frontiers in Communication

REVIEW
published: 14 October 2016
doi: 10.3389/fcomm.2016.00008

Information Communication Technology Use for Public Safety in the United States

Naim Kapucu and Brittany Haupt*

School of Public Administration, University of Central Florida, Orlando, FL, USA

Information communication technology (ICT) is a crucial tool to support effective communication and decision-making under complex and uncertain environments of disasters by enhancing cognitive capacity of emergency managers. With the continuous influence and evolution of communication technologies, information sharing and decision-making has drastically changed and affects each phase of emergency management. Researchers continue to investigate the relationship of human involvement for spreading public safety information through ICT. With each disaster holding diverse characteristics influencing prediction, detection, and specific activities required for prevention, mitigation, response and recovery, the need for interoperable and dependable communication infrastructure, a common operating picture, and supportive regulations, policies, and practice greatly increases. Although a national public safety communication system was proposed, there are implementation challenges between local, state, and federal agencies. This paper briefly examines the evolution of the use of ICT for public safety along with current trends, benefits and challenges, and future needs.

Keywords: crisis communication, ICT, disaster management, communication technologies, disaster holds

OPEN ACCESS

Edited by:
Natalie Danielle Baker, Virginia Commonwealth University, USA

Reviewed by:
Spyridon Samonas, Louisiana Tech University, USA
Beverly Ann Cigler, Penn State Harrisburg, USA

****Correspondence:***
Naim Kapucu
kapucu@ucf.edu

Specialty section:
This article was submitted to Disaster Communications, a section of the journal Frontiers in Communication

Received: *09 March 2016*
Accepted: *27 September 2016*
Published: *14 October 2016*

Citation:
Kapucu N and Haupt B (2016) Information Communication Technology Use for Public Safety in the United States. Front. Commun. 1:8. doi: 10.3389/fcomm.2016.00008

INTRODUCTION

When understanding public safety and the sharing and coordination of information, information communication technology (ICT) is a crucial asset to support effective decision-making under complex and uncertain disaster conditions. Moreover, ICT enhances cognitive capacity of emergency managers when processing large volumes of information in short time periods (Comfort, 2007; Bharosa et al., 2010; Celik and Corbacioglu, 2010; Van De Walle et al., 2010). This is a critical skill during disaster response and impacts information sharing, communication, and collaboration between response agencies. The lack thereof can lead to potentially catastrophic consequences.

With the continuous influence and evolution of communication technologies, information sharing and decision-making has drastically changed and affects each phase of emergency management (Bharosa et al., 2010). For instance, the terrorist attacks of September 11, 2001, hereafter referenced as 9/11, significantly increased priority of public safety's use of communication technology. With overloaded landline circuits in the New York City area, individuals had to rely on their smart phone Internet connections for mass communication (Fu, 2011). The heightened use of the Internet to disseminate disaster-related information led to critical research surrounding ICT as a tool for emergency management communication.

Speaking to current and future trends, researchers continue to investigate the relationship of citizen involvement for spreading public safety information through ICT (Black et al., 2014). However, effectiveness of such involvement relies on interoperable and dependable communication infrastructure, a common operating picture, and supportive regulations, policies, and practice.

The Department of Homeland Security (DHS) and the Federal Emergency Management Agency (FEMA) are responsible for coordinating a national response infrastructure through strategic planning, implementation, and training of communications equipment for relevant local, state, and tribal governments and emergency response personnel (Department of Homeland Security, 2014; Federal Emergency Management Agency, 2015). In essence, ICT must provide multi-faceted support during an emergency (Van De Walle et al., 2010). However, with the speed of technological advances surpassing policy and regulatory changes, there is a significant gap to address. Moreover, each disaster holds diverse characteristics influencing prediction, detection, and specific activities required for effective prevention, mitigation, response, and recovery.

Although a national public safety communication system was proposed, there are implementation challenges between local, state, and federal agencies. For example, participation within this national system is voluntary and furthers disconnect between policies and stakeholders (Peha, 2006; Habib and Mazzenga, 2008; Hallahan and Peha, 2008). Therefore, this paper examines the evolution of information communication technology for public safety along with current trends, benefits and challenges, and future needs. The following research questions are examined in the paper: How have information communication technology-related policies implemented? What is the relationship between ICT and public safety? What are the applications of ICT for public safety? and What are benefits and challenges with utilizing ICT for public safety?

This paper builds on and contributes to earlier studies on information communication technology use for public safety. Although earlier studies examined avenues of ICT, they did not incorporate the focus of public safety use along with historical developments and current trends. As such, this paper provides additional insight into the evolution of ICT, the development of ICT-related policies, the relationship between ICT and public safety, along with applications, benefits, and challenges.

INFORMATION COMMUNICATION TECHNOLOGY-RELATED POLICY DEVELOPMENT IN THE US

Analyzing historical influences, the field of Emergency Management shifted in the perception of information sharing needs via adaptations to policy changes and agendas (Federal Emergency Management Agency, 2015). From the early years to the Cold War Era, there was limited systemic management of disasters as government tended to focus more on threats by fires and diseases with EM operating as a function of government to avoid nuclear war. Through the Disaster Relief Act of 1950 and the creation of the FEMA in 1979, the field's focus broadened to natural disasters and coordination between federal, state, and local agencies as well as non-profit and private organizations (Kapucu and Van Wart, 2006; Federal Emergency Management Agency, 2015).

As policy-makers and practitioners noticed how each disaster or extreme event required unique information and communication needs, policy adaptations focused on information specific processes and led to the establishment of the DHS, Title XVIII of the *Homeland Security Act of 2002*, and the Office of Emergency Communications (OEC). The OEC developed the National Emergency Communications Plan (NECP) and the National Public Safety Broadband Network (NBP) to deploy wireless Internet Protocol-based technologies for information sharing (Federal Emergency Management Agency, 2015).

