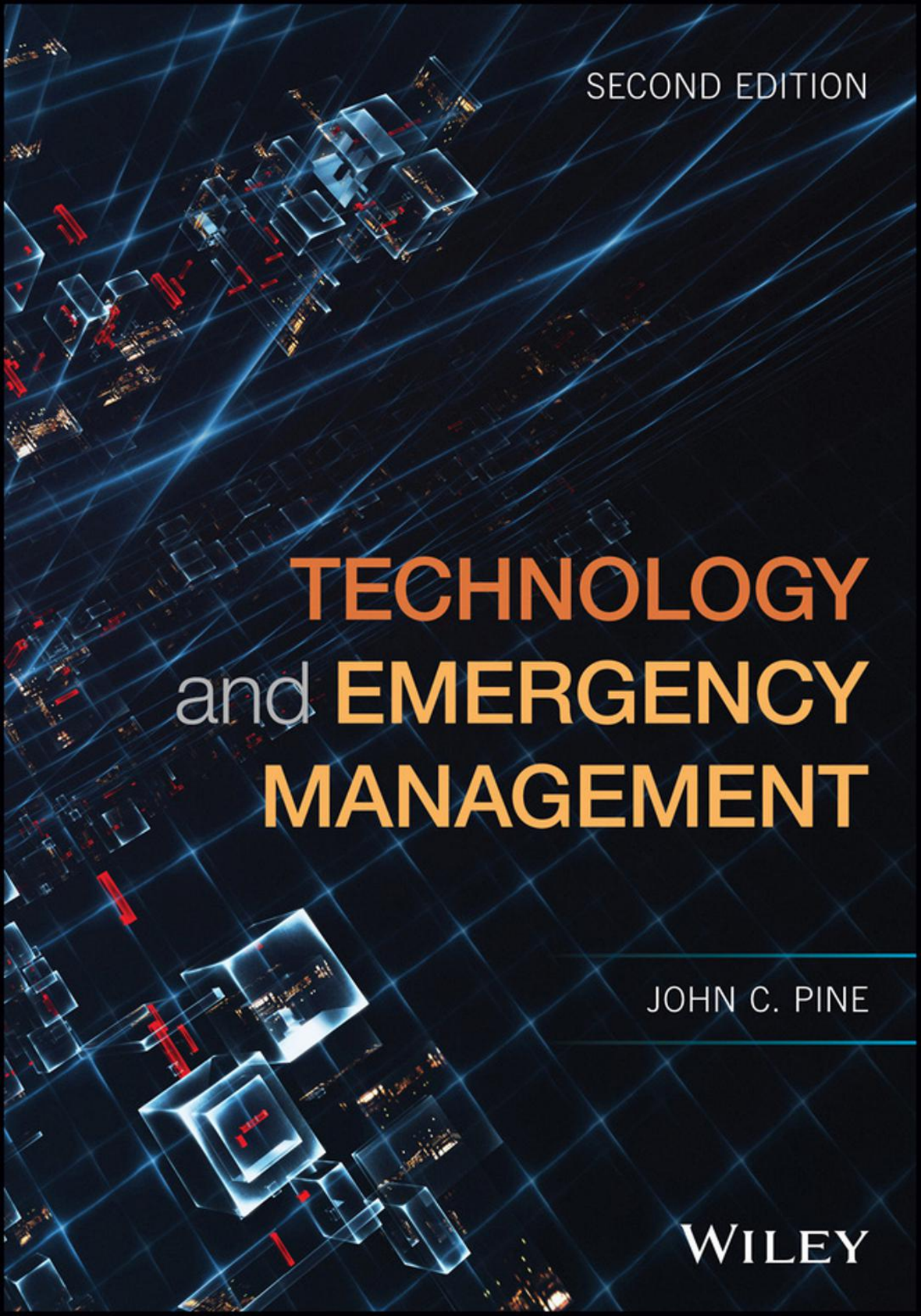

SECOND EDITION
TECHNOLOGY
and EMERGENCY
MANAGEMENT
JOHN C. PINE
WILEY

Technology and Emergency Management

Technology and Emergency Management

Second Edition

John C. Pine, Ed.D.

Research Professor
Department of Geography and Planning
Appalachian State University, Boone, NC, USA

WILEY

This edition first published 2018

First Edition published: 2007

Registered Office
John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, USA

Editorial Office
111 River Street, Hoboken, NJ 07030, USA

For details of our global editorial offices, customer services, and more information about Wiley products visit us at www.wiley.com.

Wiley also publishes its books in a variety of electronic formats and by print-on-demand. Some content that appears in standard print versions of this book may not be available in other formats.

Library of Congress Cataloging-in-Publication Data

Names: Pine, John C., 1946– author.
Title: Technology and emergency management / John C. Pine, Dr. John C. Pine, Professor, Department of Geography and Planning, Appalachian State University in Boone, North Carolina.
Other titles: Technology in emergency management.
Description: Second Edition. | Hoboken : Wiley, 2018. | Revised edition of the author's Technology in emergency management, c2007. | Includes bibliographical references and index. |
Identifiers: LCCN 2017018770 (print) | LCCN 2017034826 (ebook) | ISBN 9781119234227 (pdf) | ISBN 9781119235521 (epub) | ISBN 9781119234081 (paperback)
Subjects: LCSH: Emergency management–Technological innovations. | Emergency management–Data processing. | Information storage and retrieval systems–Emergency management. | Emergency communication systems.
Classification: LCC HV551.2 (ebook) | LCC HV551.2 .P56 2017 (print) | DDC 363.34028/4–dc23
LC record available at https://lccn.loc.gov/2017018770

Cover Design: Wiley
Cover Image: © BlackJack3D/Gettyimages

Set in 11/13pt Berkeley by SPi Global, Pondicherry, India

10 9 8 7 6 5 4 3 2 1

CONTENTS

CONCEPT

The Emergency Management Institute within the Federal Emergency Management Agency initiated the development of this publication in support of disaster science and emergency management academic programs in higher education institutions. Individuals working in disaster and emergency agencies wanted a better understanding of technology tools and their application to emergency management. Universities and colleges had developed a broad curriculum that was intended to prepare individuals for a career in emergency management in public, private, and nonprofit organizations. The scope of this book was developed in collaboration with representatives from disaster planning, response and recovery agencies, and the staff of the Emergency Management Institute.

The first edition of *Technology in Emergency Management* in 2007 provided an introduction to a rapidly developing set of resources for disaster preparedness, mitigation, response, and recovery. Much has changed since that time and this second edition provides a solid base for the many technologies that have become a critical part of emergency management within many organizations. This second edition not only clarifies the current state of the use of technology in emergency management but also provides a foundation for understanding the many emerging technologies that will be used by agencies in the future.

