners] as part of the response.

The situation is [insert "under" or "not yet under"] control. We are working with experts and our partners to [insert "contain this situation," " determine how this happened," or " determine what actions may be needed to prevent this from happening again"].

Additional information will be provided as soon as possible.

Provided below are three samples of news releases. The first is an example of a statement that might be released by a local leader or emergency responder within first minutes of an IED attack. The other two news releases show how the initial news release might be expanded once more information is obtained.

Sample News Release #1: Thirty Minutes or Less Following an IED Attack

First and foremost, I want to emphasize that our most important priority is the safety and well- being of the community members. We are working closely with local authorities to find out exactly what has occurred, why it happened, and what, if any, action needs to be taken. What we know is …

We will give you the most accurate information possible as soon as we can. [Insert name of the media liaison] has been assigned to work with the news media. I/he/she will get back to you as soon as we have more details. Information will also be posted on our Web site at (insert Web site address) for all concerned individuals as soon as it becomes available.

Sample #2: Two-to-Four Hours Following the IED Attack

We have been working closely with local authorities since the attack occurred a few hours ago. Although we do not yet understand the full scope of the incident, we do know…

We expect to more accurately understand the implications of the event as we continue our investigation. As we move forward with the investigation, we will …

We will continue to give you accurate information as soon as we can. Our Web site (insert Web site address) has now been updated with the most current information. We will continue to update the site as new information becomes available.

Sample #3: Twenty-Four Hours Following an IED Attack

During the past 24 hours we have come to understand the IED attack more fully. We know now…
[Insert information about what happened, how many people were affected, etc.]

We are still seeking more information about (the cause of the attack, the people/event behind the attack, etc.)…We have contacted…We have also enlisted the help of [list additional resources] to assist us.

We will continue to provide you with updates as new information becomes available. I urge you to monitor our Web site at (insert Web site address) for the latest information.

In the mean time, we recommend that the public…

Sample Key Messages for a Confirmed IED Attack

Use the following as a template in developing specific key messages in the event of a confirmed IED attack.

- Situation/Response

There has been a confirmed terrorist attack using an Improvised Explosive Device, or IED.

The explosion occurred at [insert place and time].

We are working with federal, state and local agencies to take the appropriate steps to ensure the health and safety of those in the affected area.

- Empathy

Our thoughts are with the victims and their families.

- Scope

At this time it is unclear if this is an isolated incident.

We are working with federal, state and local authorities to determine the extent of the situation.

- Actions

We are working with federal, state and local authorities to ensure that all who have been affected are receiving appropriate treatment.

The public can play a key role in helping authorities to be alert for further acts of terrorism or to report other water equipment damages/problems.

Be alert.

If you see something suspicious, say something.

For example, if you see an unattended or suspicious package in a public place, call 911 or local law enforcement for additional instructions.

Seek medical treatment if you have been injured.

[Insert information on recommended actions specific to the attack].

- Risk

The risk to residents in [insert area] is [insert information on risk].

Section 8:

Sample Script for Immediate Responses to Media Inquires

Consider using any or all or the following scripts if the media is "at the door" and you need time to assemble the facts for the initial I-JIC news release. Getting information out quickly and getting the facts right are among the most important priorities. It is important not give in to pressure from reporters to confirm or release information before you have confirmation. The following are responses which may help give you time to collect and confirm facts.

Sample Scripted Responses:

1. If the reporter is on the telephone inquiring about the IED attack.

"We've just learned about the situation and are trying to get more complete information now. How can I reach you when I have more information?"

"All our efforts are directed right now at bringing the situation under control. I would prefer not to speculate about event." How can I reach you when I have more information?"

"I'm not the [expert; authority] on your question. Let me have your name and I will call you right back."

"We're preparing a statement on that right now. Can I [fax; e-mail] it to you in about [insert time?"]

"The answer to your question is on our Web site. Have you checked our Web site? If you leave me you name and contact information, I will send you our next update."

2. If the reporter has arrived in person at the site of the IED attack.

"This is an evolving situation. I know you want as much information as possible right now. While I work to get answers to your questions, I want to tell you what we can confirm right now [insert information]."

"At approximately [insert time], a [insert brief description of what happened based on available facts]."

"At this point, we do not know [insert information, such as injuries, deaths, etc.]."

"We have a [insert information such as information about a system, plan, procedure, operation] in place for just such an emergency."

"We are being assisted by [provide details: for example, the fire department, the Emergency Management Office, local law enforcement, the school system, the FBI, the Red Cross, etc.) as part of our emergency response plan."