The NECP incorporates five specific goals beginning with governance and leadership to enhance coordination, planning, and decision-making for EM communications. The remaining goals focus on aspects, such as governance and leadership, to update and improve communications and readiness for dynamic environments. Moreover, remaining goals focus on improving abilities for responders to communicate and coordinate operations to improve effectiveness while engaging in evaluation activities to support responders and unveil innovative capabilities (Department of Homeland Security, 2014). The goals help with three specific priorities for EM communication: (1) identifying and prioritizing areas for improvement in emergency responders' land mobile systems; (2) ensuring that emergency responders government officials plan and prepare for the adoption, integration, and use of broadband technologies, including the planning and deployment of the NBP; and (3) enhancing coordination among stakeholders, processes, and planning activities across the emergency response community (Department of Homeland Security, 2014).

An additional influence on the evolution of ICT is through FEMA's connection with the Federal Communications Commission (FCC) to focus message distribution to those fitting within the following parameters:

1. Conditions of impending or actual nature that jeopardizes public safety during times of civil emergencies.
2. Information relating to immediate safety of life issues or property protection, maintenance of law and order, or alleviation of human suffering and need along with combating of attacks.
3. Information essential to public activities for civil defense or additional government and relief agencies.
4. Information for Radio Amateur Civil Emergency Services training, drills, and testing.

In addition to guidance from FECP and FCC, FEMA incorporates an independent study course focused on communication. Participants within this course will not only develop basic communication skills but also help individuals learn: (a) how to communicate in an emergency, (b) how to identify community-specific communication issues, (c) use technology as a communication tool, (d) develop effective oral communication, and (e) how to prepare for an oral presentation (Federal Emergency Management Agency, 2014). In addition, social media (SM) is gaining recognition in the field leading Federal Emergency Management Agency (2013) to create a course in their independent study program. The objectives include (a) explaining the importance of SM for emergency management, (b) describing major features and functions of common sites being used, (c) describing the challenges and opportunities of SM applications in relation to the five phases of emergency management, (d) discussing better practices for SM applications,

and (e) building the capability of SM use and sustaining it within an emergency management organization.

Regarding the current National Incident Management System (NIMS), the traditional approach focuses on components of preparation, mitigation, response, and recovery (Federal Emergency Management Agency, 2015). These phases are considered the life cycle of a disaster beginning with preparation, which involves increasing the readiness for potential disasters or hazards. Mitigation focuses on prevention and reduction of potential impact through (a) changing the nature of the threat; (b) decreasing vulnerability; and (c) reducing exposure. The response component increases the community's capacity to monitor, predict, avoid, and reduce potential damage or address potential threats along with strengthening preparation activities for responding to disasters and assisting those impacted (Waugh and Streib, 2006; McEntire, 2007; Kapucu and Özerdem, 2011; Kapucu and Garayev, 2012; Sylves, 2014).

Since it cannot be predicted how infrastructure failures fully affect emergency management agencies, trust, and reliance is given to an Incident Command System (ICS). This centralized command and control structure incorporates five dimensions: command, operations, planning, logistics, and finance/administration (Boin and O'Connell, 2007; Federal Emergency Management Agency, 2015). The main benefit of ICS is the ability for unified command and collaboration between local, state, and federal stakeholders (Hu et al., 2014). However, major challenges include the lack of flexibility and adaptive capability of the system in conjunction with the complex communication needs for all local, state, and federal actors (Birkland, 2009; Hu et al., 2014; Liu et al., 2014).

As previously mentioned, public safety organizations and disaster response agencies are increasingly relying on ICT for effective coordination and communication during disasters or extreme events. This reliance increased over the years due to significant events, such as the terrorist attacks of 9/11. During disaster response, first responders were unable to exchange critical, life-saving information. The interoperability between wireless radio systems among federal, state, and local agencies was considered a highly flagrant example of unpreparedness (Abusch-Magder et al., 2007). The deficiencies of communication between first responders and public safety organizations led to failure to mobilize a coordinated communications infrastructure at the site of a disaster. This communication issue has also occurred during other crises and disasters, such as Hurricane Katrina and Rita, along with the Oklahoma City Bombing (Van De Walle and Turoff, 2007; Fu, 2011). These deficiencies realized during 9/11 and further emphasized from additional disasters highlight the integral asset of ICT.

To have an effective Emergency Response Information System, it must be a structured system with interoperable and dependable structures along with comprehensible and realistic protocols (Turoff et al., 2004; Peha, 2015). Moreover, this system must balance fault tolerance, provide avenues for advanced capabilities to manage security, cost, and spectral efficiency as well as trained personnel to operate the system (Peha, 2006; Van De Walle and Turoff, 2007; Ansari et al., 2008). With the current national communication system, proposed in the NECP, the goal of interoperability strengthens the ability of individuals and organizations to communicate and disseminate information and, hopefully, overcome impediments, such as funding, incompatible systems, and geographic coverage. In addition, the national system has the capability of creating a common operating picture and vocabulary for local, state, and federal response agencies to support efficient wireless communication (Faulhaber, 2006; Peha, 2006, 2015; Manoj and Baker, 2007). As for dependability and fault tolerance, communication infrastructure and information sharing policies must be able to adapt to the needs of response agencies and support operations in regards to stationary (i.e., headquarters), semi-mobile (i.e., mobile command posts), or mobile actors (i.e., frontline personnel).

RELATIONSHIP BETWEEN THE USE OF ICT AND PUBLIC SAFETY

Regarding the relationship between the use of ICT and public safety, the integration begins with the decision-making process for policies and practice. Although EM tends to rely on the traditional, hierarchical approach, there have been adaptations and changes toward a more flexible and adaptable approach. For example, some public safety organizations keep their information process in a top-heavy format with the decision processes flowing from top to the bottom. Other response organizations, such as non-profits, tend to have a decentralized process with decision-making starting at the lowest level. Regardless of the structure, disasters or events complicate the interaction between ICT and public safety. The variations in structure impact the communication process via aspects, such as acronyms, colloquialisms, technical jargon, and other agency-specific or professional language (Waugh, 2003).