Book Organization

The book is organized to introduce the role of technology in emergency management and provide a context for addressing specific technologies and their use by agencies in emergency preparedness, mitigation, response, and recovery. The tools and resources examined in this book have been applied throughout the world as public, private, and nonprofit organizations attempt to deal with ever changing hazards and disaster impacts. It is hoped that by clarifying what technologies are being applied to the threats and impacts of disasters we can ensure that our citizens, businesses, and infrastructure are protected.

Technical Information

Technology and Emergency Management includes 11 chapters and is approximately 300 pages in length. The book includes many photographs and graphics and data tables. Each of the chapters clarifies the learning outcomes and intended outcomes along with goals and outcomes for the reader. Case studies are used throughout each chapter to demonstrate how various technologies were used in dealing with hazards and disasters. Terms are clearly defined and questions are posed throughout the book to focus on the application of technology in various situations. Today, there has been extensive research on the nature and use of technologies in disasters. An extensive reference list is included with each chapter to clarify the source for many of the concepts introduced in the text and to support further reading.

ABOUT THE AUTHOR

John C. Pine was Director of the Research Institute for Environment, Energy & Economics (RIEEE) and is Research Professor, Department of Geography and Planning, Appalachian State University, Boone, NC. He joined the Appalachian faculty in 2009 after serving 30 years at Louisiana State University in Baton Rouge where he directed a graduate and undergraduate Disaster Science and Management Program. He also served as a Professor in the Department of Geography and Anthropology and the Department of Environmental Sciences conducting research on disasters and emergency management. His research and publications focus on emergency preparedness and operations, risk assessment, and disaster recovery. He has worked with many federal, state, and local entities to identify tools and strategies to enhance community preparedness and ensure the resilience of communities impacted by disasters. His recent publications include ***Hazards Analysis: Reducing the Impact of Disasters*** from Taylor Francis Publishers in 2014, which utilizes many of the technologies addressed in this text. He serves on the board of directors for the New River Conservancy, a multistate conservation agency. His publications have been included in *The Journal of Disaster Studies, Policy and Management, Disasters, Journal of Race and Society, International Journal of Mass Emergencies and Disasters, Oceanography, Journal of Emergency Management, Natural Disaster Review, Journal of Environmental Health,* and *the Journal of Hazardous Materials*. He received his Doctorate in Higher Education Administration and Public Administration from the University of Georgia, Athens, in 1979.

Office Address: 124 North Forrest Ave. Lookout Mountain, TN 37350, USA
E-Mail: pinejc@appstate.edu, Phone: (828) 262–2764 (Office)
Web Site: http://www.rieee.appstate.edu

LIST OF CONTRIBUTORS

Dr. Andrew Curtis
Department of Geography, Kent State University, Kent, OH, USA

Dr. Jacqueline W. Curtis
Department of Geography, Kent State University, Kent, OH, USA

Josh Kastrinsky
Coastal Resilience Center of Excellence, University of North Carolina at Chapel Hill, Chapel Hill, NC, USA

Dr. John J. Kiefer
Department of Political Science, University of New Orleans, New Orleans, LA, USA

Dr. Burke McDade
Department of Geography and Planning, Appalachian State University, Boone, NC, USA

Dr. Jessica Mitchell
Department of Geography and Planning, Appalachian State University, Boone, NC, USA

Dr. Cindy Norris
Department of Computer Science, Appalachian State University, Boone, NC, USA

Dr. John J. Walsh Jr.
Program in Disaster Research and Training, Vanderbilt University Medical Center, Nashville, TN, USA

ABOUT THE COMPANION WEBSITE

This book is accompanied by Instructor and Student companion websites:

www.wiley.com/go/pine/tech&emergmgmt_2e

The Instructor website contains:

- MCQ's
- Self checks,
- Review questions,
- Applying This Chapter
- You try it
- Solutions

The student website contains:

- MCQ's
- Self checks,
- Review questions,
- Applying This Chapter
- You try it

1

THE NEED FOR TECHNOLOGY IN EMERGENCY MANAGEMENT

Starting Point

Go to www.wiley.com/go/pine/tech&emergmgmt_2e to assess your knowledge of using technology.
Assess your knowledge of emergency management and technology. (Determine where you need to concentrate your effort.)

What You'll Learn in This Chapter

- The definitions of focusing events and windows of opportunity
- The types of technology as applied to the emergency management process
- How technology can assist in emergency preparedness, mitigation, response, and recovery

After Studying This Chapter, You'll Be Able To

- Examine what technology is used in emergency management.
- Examine what technology tools have been applied during disasters.
- How focusing events can be used to gain community support for greater emergency management resources.

Goals and Outcomes

- To be able to select technology that improves disaster preparedness, response, mitigation, and recovery
- To perform a comprehensive technology needs assessment for emergency management
- To understand the value of encouraging a community to commit greater resources toward emergency management by using focusing events and the needs assessment

Technology and Emergency Management, Second Edition. John C. Pine.

Companion website: www.wiley.com/go/pine/tech&emergmgmt_2e

INTRODUCTION

We live in a highly connected global community where we have the potential to observe the nature and extent of disasters firsthand. We can receive and transmit information within seconds and can communicate from anywhere, at any time, and anyplace. **Technology** allows those engaged in emergency management to utilize resources from local, regional, and national organizations reflecting public, private, and nonprofit entities (Hodgkinson and Stewart, 1991). Technology may be used by those involved in emergency management in decision making, communication, hazard situational awareness, operational functioning, and public safety. Technologies have been developing at a fast pace and have had a dramatic impact on emergency management in communities, at regional and national levels.

We can only imagine the new ways that technology will evolve and be used in the future. Technology has allowed us to use a broader range of information resources and enhance resource acquisition and allocation. We, thus, have been able to make use of new tools and technologies and become more efficient and allow the public, public safety, and healthcare personnel to anticipate ad meet community needs in disasters (Cutter et al., 2015). Technology has enabled us to better analyze complex issues, enhance our decision making, and communicate in times of crisis. The key is to recognize that technology is critical in all stages of disaster management and supporting rapid scientific assessment of usable knowledge to decision makers (Alcántara-Ayala et al., 2015).

1.1 Technology and Disaster Management

Emergencies and disasters are extreme events that cause significant disruption. Effective response efforts in a disaster require timely information and deliberate decision making. Effective action requires coordinated application of resources, facilities, and efforts beyond those regularly available to handle routine problems. Disasters arise from both natural and human-caused events. Fortunately, we now have more technology tools and systems available for our use than ever before so that communities, organizations, and individuals manage effectively in a disaster. Technology provides a means of applying scientific concepts, methods, and principles to achieve desired outcomes (NRENaissance Committee, 1994). Technology supports the emergency management process including the following:

- Organizational and personal communication;
- Timely observations of the nature and extent of events;
- Enhancement in capabilities to estimate and model potential outcomes of disaster events;
- Recording the changing nature of response and recovery events;

- Communicating with multiple organizations and individuals simultaneously;
- Analyzing events to understand how disasters evolve and change over time;
- Connecting individuals and organizations so as to enhance communication;
- Extending how public and private organizations may access information as disaster evolve;
- Using mapping and geo-positioning systems (GPSs) to support situational awareness; and
- Taking advantage of hazard modeling technology to enhance our understanding of both the threats associated with hazards and their potential impacts.