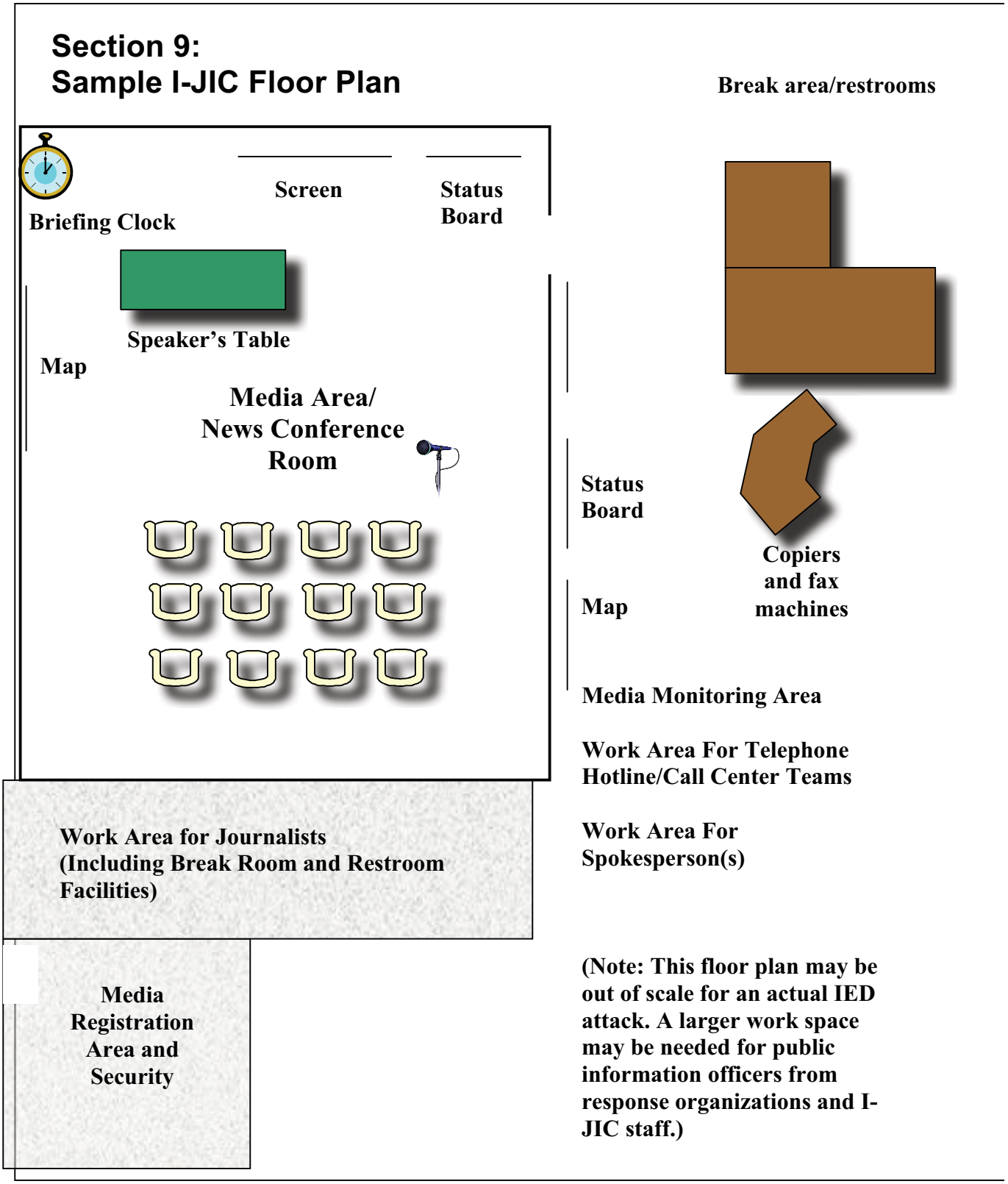
"The situation is [under] [not yet under] [currently beyond our] control."

“We are working with [insert names] to [contain this situation; determine how this happened’ determine what actions may be needed to prevent this from happening again].”

“We will continue to gather information and release it to you as soon as possible. I will be back to you within [insert amount of time] to give you an update. As soon as we have more confirmed information, it will be provided.”

“We ask for your patience as we respond to this emergency.”

Section 9:
Sample I-JIC Floor Plan



(Note: This floor plan may be out of scale for an actual IED attack. A larger work space may be needed for public information officers from response organizations and I-JIC staff.)

Section 11:

Sample Improvised Explosive Device (IED) Fact Sheet

"Preparing for an IED (Improvised Explosive Device) Attack: Frequently Asked Questions"

An improvised explosive device (IED) is a bomb and/or destructive device to destroy, incapacitate, harass, or distract. IEDs have been used by terrorists, suicide bombers, and others.