Moreover, the adoption process of these diverse technologies highlights the timely process for each new technology first entering into the federal government environment before branching out to state and local agencies. In this aspect, the size of the agency greatly affects dispersion of ICT. For instance, "large, better-resourced governments tend to adopt earlier than small and poor ones. New technology and its diffusion through government provide the potential for simple, complex, minor, and major change in organizations and institutions, but they certainly do not guarantee them" (Bretschneider and Mergel, 2011, p. 190). In addition, the process of adopting technology is, on some level, adapted to the organization, but the organizational structure affects how the agency will implement the new technology.

Information Collection

When discussing the information collection part of communication, a significant challenge for emergency responders revolves around providing timely and accurate information before, during, and after disasters and crises (Manoj and Baker, 2007; Van De Walle and Turoff, 2007). In addition, there is an aspect of filtering to occur when determining sharing needs (Meissner et al., 2002). Moreover, sharing must keep the voice of public safety in mind (i.e., first responders, practitioners, researchers, community members, etc.) while safeguarding sensitive, classified, and proprietary data (Peha, 2006; White House, 2013; Rysavy, 2015).

Information Processing and Dissemination

Once the information is collected and the necessary stakeholders are identified for sharing, then the processing and dissemination begins. With EM being a field dependent on people, it is necessary to incorporate information in diverse modes (i.e., warnings, reports, news broadcasts, and training videos) and utilize a number of communication avenues (Kapucu et al., 2008; Black et al., 2014; Peha, 2015). These steps are critical in maintaining the supportive role of ICT for EM personnel (Van De Walle et al., 2010). Another aspect to consider is interorganizational relationships when disseminating information as knowing the recipients helps optimize resource and encourage collaborative strategies (Hu et al., 2014). Moreover, sharing is dependent upon a shift in mindset from the traditional perspective. Response organizations must be comfortable with not having full access to information and being transparent to their communities. Moreover, operators must adapt and utilize innovative communication technologies to navigate dynamic situations.

Technical and Cultural Interoperability

Speaking more to the audience, the adoption of a national communication system is growing; however, the policies and practices are far from universal. Within certain demographic groups (i.e., poor, some racial and ethnic minorities, elderly, individuals with disabilities, rural, or geographically isolated citizens), the current access and implementation practices lack affordability, availability and applicability (see **Figure 1** for cultural adoption rates of broadband ICT) (Peha, 2006; Manoj and Baker, 2007; Habib and Mazzenga, 2008; Federal Communications Commission, 2010).

If policies and practice do not investigate and generate solutions for technical and cultural interoperability issues, then trust in the system is affected. As stated by Kapucu and Liou (2014), government officials should invest time and resources into developing trust prior to disasters as this aspect enhances recovery processes and supports resiliency. An avenue to develop this trust is through training of the personnel utilizing these systems while promoting transparency and accountability (Van De Walle and Turoff, 2007). If a community consists of fragmented relationships, then there is a decreased desire to participate in EM practices and act upon critical information (Waugh and Liu, 2014). The other side of access is disseminating the information in a comprehensible format. According to Roeder (2014), the information must be demonstrative of all types of disasters or events. Moreover, researchers examined diversity of ICT relating to communication and discovered a single avenue for public information only increases vulnerability because people need affirmation from several resources (Chiu et al., 2010). This may be due to recent studies showing specific racial and ethnic minorities holding higher degrees of distrust for their local, state, and federal representatives due to previous broken promises or detrimental relationships (Donner and Rodríguez, 2008).

TRENDS IN ICT APPLICATIONS FOR PUBLIC SAFETY

In reaction to 9/11, the National Research Council published a study on the Internet usage during the terrorist attacks (Computer Science and Telecommunications Board, 2003). A significant