Technology enables individuals and organizations to contribute to the emergency management process in new ways and with productive impacts (Kara-Zaitri, 1996). For example, we can identify the location of those in need for timely and effective emergency response. We can communicate simultaneously with multiple partners to enhance our capacity to cope with evolving complex situations. We have the tools not only to communicate with an unlimited audience but also to engage this audience in community and organizational decision making. Technologies allow both individuals and organizations to communicate and share information and make informed decisions as a disaster unfolds (Fischer, 1998). We can incorporate new information with existing data and visualize our analysis results in different and useful forms (Steering Committee, 1996). Technologies thus allow us to expand our individual and organizational capacities to more effectively prepare, mitigate, respond, and recover from disasters. Science-driven applications of technology allow disaster risk management to help communities become more resilient and reduce the human and economic impacts of disasters (Alcántara-Ayala et al., 2015).

1.1.1 Focus on Current and Emerging Technology

Alcántara-Ayala et al. (2015) suggest that there is a lack of a comprehensive assessment of disasters limiting our understanding of disaster risk research, practice, and experience. This text is intended to examine the current state of technology and emergency management and clarify how technology may be used to support those engaged in all phases of disaster management.

Technologies are being used in innovative ways and are impacting our capacity to manage effectively in times of crisis (Cutter et al., 2015; Hodgkinson and Stewart, 1991). Becoming more aware of the application of technology in emergency management allows individual citizens and organizations to cope in times of crisis and minimize or avoid the adverse effects of disasters.

Research on the weather–climate nexus has also advanced our understanding of the global oceanic forcing of drought and flood conditions across continents. Public health surveillance systems and disease outbreak detection have been enhanced with the use of the Internet and social media such as Twitter, providing real or near-real time health surveillance (Brownstein et al., 2009; Chunara et al., 2013).

Despite our great success in understanding of the dynamics and processes behind hazards, there are still many challenges related to hazards science. Specifically, we need to reduce uncertainties in forecasting of hazard events, local resolution of models, and prediction of lead time, among others (Alcántara-Ayala et al., 2015). Technology provides us with many tools and resources to allow us to reduce uncertainties.

In this chapter, we will gain insights on how technology contributes to the emergency management process and how to prioritize what technology tools are needed, and understand what resources are required for the effective use of technology.

1.2 Technology as a Management Tool

We use technology to manage our personal time and our organization. We also use technology to manage disasters and hazards. **Hazards** are events or conditions that have the potential to create loss. Technology can be used to prepare for, respond to, recover from, and mitigate future disasters. We prepare for disasters before they happen, often without definite knowledge that they will happen. We respond to disasters when they happen and recover from disasters after they happen. During and after recovery and preparation, we try to mitigate disasters. To **mitigate** a disaster means that we try to lessen the effects of the disaster. For example, to mitigate a levee collapse, the Army Corps of Engineers would try to strengthen it with sandbags or use barges to prevent the water from flooding an area. To mitigate the effects of a hurricane, many home and business owners board up their property to prevent damage. Throughout the entire emergency management cycle, technology is a key contributor to building resilient communities. Technology helps us in many ways. We can be better prepared by recording weather data in remote locations. We can do this by using satellites. We can also process information in new ways. We can directly observe disaster events. In an emergency response, computer applications allow us to access detailed information, such as data about hazardous chemicals, in more assessable ways (Pine, 2014). In mitigation and recovery, we use technology to model disasters and devise an emergency response plan. Technology is especially important in conducting mitigation activities. Mitigation activities include boarding up homes before a hurricane, evacuating an area, and other actions that reduce losses.

Alcántara-Ayala et al. (2015) stress that scientific assessments of disaster risks can contribute to our enhancement of knowledge on risk at scales ranging from local to global. Bessis et al. (2011) stress that during an emergency response information management becomes crucial.

Technology gives us the ability to receive and send information quickly. Information is critical for all involved in the emergency management process. Weather, chemical, security, and transportation information are just a few types of essential data. Quick access to information is important not only to emergency managers, but also to citizens. The quicker emergency managers can give orders to evacuate or to shelter in-place, the more lives are saved. Technology ranges from individual sensors that record information to internal and external organization

networks, including the Internet, to the Emergency Broadcast System. Communication devices are ever-changing, from vehicle-mounted applications to remote satellite systems and real-time video teleconferencing. The frequency of natural disasters has steadily increased from 405 per year in 1980 to 650 in the 1990s, 780 in 2000–2009, and 800 events in 2010s (Wirtz et al., 2014).

1.2.1 Response to Complex Disaster Events

Kapucu and Garayev (2013) note that the complex nature and great impacts of disasters proves to be a major factor for a single organization to tackle on their own and reveals the need for a collaborative approach to management. Organizations find themselves involved in a networked governance that involves shared goals and responsibilities as well as the need for a coordinated and unified action to produce desired community results. Networked governance is a combination of interorganizational interactions spread across a timeline and greatly influenced by the structure of the network, the organizational relationships, and contextual factors (Birkland, 1997; NII 2000 Steering Committee, 1996).

Networks are dynamic structures comprising multiple organizations often located in geographically different sites. A **network** is a set of two or more devices, typically called **nodes**, which are connected in some way to allow communication between them (see Chapter 2). They are multisite groups of organizations with different informal preferences, norms, and values or mandated by legal or regulatory arrangements coming together for a common goal and relying mainly on common interfaces and communication (Isett et al., 2011). Networks are generally characterized by a flexible administrative structure but impacted by issues pertaining to leadership, trust, accountability, and performance measurement (Ward and Wamsley, 2007).

Kapucu and Garayev (2013) found that information communication technology, network relationships, and network complexity all contribute to the overall effectiveness of collaborative networks and impact the sustainability of the network. They note that "emergency management networks are effective to the extent that agency relationships are enhanced for more sustainable relationships" (p. 325).

Further, the exposure of people, assets, and infrastructure in hazard-prone areas affects vulnerability (UNISDR, 2013). Changing population patterns and human-induced environmental changes increase the adverse impacts of disasters (Pelling and Blackburn, 2013) so as to create the frequency of billion dollar events.

1.2.2 Ease of Use of Technology

Technology needs to be easy to use for anyone in the emergency management process. It should not be viewed as an "expert system" only available to a select few. Ongoing training for officials will be critical in the effective use of technology in crisis situations.