Terrorists engaged in a hostile action in the United States are likely to use IEDs. IEDs are widely recognized as being among the weapons of choice of terrorists throughout the world. The reasons are clear: the materials to make IEDs are often easy to find, the devices are relatively simple to construct, they are difficult to combat, and they can be devastatingly effective.

This document focuses on common sense principles that can be useful before, during, and after an IED attack.

1. What can I do now?

Every organization, family and individual should take the time needed to prepare for an emergency or disaster. These steps can help you get started:

- **Know your work, school and community disaster plans.** If you are not familiar with the plans, contact your supervisor, school administrators, or your local fire department for information.
- **Identify an alternative hospital.** Hospitals closest to the event are always the busiest.
- **Visit http://www.redcross.org/preparedness.** The site provides guidance on creating a disaster plan and steps you can take now to protect you and your loved ones.

2. What should I do if I think someone is going to set off an IED?

- Leave the area immediately.
- Follow existing evacuation guidelines.
- Leave the area immediately.
- Call 9-1-1. Tell the operator what you saw or know (suspicious persons, packages, or vehicles).

3. What should I do if I am present during an IED attack?

- **Leave the area immediately**.
- **Avoid crowds.** Crowds of people may be targeted for a second attack.
- **Avoid unattended cars and trucks**. Unattended cars and trucks may contain explosives.
- **Stay away from damaged buildings** to avoid falling glass and bricks. Move at least 10 blocks or 200 yards away from damaged buildings.
- **Follow directions from people in authority** (police, fire, emergency management officials, or military personnel, or from school or workplace supervisors).
- **Call 9-1-1 once you are in a safe area**, but only if police, fire, or emergency management officials has not arrived.
- **Help others who are hurt or need assistance to leave the area** if you are able. If you see someone who is seriously injured, seek help. Do not try to manage the situation alone.

4. What should I do after an IED attack?

- **Follow your family, job, or school emergency disaster plan for leaving and staying away from the scene of the event.** Remember, returning to the scene will increase the risk of danger for rescue workers and you.
- **Avoid crowds.** Crowds of people may be targeted for a second attack.
- **Avoid unattended cars and trucks.** Unattended cars and trucks may contain explosives.
- **Stay away from damaged buildings** to avoid falling glass and bricks. Move at least 10 blocks or 200 yards away from damaged buildings.
- **Follow directions from people in authority** (police, fire, local emergency management personnel, military personnel, or from school or workplace supervisors).
- **Call 9-1-1** if police, fire, or local emergency management personnel have not arrived to help injured people.
- **Help others who are hurt or need assistance to leave the area** if you are able. If you see someone who is seriously injured, seek help. Do not try to manage the situation alone.
- **Listen** to your radio or television for news and instructions.

5. What should I do if rescue workers are not available to transport me or other injured persons?

9-1-1 services (for example, police, fire, and ambulance services) might be delayed following an IED attack. Therefore:

- **Have a back-up plan** for transportation.
- **Follow advice from your local public safety offices** (local health department, local emergency management personnel, fire and police departments and reliable

news sources).

6. When should I go to the hospital or clinic?

- **Seek medical attention if you have any of the following problems:**

  - Excessive bleeding
  - Trouble breathing
  - Persistent cough
  - Trouble walking or using an arm or leg
  - Stomach, back or chest pains
  - Headache
  - Blurred vision or burning eyes
  - Dry mouth
  - Vomiting or diarrhea
  - Rash or burning skin
  - Hearing problems
  - Injuries that increase in pain, redness or swelling
  - Injuries that do not improve after 24 to 48 hours

- **Help others who are hurt or need assistance to leave the area**, if you are able. If you see someone who is seriously injured, seek help. Do not try to manage the situation alone.

7. Where should I go for care?

Go to a hospital or clinic away from the event if you can. Most victims will go to the nearest hospital. Hospitals away from the event will be less busy.

8. What can I expect at the hospital?

- **Long waits.** To avoid long waits, choose a hospital farther away from the event. While this might increase your travel time, you might receive care sooner.
- **Triage**. Following an IED attack or other disasters, injuries are generally treated on a "worst first" basis, called "triage." Triage is not "first come, first served". If your injuries are not immediately life threatening, others might be treated before you. The goal of triage is to save as many lives as possible.
- **Limited information**. After a large-scale IED attack, police, fire, hospitals and clinics will not be able to track every individual by name. Keep in mind that it may be difficult for hospitals to provide information about loved ones following an IED attack. Please be patient as you seek information.