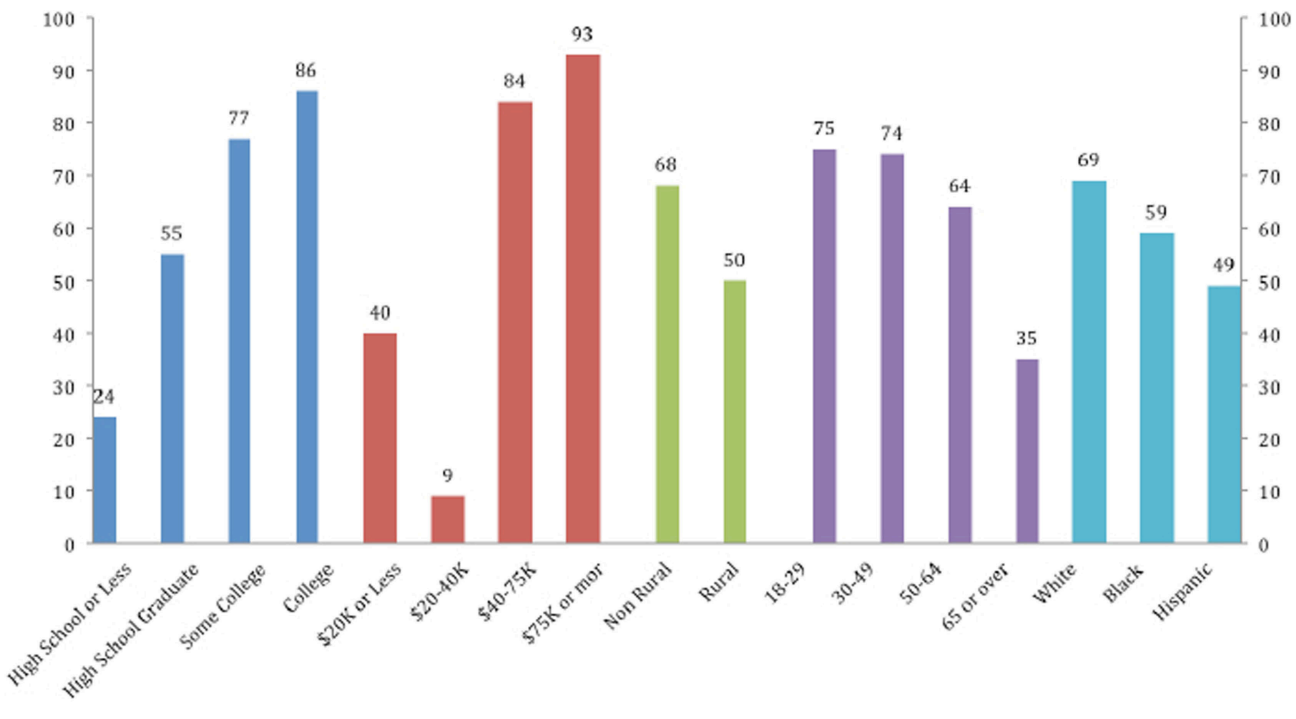

FIGURE 1 | Broadband adoption exhibit from National Broadband Plan based on socio-economic and demographic factors (Federal Communications Commission, 2010, p. 23).

finding included the ability to use the Internet in future events. With efficient technology, such as text messaging and e-mail, communication capabilities of response organizations are enhanced. Moreover, 9/11 saw an increase in the use of personal web sites for information dissemination and became a tool utilized during Hurricane Katrina and the 2011 tsunami crisis (O'Grady, 2005). With the continued integration of ICT with the Internet, response organizations are able to communicate in crisis situations in a variety of ways. The Internet is also ideal in its availability, reliability, flexibility, and redundancy of network design. In addition, the real-time capabilities for information exchange enhance preparation, mitigation, response, and recovery activities (Jefferson, 2006).

Software Generation

The foundation of ICT begins with its software. Programs, such as WORKPAD (Mecella et al., 2006), provide adaptable peer-to-peer software for communication infrastructure to support collaboration between agency operators within disaster situations. Additional programs, such as WebEOC, E-Team, and SharePoint, allow for quick dissemination of information to assist responders with making informed decisions (Hu and Kapucu, 2014). This issue, however, is system-to-system collaborations, and urgency notifications are not fully supported within all system types. To address these issues, Fiedrich and Burghardt (2007) researched the deployment of response agencies and promoted improved communication among key personnel, as presented at the First International Workshop on Agent Technology for Disaster Management (Jennings et al., 2006). For example, Buono et al. (2008) proposed WIISARD, a Wireless Internet Information System for Medical Response in Disasters, to band broad-based collaboration from all sectors, such as academia, industry, military, and emergency responders, in order to enhance care in a natural disaster or terrorist attack (Chiu et al., 2010). Through utilization of a mesh network, WIISARD enhance communication technologies among emergency responders and improved safety through tracking the "hot zone." This zone is a location where impact of a natural disaster or terrorist attack is centralized and affects the most civilians (Chiu et al., 2010).

Radio and Wireless Technology

Bridging off of the software, the implementation of the generated program hinges on suitable ICT. For instance, radio technology is a direction used within response networks. By utilizing mobile cellular networks and wireless fidelity (Wi-Fi), then organizations are able to connect systems for worldwide operability. Another approach is through technology, such as land mobile radio (LMR) or terrestrial trunked radio (TETRA). The employment of commercial technology provides several significant benefits (see **Figure 2** for visualization of a mobile network utilizing these technologies): "Wide availability of commercial handsets during emergencies, Significant cost savings from economies of scale because of large-scale deployment of commercial technologies, Rapid evolution and feature development in handset capabilities and services driven by competition in the commercial market, and Multi-vendor interoperable solutions" (Abusch-Magder et al., 2007, p. 115).

Virtual Organizations

During 9/11, the technological infrastructure of New York City was seriously damaged. With complete or partial damage to surrounding buildings, destruction of electrical power generation and distribution system for lower Manhattan, immobilization of the water distribution system, along with disruptions within gas pipelines and the telephone and telecommunications services (Kapucu, 2006). The damage resulted in emergency management response agencies scrambling to initiate response activities and create avenues for communication to affected communities. To circumvent this issue in the future, an avenue for ICT and public safety was created with the use of virtual organizations. These organizations are made up of a formal and informal organizational workflow processes (**Figure 3**) and a meta-process (**Figure 4**) to regulate structure (Turoff et al., 2004).

Becerra-Fernández et al. (2008) conceptualized and developed measures for the virtual emergency operations center. A goal is to mediate knowledge integration between task performance and complexity/uncertainty. However, a challenge faced is redundancy between virtual organizations, virtual emergency operations centers, and another avenue of Virtual Operations Support Teams (VOSTs) to monitor disasters and events via Social Media (Steen, 2015). To reduce redundancy, Roman et al. (2008) proposed electronic knowledge management (eKM) tools to reduce the magnitude of information people read and maintain awareness of web content during emergencies. By using eKM, responders and communities are able to quickly gather information from many websites and learn about specific issues. Moreover, the navigation portion of the eKM guides information seekers to the relevant websites depending on search criteria (Chiu et al., 2010).

This specialized navigation is completed through a specialized design program using eight principles. The first focuses on the directory, which provides a hierarchical structure for current data and information within the system. In addition, it allows for search capabilities to navigate toward subsets of the material. The second principle incorporates information source and timeliness. In an emergency, it is critical that all data are identified by source, time of occurrence, and status. Third is an open multi-directional communication system for all those involved in reacting to the disaster. The fourth and fifth principles address the content and making sure the information is up-to-date and is comprehensible. Sixth is the focus on linking relevant information and data followed by the seventh principle of authority, responsibility, and accountability. Last is the eighth principle of psychological and sociological factors to encourage and support the social needs of the crisis response team (Turoff et al., 2004).