Singh et al. (2009) stress the importance of information sharing in response to catastrophic events. Given the interdependence of organizations in disaster response,

organizations can benefit from sharing information quickly in a secure environment. They stress the need for information quality including timeliness, security, accessibility, completeness, accuracy, coherence, relevance, validity, and format.

We have seen improvements in hazard modeling and geo-referenced tools and spatial information (Birkland, 2014; Emrich and Cutter, 2011). We thus have great tools for evidence-based hazards analysis to base our emergency preparedness programs. Disaster risk data associated with vulnerability and exposure are a key research and policy issue. Data reflecting our assets and human capital is not widely available and must be developed beyond baseline effort to allow officials to make sound decisions (Gall et al., 2009; Kron et al., 2012; Wirtz et al., 2014).

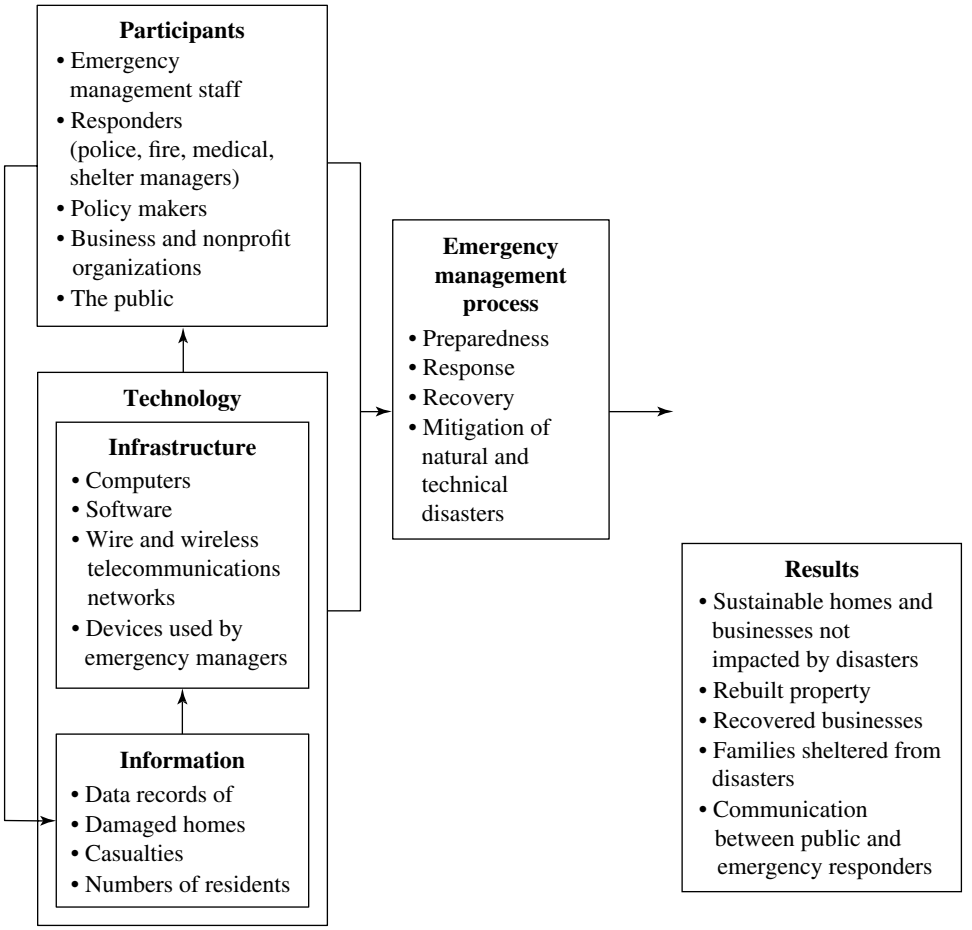
Information technology is widely used extensively and effectively throughout the United States as explained by Reddick (2011). This national study of emergency managers identified a wide range of technologies used in emergency preparedness and response. All the technologies were viewed as very helpful but the lack of financial resources and support from public officials was a significantly limiting factor on state and local capabilities. Organizational performance was enhanced where public agencies utilized e-government technology and had robust information networks and capable support staff.

1.3 Using Technologies

Also, not every new technology will be applicable for every hazard nor will every new technology be applicable to every emergency management organization. For example, you may live in California and appreciate earthquake risks and be concerned about preparing for earthquakes. Another emergency manager may live in Texas and be concerned about the next hurricane. You may wish to understand how to utilize hazard modeling and remote sensing technologies that clarify possible hazards and provide current information for an emergency response. We thus need to use technology effectively within our own region to support emergency management activities. In a survey of state emergency management agencies, information technology was viewed as very helpful and effective in the emergency planning and response phases (Reddick, 2011). Communication technologies, database resources, mapping sciences, and hazard modeling were seen as very helpful in times of disaster. Figure 1-1 diagrams the role of technology in the emergency management process.

Information technologies have been widely adopted not only in networks and communication devices but also in interconnected objects that provide information from environmental sensing associated with buildings, transportation networks, community utilities, business transactions, and the analysis of information to provide information for situational awareness. The range and extensiveness of things that are now connected allows for the manipulation and control of our systems so that if there is a system failure, immediate action may be possible for immediate action (Gubbi et al., 2013). The Internet of things allows the technology to make critical infrastructure elements and services including administration, education, healthcare, public safety, real estate, transportation, and utilities more aware, interactive and efficient (Belissent, 2010). One ends up with a smart home or office environment, smart business transactions, an array of smart city utility services, smart agriculture, and

Figure 1-1



The role of technology in the emergency management process.

transportation. Information and communication technology reflecting business, information, and social processes and able to interact with the environment to exchange data and take action without direct human intervention. The system may be user-centric but also has the capacity to operate within a large network so as to store and analyze information on an ongoing basis (Zanella et al., 2014).

FOR EXAMPLE

When Technology Fails

In May 2006, a strong earthquake with a magnitude of 6.0 hit near Tonga, a group of 170 islands. The Pacific Tsunami Warning Center in Hawaii issued a tsunami alert. Tonga, however, failed to receive the warning due to power outages. Although a tsunami did not occur there, the inability to receive the warning was troubling and is forcing the Pacific Tsunami Warning Center to create additional methods for sending warnings.

1.3.1 Technology in a Changing Environment

Emergency management is an ever-changing process and is not static. We respond to emergencies in an effort to reduce losses which are defined as loss of property and loss of life. As we saw with Hurricane Katrina (2005) and later for Hurricane Sandy (2012), natural hazards can create great losses. As we saw with the terrorist attacks of 9/11, human-caused hazards can cause substantial direct and indirect losses as well. Emergency managers try to reduce any and all potential losses. To do this, we have to prepare for disasters, have a good response plan when there is a disaster, and reduce our vulnerability to hazards. Emergency management is based on a systems approach, which means that each organization has a unique role in reducing losses and contributing to an effective local response. In addition, public agencies at all levels have to all work together to successfully prepare for and respond to hazards.