For more information about how to prepare for an IED attack and other disasters, click on the related links:

- American Red Cross, www.redcross.org
- Federal Emergency Management Agency (FEMA), www.fema.gov
- Department of Homeland Security, www.ready.gov

References

Auf der Heide, E. (2004) Common misconceptions about disasters: Panic, the "disaster syndrome" and looting, pp. 340-380 in O'Leary M. The First 72 Hours: A Community Approach to Disaster Preparedness. Lincoln (Nebraska), iUniverse Publishing.

Bennett, P., and Calman, K. (1999) Editors. Risk communication and public health. New York (NY): Oxford University Press.

Bennett, P., Coles, D., and McDonald, A. (1999) Risk communication as a decision process: Risk Communication and Public Health, P. Bennett and Calman, K., editors, New York: Oxford University Press.

Blendon, R.J., Benson, J.M., DesRoches, C.M., Raleigh, E., and Taylor-Clark, K. (2004) The public's response to Severe Acute Respiratory Syndrome in Toronto and the United States. Clinical Infectious Diseases, 38, 925-931.

Brunk, D. (2003) Top 10 lessons learned from Toronto SARS outbreak: a model for preparedness. Internal Medicine News. Volume 36, Issue 21, p. 4.

Centers for Disease Control and Prevention (2002) Emergency and Risk Communication. Atlanta, Georgia

Centers for Disease Control and Prevention, National Center for Health Marketing (2007) Plain English Thesaurus for Health Communications, Atlanta, Georgia (www.nphic.org/files/editor/file/thesaurus_1007.pdf)

Chess C., Hance B.J., and Sandman P.M.. Planning Dialogue with Communities: A Risk Communication Workbook (1986) New Brunswick, NJ: Rutgers University, Cook College, Environmental Media Communication Research Program.

Covello, V. (1992) Risk Communication: An Emerging Area of Health Communication Research. In S. Deetz, ed. Communication Yearbook 15. P. 359–373. Sage Publications, Newbury Park and London.

Covello, V.T. (2003) Best practice in public health risk and crisis communication. Journal of Health Communication, Vol. 8, Supplement 1, June: 5-8.

Covello, V.T. (2006) Risk communication and message mapping: A new tool for communicating effectively in public health emergencies and disasters. Journal of Emergency Management, Vol. 4 No.3, 25-40.

Covello, V.T. and Allen, F. (1988) Seven Cardinal Rules of Risk Communication. Washington (DC): Environmental Protection Agency.

Covello, V.T., Clayton, K., and Minamyer, S., (2007) Effective Risk and Crisis Communication During Water Security Emergencies: Summary Report of EPA Sponsored Message Mapping Workshops. EPA Report No. EPA600/R-07/027. Cincinnati, Ohio: National Homeland Security Research Center, Environmental Protection Agency.

Covello, V.T., McCallum, D.B., Pavlova, M.T. (1989) Eds. Effective Risk Communication: The Role and Responsibility of Government and Nongovernment Organizations. New York, NY: Plenum Press.

Covello, V.T., Peters, R., Wojtecki, J., and Hyde, R. (2001) Risk communication, the West Nile Virus epidemic, and bio-terrorism: Responding to the communication challenges posed by the intentional or unintentional release of a pathogen in an urban setting. Journal of Urban Health. Vol. 78(2), June: 382-391.

Covello, V.T. and Sandman, P. (2001) "Risk Communication: Evolution and Revolution," in Wolbarst A. (ed.) Solutions to an Environment in Peril. Baltimore, MD: John Hopkins University Press: 164-178.

Covello, V.T., Slovic, P., and von Winterfeldt, D. (1986) Risk communication: a review of the literature. Risk Abstracts. 3(4):171-182.

Davies C.J., Covello, V.T. and Allen, F.W. (Eds.) (1987) Risk Communication: Proceedings of the National Conference on Risk Communication., Washington, D.C., The Conservation Foundation.

Douglas, M., and Wildavsky, A. (1982) Risk and culture: An essay on the selections of technological and environmental dangers. University of California Press, Berkeley, California.

Environmental Protection Agency (US) (2007) Communicating Radiation Risks: Crisis Communication for Emergency Responders. United States Environmental Protection Agency, Office of Radiation and Indoor Air. EPA-402-F-07-008. July. Washington, DC

Embrey, M. and Parkin, R. "Risk communication." In: Embrey M. et al. 2002. Handbook of CCL Microbes in Drinking Water. Denver, CO: American Water Works Association, 2002.