Social Media Use

A key component of response and virtual organizations that utilize the Internet is the current trend of SM as an avenue for information dissemination. It began with the personal website usage after 9/11 and continued with focused blogs before specific web applications were created, such as Facebook, Twitter, and LinkedIn (O'Grady, 2005; Sutton et al., 2008; Latonero and Shklovski, 2011). Dissemination of disaster-related information has increased on SM as it connects to all phases of emergency management and to engage members of the community. Some

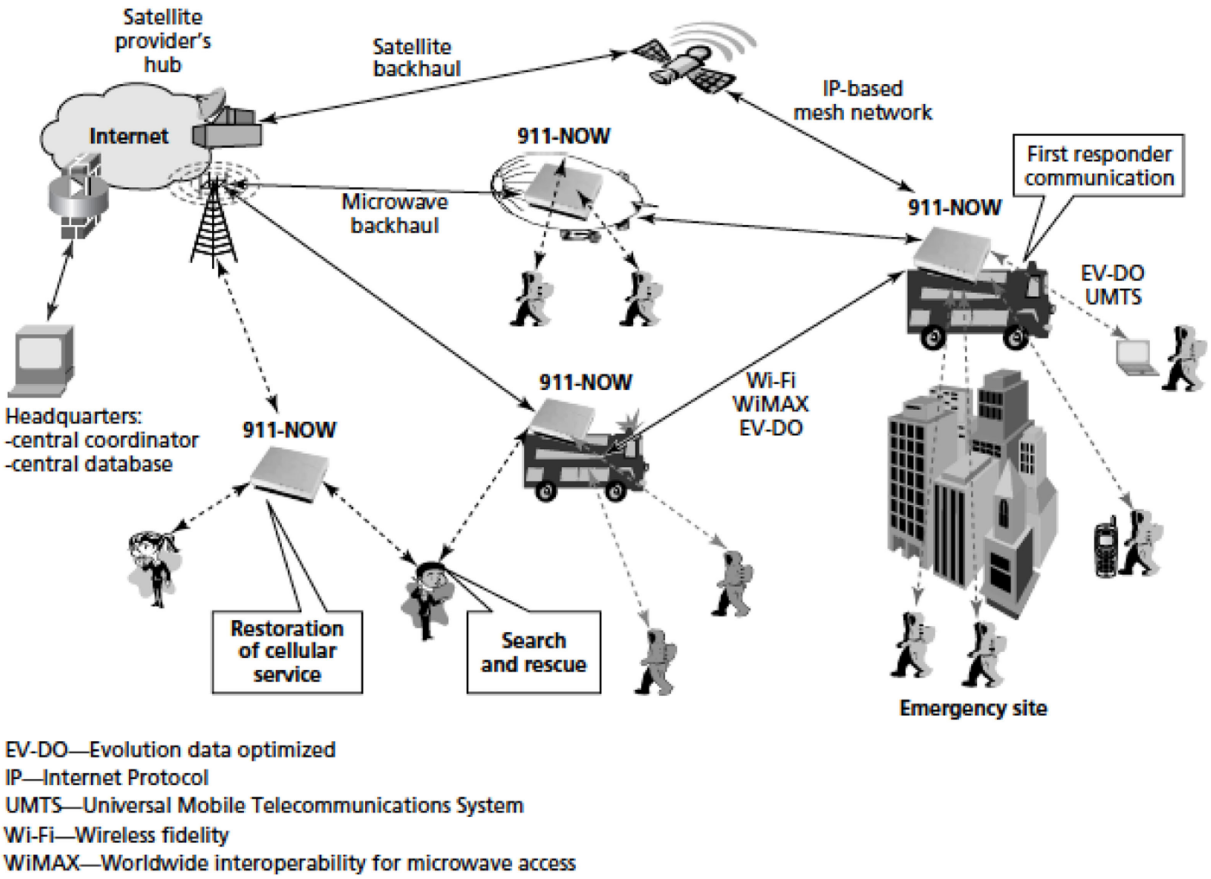

FIGURE 2 | **Adapted visualization of mobile networks utilizing ICT (Abusch-Magder et al., 2007).**

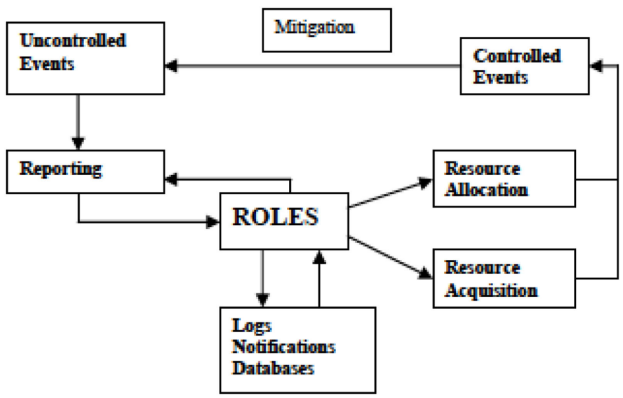

FIGURE 3 | **Work flow processes for virtual organizations (Turoff et al., 2004).**

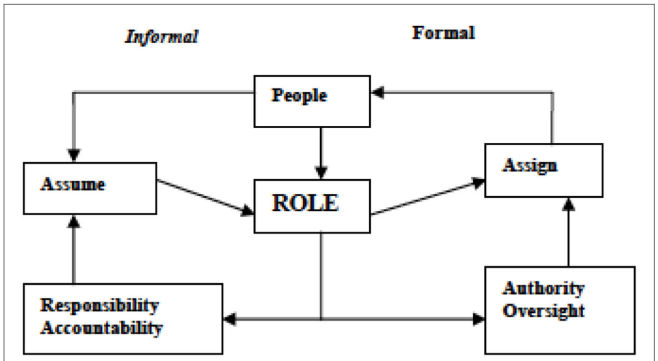

FIGURE 4 | **Meta-process for virtual organizations (Turoff et al., 2004).**

researchers see SM as a direct way to provide information between the response organization and community members (Flynn and Bates, 2011; Appleby, 2013).

The use of SM gives disaster-related organizations a unique way to connect individuals who may not be geographically impacted by the incident (Palen et al., 2009). By providing diverse avenues for communication, SM extends the reach of a disaster past its own community and creates more sources for information dissemination and collection. However, these "backchannel" avenues can also provide channels for misinformation and confusion (Sutton et al., 2008). Yet, the benefits of SM outweigh the weaknesses.