To reduce losses, emergency managers and agencies have to achieve a high degree of performance. Any misstep could cost lives. Technology not only enhances emergency response capabilities in times of crisis, but also helps in a wide range of preparedness activities. Technology has also had major effects on all organizations, allowing emergency managers to clarify the nature and extent of a potential hazard. In addition, technology can help us understand risks from hazards locally, regionally, and nationally. Further, technology such as remote sensing can be used to clarify the nature of a hazard over time.

1.3.2 Examples of Technology

Chemical sensors help us detect harmful chemicals. After the devastating tsunami of 2005, the Pacific Rim countries have installed a tsunami warning system for a timely emergency response. There are several software programs that help model what would happen if an area were hit by a disaster. For example, before Hurricane Katrina, emergency managers simulated what a Category 5 storm would do to New Orleans. The software modeling program showed public officials that the city of New Orleans would flood. These modeling programs help responders know what the outcome of different hazards could be, and therefore know what planning should address. GPS software can help in effective response effort and track supplies, getting the supplies to their target destination very quickly. They can pinpoint where to direct emergency personnel for rescue operations or postdisaster cleanup of chemical containers, boats, or building debris.

1.3.3 Communicate Quickly

With cell phones, the Internet, e-mail, and satellite phones, we can now communicate in any type of disaster, regardless of the damage to the area's infrastructure. We can also quickly send large amounts of information instantaneously through e-mail. Plus, we can quickly warn people to evacuate through the use of

information on Web sites and e-mails in addition to the traditional media of television, radio, and newsprint.

1.3.4 Develop a Better Understanding of Hazards

With our advanced equipment, we can better understand how hazards occur. For example, with the tsunami sensor system in place in the Pacific Rim, we can gain a better understanding of tsunamis and increase our ability to predict and warn residents of a tsunami.

1.3.5 Improve Response

With the enhanced ability to communicate quickly, we also know when response activities are not going well. For example, during Hurricane Katrina we all saw that there were problems getting supplies to New Orleans. Based on that information, public and nonprofit agencies were able to adapt their efforts to get supplies to the hurricane victims.

1.3.6 Increase Coordination

With increased communication and an increased ability to predict hazards, it is easier for emergency managers to work with first responders in their own community. It is also easier for emergency managers to work with state emergency management agencies and the Federal Emergency Management Agency.

1.3.7 Improve Efficiency

Computers and other forms of technology have made all organizations more efficient, which has led to a reduction in the number of people needed in each organization.

1.3.8 Training

Improve training and risk communication programs. With software programs, it is very easy to scan the results of surveys on training and risk communication programs and evaluate the results. This evaluation process leads to improvements in the programs.

The National Research Council noted in 2005 that many technology issues are human in nature and not just issues associated with the technology resources used by public agencies. They note that "better human organization, willingness to cooperate and a willingness of government at higher levels to listen to those at local levels are critical factors in making better use of information technology for disaster management" (p. 2).

1.4 Completing a Needs Assessment

FOR EXAMPLE

Training

For the use of technology to be effective, staff members must be trained. Research has indicated that many tools that are available to emergency managers and staff, such as software modeling programs, are not used because the staff is not properly trained on how to use it. FEMA and state emergency management agencies offer different types of training. Not only should staff members be trained initially on the technology, but refresher courses should also be held periodically.

1.4.1 Nature of a Needs Assessment

Participants in the emergency management system from public agencies, nonprofit and profit business organizations, and the general public all make use of technology. Each agency has its own perspective, role, needs, and capabilities, which enables the emergency management system to function. Understanding the players in the system is critical to effective use of technology. Not every emergency management organization has a budget for all the software and computers that they would like to have. Nonetheless, there are certain items that every organization should have:

- Satellite phones. During Hurricane Katrina, the New Orleans infrastructure was badly damaged. Mayor Ray Nagin was cut off from all communications and could not contact anyone at the state and federal level to update them on the situation. Mayor Nagin's staff ended up breaking into an office supply store and taking satellite phones so they could communicate their needs. This is just one example of why every emergency manager needs satellite phones.
- Web sites. Web sites are a great way to warn people of hazards, provide information on hazards, and outline mitigation strategies. For large jurisdictions, you can give specific neighborhood information. For example, some neighborhoods may be in the hazard's direct path and will be more affected than those neighborhoods outside the hazard's path. Web-based resources are being used today by public agencies, citizens, businesses, and nonprofit agencies in gathering information about disasters. The National Hurricane Center provides ongoing information about hurricanes for state and local emergency management agencies, businesses, and the general public to support decision making. The number of people who rely on Web sites for information is growing every day. At the very least, many people will use the Web as one of their sources for information.
- Digital cameras. You may need to take photos of hazard damage and transmit them quickly over the Internet to state or federal authorities. Digital cameras

were an essential resource in documenting property damage following Hurricanes Katrina and Rita.

- Access to HAZUS-MH. HAZUS-MH stands for the software program Hazards US-Multi Hazard. You can use this program to estimate losses from earthquakes, floods, and hurricane winds. The program analyzes the impact of a disaster. The program also displays estimates of damages and losses. You can request this program through the FEMA Web site (www.fema.gov).

You may be the emergency manager of a small community. If so, you may need only the basic equipment. Or you may be the emergency manager of a large jurisdiction and need every advantage new technology offers. Before you can submit a budget request for new technology, you must determine what you truly need.

1.4.2 Steps to Complete a Needs Assessment

Step 1: Inventory your use of technology today. How are you using technology and contributing to the emergency management system? What do you need to know to identify other means of utilizing technology?

Step 2: Determine your community's vulnerability. For example, if you have several industrial facilities that work with hazmat, then you may need chemical sensors installed. If you live in a community that is on the transportation route for dangerous nuclear waste, you may need cameras installed along the route within your community in an effort to prevent a terrorist hijacking. If you have completed a Hazard Vulnerability Assessment (HVA), this will go a long way in determining what type of technology you need.

Step 3: Determine how to educate the community on mitigation strategies. For example, you may determine that one way to educate the public is to provide a comprehensive Web site. You may decide that you need to send e-mail messages to residents. Or you could decide to hold several news conferences. Your strategy will most likely consist of reaching people through several different media.

Step 4: Determine how the emergency management community can better coordinate efforts between agencies (including first responders). For example, you may need satellite phones, GPS devices, or a Web portal to streamline communication and provide assistance more efficiently.

Step 5: Determine how you could be more effective in predicting hazards. For example, you may need modeling software to determine what parts of the jurisdiction would be affected by a hurricane.