Fischhoff, B. (1995) Risk perception and communication unplugged: twenty years of progress. Risk Anal. 15 (2): 137-145.

Hance, B.J., Chess, C., Sandman, P.M. (1990) Industry Risk Communication Manual. Boca Raton, FL: CRC Press/Lewis Publishers

Hyer, R. and Covello, V.T. (2007) Effective Media Communication During Public Health Emergencies: A World Health Organization Handbook. Geneva, Switzerland: World Health Organization.

Johnson, B.B., & Covello, V. (1987) The Social and Cultural Construction of Risk: Essays on Risk Selection and Perception. Dordrecht, Holland: D. Reidel Publishing.

Kahneman, D., Slovic, P., Tversky, A. (Ed). (1982) Judgment under uncertainty: heuristics and biases. Cambridge University Press. New York.

Kahneman, D. and Tversky, A. (1979) Prospect theory: An analysis of decision under risk. Econometrica. 47(2):263-291.

Kasperson, R.E., Renn, O., Slovic, P., Brown, H.S., Emel, J., Goble, R., Kasperson, J.X., and Ratick, S. (1987) The social amplification of risk: A conceptual framework. Risk Anal. 8:177-187.

Krimsky, S., & Plough, A. (1988) Environmental Hazards: Communicating Risks as a Social Process. Dover, MA: Auburn House.

Lindell, M. K. and V. E. Barnes, V.E. (1986) "Protective Response to Technological Emergency: Risk Perception and Behavioral Intention." Nuclear Safety. Vol. 27, No. 4. October-December.

Lofstedt, R.E., and Renn, O. (1997). The Brent Spar controversy: An example of risk communication gone wrong. Risk Analysis, 17(2), 131–135.

McKechnie, S. and Davies, S. (1999) Consumers and risk. In: Risk Communication and Public Health. ed. P. Bennett. Oxford University Press, Oxford, p. 170.

Mileti, D. S. and Beck, S. (1975) Communication in Crisis: Explaining Evacuations Symbolically. Communication Research. Vol. 2, No. 1. January.

Mileti, D. S. and L. Peek, L. (2000) The social psychology of public response to warnings of a nuclear power plant accident. Journal of Hazardous Materials. 75(2): 181-194.

Lundgren, R. and McKakin, A. (2004) Risk Communication: A Handbook for Communicating Environmental, Safety, and Health Risks. Third Edition. Batelle Press. Columbus, Ohio.

Morgan, M.G., Fischhoff, B., Bostrom, A., Atman, C.J. (2001) Risk Communication: A Mental Models Approach. Cambridge University Press, Cambridge, UK.

Morgan, G., Fischhoff, B., Bostrom, A., Lave, L., & Atman, C.J. (1992). Communicating Risk to the Public. Environmental Science and Technology, 26(11), 2048–2056.

National Research Council/National Academy of Sciences (1989) Improving Risk Communication. National Academy Press, Washington, DC.

National Research Council/National Academy of Sciences (1996) Understanding Risk: Informing Decisions in a Democratic Society. National Academy Press, Washington, DC.

Peters, R., McCallum, D., and Covello, V.T. (1997) The determinants of trust and credibility in environmental risk communication: An empirical study. Risk Analysis, Vol. 17(1):43-54.

Powell, D., and Leiss, W. (1997). Mad Cows and Mother's Milk: The Perils of Poor Risk Communication. Montreal, Canada: McGill-Queen's University Press.

Renn, O., Bums, W.J., Kasperson, J.X., Kasperson, R.E., and Slovic, P. (1992). The Social Amplification of Risk: Theoretical Foundations and Empirical Applications. Journal of Social Science Issues, 48, 137–160.

Sandman, P.M. (1989) Hazard Versus Outrage in the Public Perception of Risk. In: Covello, V.T., McCallum, D.B., Pavlova, M.T., Eds. Effective Risk Communication: The Role and Responsibility of Government and Non-government Organizations. New York, NY: Plenum Press; 1989:45-49.

Slovic, P. (Ed.) (2000) The Perception of Risk. London: Earthscan Publication, Ltd.

Slovic, P. (1987) Perception of risk. Science. 236: 280-285.

Slovic, P., Fischhoff, B., & Lichtenstein, S. (2001). Facts and Fears: Understanding Perceived Risk. In Slovic, P., (Ed.) The Perception of Risk (pp. 137–153). London: Earthscan Publications Ltd.

Stallen, P.J.M, Tomas, A. (1988) Public concerns about industrial hazards. Risk Anal., 8, 235-245.

Weinstein, N.D. (1987) Taking Care: Understanding and Encouraging Self-Protective Behavior. Cambridge University Press. New York.