Due to increasing popularity, many agencies incorporated SM into their communications and public relations strategies team in addition to promoting services and providing information regarding their mission and community events. For example, Facebook and Twitter have been used after disasters, such as Hurricane Katrina or the Great East Japan Earthquake, to help individuals locate missing family members or verify significant others were alive. Additional examples of SM use is via YouTube, which increased in popularity as organizations began to post informational and instructional videos to help prepare communities to respond to a crisis, thereby increasing resiliency (Appleby, 2013). Furthermore, SM has been used to accumulate funds for relief efforts. Some organizations have promoted monetary donations through the use of a Twitter hashtag or a text message from specific cellular providers (Flynn and Bates, 2011).

CONCLUSION

When identifying benefits and challenges for ICT use, it is important to recognize the historical advances. Moreover, it is difficult to address every disaster or event and keep from any negative impacts. However, advances in policies and practice provide hope for effective crisis communication and response for future disaster situations. The demonstration of strategic and technical issues in the response to 9/11 prompted needed changes in policies and practice. For instance, there was a change in depending upon one physical command center. Moreover, virtual organizations became an intrinsic part of communication infrastructure to enhance capabilities and inform communities (Turoff et al., 2004). Response to the aforementioned extreme events also highlighted the benefit of equipment redundancy as a characteristic for reliable communications. As stated by Fu (2011), "the idea of built-in architectural redundancy is demonstrated by revisions made by phone service providers who no longer route multiple lines of communication through the same hub. Agencies also duplicate their protocols to ensure that certain tasks are completed by at least one department" (p. 109).

Another benefit is the naturally evolving realm of ICT itself. In past events, there were issues of connecting local systems or managing coordination events (Manner et al., 2010; Hallahan and Peha, 2008). However, development of the Internet and the use of ICT led to generation of critical communication points that can intelligently route information and provide flexibility (Kapucu, 2006). This connects to the ability to cover all geographic areas to maximize capacity and promote strategic infrastructure allocation (Meissner et al., 2002; Peha, 2006). Although the system is not fully reaching, there are rural areas with limited resources that are being reached making concerns about their remote nature less extensive (Donner and Rodríguez, 2008; Kapucu et al., 2013). In addition, developing trust between local, state, and federal agencies further supports preparation, mitigation, response, and recovery activities (Hu and Kapucu, 2014).

Aside from benefits, there are critical challenges beginning with the debate on centralized versus a decentralized system (Liu et al., 2014). A centralized system is considered more efficient and projected to outperform a decentralized system with regard to managing public safety communication networks. However, a decentralized system is flexible, adaptable to local needs, and results in higher social welfare (Kapucu, 2006; Peha, 2006). In terms of emergency management, the response hinges on knowledge of communities and the capabilities of its members (Kapucu and Liou, 2014). If response agencies are unaware of community dynamics, then issues with technology and sharing will occur and affect response activities. Strong information sharing between local, state, and federal organizations is critical for efficient and effective recovery; therefore, it is important to understand the community's abilities to prepare, mitigate, respond, and recover from an event (Palen et al., 2009; Kapucu et al., 2013; Waugh and Liu, 2014). Another challenge is the inability for EM to "hide" negative impacts of disasters or extreme events. Every situation causes communities to question the ineffectiveness of response organizations. This is impacted by the frequency of action, or lack thereof, during response activities (Turoff et al., 2004).

AUTHOR NOTES

Dr. Naim Kapucu, Ph.D., is director and professor of public policy and administration and founding director of the Center for Public and Non-profit Management (CPNM) in the School of Public Administration at the University of Central Florida (UCF). His main research interests are network governance, emergency and crisis management, decision-making in complex environments, and organizational learning and design. His work has been published in *Public Administration Review, Administration and Society, Journal of Public Administration Research and Theory, the American Review of Public Administration, and Disasters*, among many others. His recent book *Disaster Vulnerability, Hazards and Resilience,* was published in 2012 (with Rivera). He teaches network governance, public service leadership, emergency and crisis management, research methodology, and analytic techniques for public administration courses. Brittany "Brie" Haupt, M.Ed., is a Graduate Research Associate at the University of Central Florida. Her research interests include the areas of cultural competency, emergency management communication, community resilience, and competency-based education. She has published in *Public Administration Review, Disaster Prevention and Management* and presented at the American Society for Public Administration along with previous presentations centered on identity and development through her research efforts.

AUTHOR CONTRIBUTIONS

All authors listed have made substantial, direct, and intellectual contribution to the work and approved it for publication.

FUNDING

This material is based on work supported by the National Science Foundation under grant no NSF EARS-2014-1443946, titled Collaborative Research: Pervasive Spectrum Sharing for Public Safety. Dr. NK serves as PI for the grant.

REFERENCES

Abusch-Magder, D., Bosch, P., Klein, T. E., Polakos, P. A., Samuel, L. G., and Viswanathan, H. (2007). 911-NOW: A network on wheels for emergency response and disaster recovery operations. *Bell Labs Tech. J.* 11, 113–133. doi:10.1002/bltj.20199

Ansari, N., Zhang, C., Rojas-Cessa, R., Sakarindr, P., and Hou, E. S. (2008). Networking for critical conditions. *IEEE Wireless Commun.* 15, 73–81. doi:10.1109/MWC.2008.4492980

Appleby, L. (2013). *Connecting the Last Mile: The Role of Communications of the Great East Japan Earthquake*. Available at: http://internews.org/research-publications/connecting-last-mile-role-communications-great-east-japan-earthquake

Becerra-Fernández, I., Prietula, M., Valerdi, R., Madey, G., Rodríguez, D., and Wright, T. (2008). "Design and development of a virtual emergency operations center for disaster management research, training, and discovery," in *Proceedings of the 41st Annual Hawaii International Conference of System Sciences* (Hawaii: IEEE), 27–27.