Step 6: Determine how you could be more effective in responding to hazards. For example, if all traditional lines of communication are knocked out, you may need satellite phones or some other means of communication.

Step 7: Assess the threat and your needs. What is the most likely threat? What hazard would cause the most damage? What equipment and software would help you the most?

1.4.3 Implementing the Needs Assessment

Once you determine your needs, you need to prioritize them based on the greatest need. You will want to submit budget requests for new equipment and software that can be useful for all hazards. You will also want to submit budget requests for equipment that will have a direct impact should you get hit with the hazard that your community is most vulnerable to. Public organizations have been facing critical financial limitation. Expenditures for technology must be viewed as cost-effective, especially in serving the community in nonemergency operations.

Outside the normal budget cycle, a good time to submit a request for new equipment is when there is a **focusing event**. A focusing event is a national disaster resulting in large losses that receives extensive media coverage. Hurricane Katrina is a focusing event. The tsunami in the Pacific Rim is a focusing event. These events give you a **window of opportunity** to advocate for better and newer equipment. A window of opportunity is the chance to argue that a focusing event could occur locally if certain precautions are not taken. During this window of opportunity, you will need to make the argument that such a disaster "could happen here." Because this window of opportunity will not be open for long, you must take advantage of it as soon as you can. Once decision makers are over the shock of the magnitude of the disaster, they will turn their attention to the annual necessities for the community. For example, decision makers know they have to fund the school bus system, as this is a definite need. Your job is to convince decision makers to prepare for a disaster that may or may not happen.

1.4.4 Impacts of Implementing Innovation

Technology innovations have resulted in more than just new devices; they have also resulted in changes in human interactions. The changes, especially those in communications, provide more information for decision making and provide key linkages between response agencies, the public, and local enterprises. This would be a positive impact if it were not for the possibility of inaccurate, incomplete, or misdirected information. So often our developments in technology suggest that there is a quick fix for whatever our problems are (Quarantelli, 1997). A focus on gadgetry leads us in the wrong direction; we need to view technology as simply a tool with strengths and limitations. Technology brings us unprecedented amounts of information that can clarify problems or confuse us. For example, a geographic information system on a personal computer can provide us with extensive information about a jurisdiction; however, the emergency manager may need simple directions from one location to another as provided by many Internet sites, such as MapQuest or Google Earth. The key is to find the fit between technology and our emergency management needs.

The Internet provides a great resource to the emergency management community by allowing agencies to communicate in real time and in a manner that fosters coordinated outcomes and accurate activities. Internet-based system can link and integrate federal, state, local, and nonprofit agencies and facilitate resource allocation and task tracking. Because it is digital, it maintains a historical memory (data files) for evaluating agency response and coordination.

The photo in Figure 1-2, from New Orleans after Hurricane Katrina, illustrates several applications of technology and emergency management. First, the Red

Cross, local government damage assessment teams, and insurance adjusters linked photos of residents, businesses, and critical infrastructure to datasets documenting property damage from disasters. Second, the high watermarks on the house were used by a survey team to document high water elevations in the city; the high water levels were used by digital surveying equipment. Finally, digital images such as this photo of a home are used by the media, public officials, and many other organizations to document in printed and online documents and presentations the social, economic, and environmental impacts of disasters.

FOR EXAMPLE

Focusing Event: 9/11

One of the many tragedies of 9/11 was the fact that so many firefighters had faulty communications equipment, and they did not hear the directive to vacate the World Trade Center. If they had heard these instructions, there is no doubt that more lives would have been saved. The 9/11 Commission issued their report months later and urged all municipalities to ensure their communications equipment is maintained and always works properly.

Figure 1-2

Digital images used in post Katrina needs assessment September 2005.

SUMMARY

In this lesson, you have defined focusing events and windows of opportunity. You have assessed different ways that technology can help you be more effective in all phases of emergency management. You have evaluated how to perform a needs assessment and how to ask your community for more resources. Technology provides tools to link local, regional, and national resources. A technology needs assessment is critical because agencies in the emergency management system have different technology needs and financial resources. Once you know your needs, you can ask for the tools that will help you mitigate and respond to hazards more effectively.

KEY TERMS

Focusing event	A disaster resulting in losses that receives extensive media coverage as well as public attention by citizens, agencies, and public and private officials.
Hazard	An event or physical condition that has the potential to create loss (economic, social, or environmental).
Mitigate	To take an action that may reduce vulnerability to a hazard.
Network	A set of two or more devices, typically called **nodes**, which are connected in some way to allow communication between them.
Technology	The application of scientific methods or objects to achieve a practical purpose.
Window of opportunity	A chance to compare areas that have been impacted by a disaster event with other similar areas allowing emergency managers the opportunity to explain that the "same situation could happen here" and to gain support to provide resources to enhance emergency preparedness, response, recovery, and mitigation at a local, regional, or national scale.

ASSESS YOUR UNDERSTANDING

Go to www.wiley.com/go/pine/tech&emergmgmt_2e to evaluate your knowledge of using technology. This website contains MCQ's, self checks, review questions, applying this chapter and you try it.

References

Alcántara-Ayala, I., Altan, O., Baker, D., Briceño, S., Cutter, S., Gupta, H., Holloway, A., Ismail-Zadeh, A., Díaz, V. J., Johnston, D., McBean, G., Ogawa, Y., Paton, D., Porio, E., Silbereisen, R., Takeuchi, K., Valsecchi, G., Vogel, C., Wu, G., & Zhai, P. (2015). *Disaster Risks Research and Assessment to Promote Risk Reduction and Management*. Paris, France: International Council for Science and the International Social Science Council. http://www.icsu.org/ (accessed May 10, 2017).

Belissent, J. (2010). *Getting Clever About Smart Cities: New Opportunities Require New Business Models*. Cambridge, MA: Forrester Research.

Bessis, N., Asimakopoulou, E., & Xhafa, F. (2011). A next generation emerging technologies roadmap for enabling collective computational intelligence in disaster management. *International Journal of Space-Based and Situated Computing*, *1*(1), 76–85.

Birkland, T. A. (1997). *After Disaster: Agenda Setting, Public Policy, and Focusing Events*. Washington, DC: Georgetown University Press.

Birkland, T. A. (2014). *An introduction to the policy process: Theories, concepts and models of public policy making*. Abingdon: Routledge.

Brownstein, J. S., Freifeld, C. C., & Madoff, L. C. (2009). Digital disease detection—harnessing the Web for public health surveillance. *New England Journal of Medicine*, *360*(21), 2153–2157.

Chunara, R., Aman, S., Smolinski, M., & Brownstein, J. S. (2013). Flu near you: An online self-reported influenza surveillance system in the USA. *Online Journal of Public Health Informatics*, *5*(1), e53. http://nrs.harvard.edu/urn-3:HUL.InstRepos:11708633 (accessed May 5, 2017).

Cutter, S. L., Ismail-Zadeh, A., Alcántara-Ayala, I., Altan, O., Baker, D. N., Briceno, S., Gupta, H., Holloway, A., Johnston, D., McBean, G. A., Ogawa, Y., Paton, D., Porio, E., Silbereisen, R. K., Takeuchi, K., Valsechhi, G. B., Vogel, C., & Wu, G. (2015). Global risks: Pool knowledge to stem losses from disasters. *Nature*, *522*, 277–279.

Emrich, C. T., & Cutter, S. L. (2011). Social vulnerability to climate-sensitive hazards in the southern United States. *Weather, Climate, and Society*, *3*(3), 193–208.

Fischer, H. W. (1998). The role of the new information technologies in emergency mitigation, planning, response and recovery. *Disaster Prevention and Management: An International Journal*, *7*(1), 28–37.

Gall, M., Borden, K., & Cutter, S. L. (2009). When do losses count? Six fallacies of natural hazards loss data. *Bulletin of the American Meteorological Society*, *90*(6), 799–809.

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, *29*(7), 1645–1660.

Hodgkinson, P. E., & Stewart, M. (1991). *Coping with Catastrophe: A Handbook of Disaster Management*. London: Taylor & Frances/Routledge.

Isett, K. R., Mergel, I. A., LeRoux, K., & Mischen, P. A. (2011). Networks in public administration scholarship: Understanding where we are and where we need to go. *Journal of Public Administration Research and Theory*, *21*, 157–173.

Kapucu, N., & Garayev, V. (2013). Designing, managing, and sustaining functionally collaborative emergency management networks. *The American Review of Public Administration*, *43*(3), 312–330.

Kara-Zaitri, C. (1996). Disaster prevention and limitation: State of the art tools and technologies. *Disaster Prevention and Management*, *5*(1), 30–39.

Kron, W., Steuer, M., Löw, P., & Wirtz, A. (2012). How to deal properly with a natural catastrophe database—analysis of flood losses. *Natural Hazards and Earth System Sciences*, *12*(3), 535–550.

NII 2000 Steering Committee. (1996). *The Unpredictable Certainty: Information Infrastructure Through 2000*. Washington, DC: National Academies Press.

NRENaissance Committee. (1994). *Realizing the Information Future: The Internet and Beyond*. Washington, DC: National Academies Press.

Pelling, M., & Blackburn, S. (Eds.). (2013). *Megacities and the Coast: Risk, Resilience and Transformation*. London: Earthscan.

Pine, J. C. (2014). *Hazards Analysis: Reducing the Impact of Disasters*. Boca Raton, FL: CRC Press/Taylor Francis Group.

Quarantelli, E. L. (1997). Problematical aspects of the information/communication revolution for disaster planning and research: Ten non-technical issues and questions. *Disaster Prevention and Management: An International Journal*, *6*(2), 94–106.

Reddick, C. (2011). Information technology and emergency management: preparedness and planning in US states. *Disasters*, *35*(1), 45–61.

Singh, P., Singh, P., Park, I., Lee, J., & Rao, H. R. (2009). Information sharing: A study of information attributes and their relative significance during catastrophic events. In K. J. Knapp (Ed.), *Cyber-Security and Global Information Assurance: Threat Analysis and Response Solutions*. Hershey, PA: IGI Publishers.

Steering Committee. (1996). *Computing and Communications in the Extreme: Research for Crisis Management and Other Applications*. Washington, DC: National Academies Press.

UNISDR. (2013). *The Global Assessment Report on Disaster Risk Reduction*. Geneva: UN Office for Disaster Risk Reduction (UNISDR). Available at: http://www.preventionweb.net/english/hyogo/gar/2013/en/home/GAR_2013/GAR_2013_2.html (retrieved on October 16, 2014; accessed April 24, 2017).

Ward, R., & Wamsley, G. (2007). From a painful past to un uncertain future. In C. B. Rubin (Ed.), *Emergency Management: The American Experience 1900–2005* (pp. 207–242). Fairfax, VA: Public Entity Risk Institute.

Wirtz, A., Kron, W., Löw, P., & Steuer, M. (2014). The need for data: natural disasters and the challenges of database management. *Natural Hazards*, *70*, 135–157.

Zanella, A., Bui, N., Castellani, A., Vangelista, L., & Zorzi, M. (2014). Internet of things for smart cities. *Internet of Things Journal, IEEE*, *1*(1), 22–32.

2

COMPUTER NETWORKS AND EMERGENCY MANAGEMENT

Cindy Norris

Department of Computer Science, Appalachian State University, Boone, NC, USA

Starting Point

Go to www.wiley.com/go/pine/tech&emergmgmt_2e to assess your knowledge of computer systems.
(Determine where you need to concentrate your effort.)

What You'll Learn in This Chapter

- Components of a network
- Categories of networks based upon the distance spanned
- What the Internet is and its protocols and implementation
- Wired communication technologies
- Wireless communication technologies
- Internet of Things concept and implementation
- How the Internet has changed emergency management
- What a Smart City is and what technologies support it

After Studying This Chapter, You'll Be Able To

- List the types of networks based upon the distance spanned.
- Explain the difference between an access network and a backbone network.
- Compare the various types of wired access networks.
- Compare the various types of wireless network technologies.
- Understand how network communications can fail during an emergency.
- Explain why some communication technologies are more robust than others.
- Explain how the Internet is different from the traditional telephone network.
- Examine what technologies can be applied during each phase of emergency management.
- Explain how IoT technologies can be useful for emergency management.

Technology and Emergency Management, Second Edition. John C. Pine.

Companion website: www.wiley.com/go/pine/tech&emergmgmt_2e

Goals and Outcomes

- Use the Internet effectively in the emergency management process
- Come up with recovery solutions in the event of network failure
- Argue for Smart City initiatives that can support emergency management
- Select appropriate technologies that will facilitate emergency management

INTRODUCTION

The Internet and mobile communication devices allow residents and professional emergency responders to share information and coordinate activities in response to emergencies and major disasters. Many uses of the technology are planned and coordinated among federal and local organizations. For example, Presidential Alerts (warnings of national concern), Imminent Threat Alerts (alerts about weather events), and Amber Alerts (alerts about the disappearance of persons) are automatically sent to Wireless Emergency Alert–enabled cell phones (https://www.ready.gov/alerts). Another example is the Person Finder service provided by Google. This service has been used after major disasters including the Kyusyu Kumamoto Earthquake, Typhoon Yolanda, and the Boston Marathon bombing to find and report the finding of missing individuals. However, often the use of the Internet for communication during an emergency is unplanned and occurs spontaneously in response to an ongoing crisis. For example, during the peak of Hurricane Sandy, users made 20 million Twitter posts related to the storm in spite of the loss of cell phone service.