Bharosa, N., Lee, J., and Janssen, M. (2010). Challenges and obstacles in sharing and coordinating information during multi-agency disaster response: propositions from field exercises. *Inform. Syst. Front.* 12, 49–65. doi:10.1007/s10796-009-9174-z

Birkland, T. A. (2009). Disasters, lessons learned, and fantasy documents. *J. Contingen. Crisis Manag.* 17, 146–156. doi:10.1111/j.1468-5973.2009.00575.x

Black, D. R., Dietz, J. E., Stirratt, A. A., and Coster, D. C. (2014). Do social media have a place in public health emergency response? *J. Emerg. Manag.* 13, 217–226. doi:10.5055/jem.2015.0235

Boin, A., and O'Connell, A. (2007). Preparing for critical infrastructure breakdowns: the limits of crisis management and the need for resilience. *J. Contingen. Crisis Manag.* 15, 50–59. doi:10.1111/j.1468-5973.2007.00504.x

Bretschneider, S. I., and Mergel, I. (2011). "Technology and public management information systems," in *The State of Public Administration: Issues, Challenges, and Opportunities*, eds D. C. Menzel, and H. L. White (Aramonk, NY: ME Sharpe), 187–203.

Buono, C. J., Chan, T. C., Griswold, W. G., Huang, R., Liu, F., Killeen, J., et al. (2008). "WIISARD: wireless Internet information system for medical response to disasters," in *Proceedings of the 5th International Conference on Information Systems for Crisis Response and Management (ISCRAM 2008)* (Washington, DC), 126–126.

Celik, S., and Corbacioglu, S. (2010). Role of information in collective action in dynamic disaster environments. *Disasters* 34, 137–154. doi:10.1111/j.1467-7717.2009.01118.x

Chiu, D. K., Lin, D. T., Kafeza, E., Wang, M., Hu, H., Hu, H., et al. (2010). Alert based disaster notification and resource allocation. *Inform. Syst. Front.* 12, 29–47. doi:10.1007/s10796-009-9165-0

Comfort, L. K. (2007). Crisis management in hindsight: cognition, communication, coordination, and control. *Public Adm. Rev.* 67, 189–197. doi:10.1111/j.1540-6210.2007.00827.x

Computer Science and Telecommunications Board. (2003). "The Internet under crisis conditions: learning from September 11," in *National Research Council of the National Academies* (Washington, DC: The National Academies Press), 9–10.

Department of Homeland Security. (2014). *National Emergency Communications Plan*. Available at: http://www.dhs.gov/sites/default/files/publications/2014%20National%20Emergency%20Communications%20Plan_October%2029%202014.pdf

Donner, W., and Rodríguez, H. (2008). Population composition, migration and inequality: the influence of demographic changes on disaster risk and vulnerability. *Soc. Forces* 87, 1089–1114. doi:10.1353/sof.0.0141

Faulhaber, G. R. (2006). Solving the interoperability problem: are we on the same channel: an essay of the problems and prospects for public safety radio. *Federal Commun.* 59, 493.

Federal Communications Commission. (2010). *National Broadband Plan*. Available at: https://www.fcc.gov/national-broadband-plan

Federal Emergency Management Agency. (2013). *Social Media in Emergency Management*. Available at: https://training.fema.gov/EMIWeb/IS/courseOverview.aspx?code=is-42

Federal Emergency Management Agency. (2014). *Effective Communication*. Available at: https://training.fema.gov/EMIWeb/IS/courseOverview.aspx?code=IS-242.b

Federal Emergency Management Agency. (2015). *Disaster Emergency Communications Division*. Available at: http://www.fema.gov/disaster-emergency-communications-division

Fiedrich, F., and Burghardt, P. (2007). Agent-based systems for disaster management. *Commun. ACM* 50, 41–42. doi:10.1145/1226736.1226763

Flynn, S., and Bates, S. (2011). *Connecting America: Building Resilience with Social Media*. Available at: https://www.cnponline.org/wp-content/uploads/2014/04/Connecting-America.pdf

Fu, L. (2011). The government response to 9/11: communications technology and the media. *Lib. Archiv. Security* 24, 103–118. doi:10.1080/01960075.2011.592034

Habib, I., and Mazzenga, F. (2008). Wireless technologies advances for emergency and rural communications. *IEEE Wireless Commun.* 15, 6–7. doi:10.1109/MWC.2008.4547516

Hallahan, R., and Peha, J. M. (2008). "Quantifying the costs of a nationwide broadband public safety wireless network," in *36th Telecommunications Policy Research Conference*. Available at: http://repository.cmu.edu/cgi/viewcontent.cgi?article=1039&context=epp

Hu, Q., and Kapucu, N. (2014). Information communication technology utilization for effective emergency management networks. *Publ. Manag. Rev.* 18, 323–348. doi:10.1080/14719037.2014.969762

Hu, Q., Knox, C. C., and Kapucu, N. (2014). What have we learned since September 11, 2001? A network study of the Boston Marathon bombings response. *Public Adm. Rev.* 74, 698–712. doi:10.1111/puar.12284

Jefferson, T. L. (2006). Using the internet to communicate during a crisis. *VINE* 36, 139–142. doi:10.1108/03055720610682933

Jennings, R. B., Nahum, E. M., Olshefski, D. P., Saha, D., Shae, Z. Y., and Waters, C. (2006). A study of internet instant messaging and chat protocols. *IEEE Network* 20, 16–21.

Kapucu, N. (2006). Interagency communication networks during emergencies boundary spanners in multiagency coordination. *Am. Rev. Publ. Adm.* 36, 207–225. doi:10.1177/0275074005280605

Kapucu, N., Berman, E., and Wang, X. (2008). Emergency information management and public disaster preparedness: lessons from the 2004 Florida hurricane season. *Int. J. Mass. Emerg. Disasters* 26, 169–197.

Kapucu, N., and Garayev, V. (2012). Designing, managing, and sustaining functionally collaborative emergency management networks. *Am. Rev. Public Adm.* 20, 1–19. doi:10.1177/0275074012444719

Kapucu, N., Hawkins, C. V., and Rivera, F. I. (2013). Disaster preparedness and resilience for rural communities. *Risk Hazards Crisis Publ. Policy* 4, 215–233. doi:10.1002/rhc3.12043

Kapucu, N., and Liou, K. T. (2014). "Disasters and development: investigating an integrated framework," in *Disaster and Development*, eds N. Kapucu, and K. T. Liou (Switzerland: Springer International Publishing), 1–15.

Kapucu, N., and Özerdem, A. (2011). *Managing Emergencies and Crises*. Burlington: Jones & Bartlett Publishers.

Kapucu, N., and Van Wart, M. (2006). The emerging role of the public sector in managing extreme events: lessons learned. *Adm. Soc.* 38, 279–308. doi:10.1177/0095399706289718

Latonero, M., and Shklovski, I. (2011). Emergency management, Twitter, and social media evangelism. *Int. J. Inform. Syst. Crisis Res. Manag.* 3, 1–16. doi:10.4018/jiscrm.2011100101

Liu, Y., Guo, H., and Nault, B. R. (2014). Centralized versus decentralized provision of public safety networks. *Centralized Decentralized Prov. Publ. Safety Technol.* 1–27.

Manner, J. A., Newman, S., and Peha, J. M. (2010). "The FCC plan for a public safety broadband wireless network," in *38th Telecommunications Policy Research Conference*. Available at: http://www.ece.cmu.edu/~peha/FCC_plan_for_public_safety.pdf

Manoj, B. S., and Baker, A. H. (2007). Communication challenges in emergency response. *Commun. ACM* 50, 51–53. doi:10.1145/1226736.1226765

McEntire, D. A. (2007). *Disciplines, Disasters, and Emergency Management: The Convergence and Divergence of Concepts, Issues and Trends from the Research Literature*. Springfield: Charles C Thomas Publisher.

Mecella, M., Angelaccio, M., Krek, A., Catarci, T., Buttarazzi, B., and Dustdar, S. (2006). "Workpad: an adaptive peer-to-peer software infrastructure for supporting collaborative work of human operators in emergency/disaster scenarios," in *International Symposium on Collaborative Technologies and Systems*, 173–180.

Meissner, A., Luckenbach, T., Risse, T., Kirste, T., and Kirchner, H. (2002). "Design challenges for an integrated disaster management communication and information system," in *IEEE Workshop on Disaster Recovery Networks, June 24*, New York.

O'Grady, P. (2005). A new medium comes of age. *New Statesman* 134, 14–15.

Palen, L., Vieweg, S., Sutton, J., and Liu, S. B. (2009). Crisis informatics: studying crisis in a networked world. *Soc. Sci. Comput. Rev.* 27, 467–480. doi:10.1177/0894439309332302

Peha, J. M. (2006). Fundamental reform in public safety communications policy. *Federal Commun. L. J.* 59, 517.

Peha, J. M. (2015). *From TV to Public Safety: The Need for Fundamental Reform in Public Safety Spectrum and Communications Policy*. Available at: http://repository.cmu.edu/cgi/viewcontent.cgi?article=1022&context=epp

Roeder, L. (2014). Understanding emergency information management. *J. Emerg. Manag. (Weston, Mass.)* 13, 188–190. doi:10.5055/jem.2015.0231

Roman, J. H., Collins, L. M., Mane, K. K., Martinez, M. L., Dunford, C. E., and Powell, J. E. Jr. (2008). "Reducing information overload in emergencies by detecting themes in web content," in *Proceedings of the Fifth International Conference on Information Systems for Crisis Response and Management (LA-UR-08-2522)* (Washington, DC), 101–107.

Rysavy, P. (2015). "Spectrum sharing: the promise and the reality," in *Wireless Spectrum Research Development Workshop IV* (Cambridge, MA: MIT). Available at: http://www.rysavy.com/Articles/2012_07_Spectrum_Sharing.pdf

Steen, M. (2015). *Virtual Operations Support Teams Monitor Incidents via Social Media*. Available at: http://www.emergencymgmt.com/disaster/Virtual-Operations-Support-Teams-Monitor-Incidents-via-Social-Media.html

Sutton, J., Palen, L., and Shklovski, I. (2008). "Backchannels on the front lines: emergent uses of social media in the 2007 Southern California wildfires," in *Proceedings of the International Community on Information Systems for Crisis Response and Management Conference* (Washington, DC: ISCRAM), 1–9.

Sylves, R. (2014). *Disaster Policy and Politics: Emergency Management and Homeland Security*. Washington, DC: CQ Press.

Turoff, M., Chumer, M., de Walle, B. V., and Yao, X. (2004). The design of a dynamic emergency response management information system (DERMIS). *J. Inform. Technol. Theory Appl.* 5, 3.

Van De Walle, B., and Turoff, M. (2007). Information systems: emerging trends and technologies emergency response. *Commun. ACM* 50, 28–31.

Van De Walle, B., Turoff, M., and Hiltz, S. R. (2010). *Information Systems for Emergency Management*. Armonk, NY: M.E.Sharpe.

Waugh, W. L. (2003). Terrorism, homeland security and the national emergency management network. *Publ. Org. Rev.* 3, 373–385. doi:10.1023/B:PORJ.0000004815.29497.e5

Waugh, W. L., and Liu, C. Y. (2014). "Disasters, the whole community, and development as capacity building," in *Disaster and Development*, eds N. Kapucu, and K. T. Liou (Switzerland: Springer International Publishing), 167–179.

Waugh, W. L., and Streib, G. (2006). Collaboration and leadership for effective emergency management. *Public Adm. Rev.* 66, 131–140. doi:10.1111/j.1540-6210.2006.00673.x

White House. (2013). "Expanding America's leadership in wireless innovation," in *White House, Office of the Press Secretary*. Available at: http://assets.fiercemarkets.net/public/newsletter/fiercewireless/whitehousememo.pdf

Conflict of Interest Statement: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.