The Internet can play a particularly vital role in communication during an emergency as other forms of communication often fail. For example, during the Tohuku Earthquake and Tsunami in 2011, residents used the Internet to communicate after landlines and cell phones failed (EJC, 2012). A special hashtag, #j_j_helpme, was used on Twitter to identify people that were in need of assistance. Google engineers had Google Person Finder online within 2 hours after the earthquake and over 140 000 names were entered during the search and rescue period. In addition, Google maps helped rescuers navigate through the devastated area. In response to the failure of landlines and cell phones, Next Human Network (NHN) Corporation created the line application which allows users to exchange texts, images, video, and audio, and conduct free voice over IP (VoIP) conversations and video conferences. VoIP, or Internet telephony, allows interactive voice communication over the Internet.

The implementation of an increasingly popular concept known as the **Internet of Things (IoT)** can significantly improve the ability of emergency personnel to detect and respond to an emergency or potential emergency. The driving idea between IoT is that any device can be connected to the Internet. Consider the August 2007 collapse of the I-35W bridge over the Mississippi River in Minneapolis, Minnesota. When the bridge collapsed, dozens of cars plunged into the river resulting in the deaths of 13 people and the injury of 145. The cause of the collapse was undersized steel gusset plates that were inadequate to support the intended load of the bridge, a load that had increased over time as the bridge continued to

be resurfaced. When the new I-35W bridge was built, it was instrumented with more than 300 sensors that monitor movement, strain, load distribution, vibrations, temperature, and potential for corrosion. The data from the sensors flows through wires to a nearby computer that is hooked up to optical fiber cables leading to the Department of Transportation and University of Minnesota networks. The use of the sensor network allows structural problems to be detected and shared, averting a potential emergency.

The ability to communicate to the public and professional emergency responders is vital in the fight to protect lives and property. This chapter covers the technologies that enable communication over the Internet, the technologies behind the IoT concept, and how emergency personnel use these technologies in all four phases of emergency management: mitigation, preparedness, response, and recovery. In addition, the chapter discusses how network technologies can fail and how to recover from those failures.

2.1 What Is a Network?

A **network** is a set of two or more devices, typically called nodes, which are connected in some way to allow communication between them. A device may be a host (or end system) such as a desktop, laptop, smartphone, tablet, gaming console, security system, or even an appliance such as an Internet-enabled toaster. These devices are called end systems because they are typically the source or destination of a communication. If not an end system, a device is a connecting device, such as a **router**, which connects networks to other networks, or a switch, which is used to connect devices. Devices are connected by communication links made from various materials including coaxial cable, copper wire, optical fiber, and radio spectrum. Connecting devices receive data from one incoming communication link and forward that data onto one or more outgoing communication links. The process of determining the outgoing communication link is called **switching**. Figure 2-1 displays a picture of a local area network connected to other networks, that is, a network of networks. Note that the switch connects the end systems to create a network and the router connects the network to other networks (not shown).

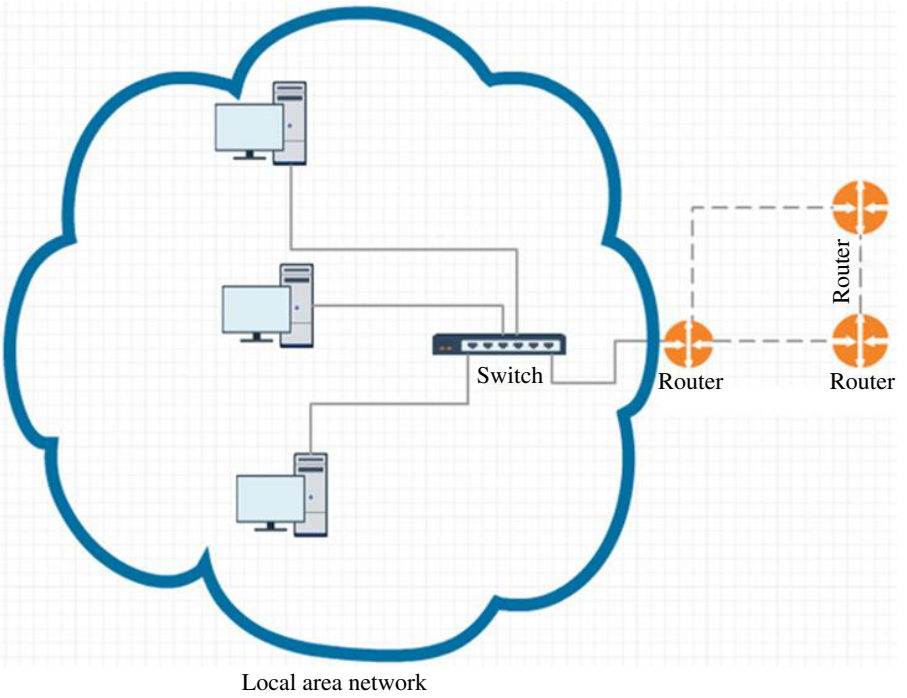
2.2 Types of Networks

A traditional method to categorize the types of networks is by the distance the network spans. This categorization yields the following types of networks: local area network (LAN), metropolitan area network (MAN), wide area network (WAN), and personal area network (PAN).

2.2.1 Local Area Network

A **local area network (LAN)** is one that connects end systems in a single geographic area such as an office, a building, or a campus. All of the devices on the network are owned by a single entity such as a university or business. A LAN could be as simple

Figure 2-1



Network diagram.

as two computers and a printer within a single office. Figure 2-1 shows a picture of a LAN consisting of an Ethernet switch connected to three desktop machines.

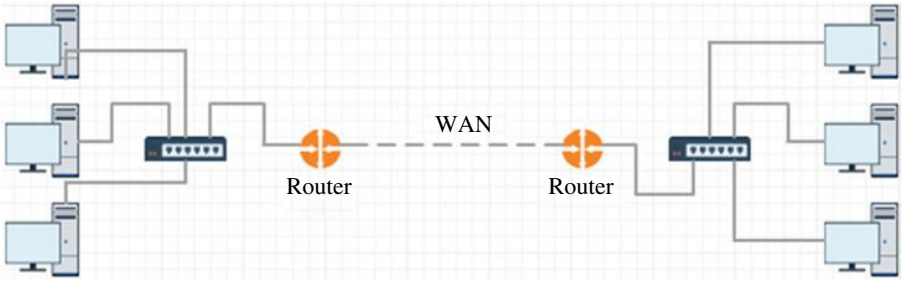
2.2.2 Metropolitan Area Network

A **metropolitan area network (MAN)** is one that spans a city or a town. A MAN connects multiple LANs via high-speed communication links such as optical fiber links. Unlike a LAN, the devices within a MAN are not necessarily owned by a single entity, but the entities that own the LANs want to be able to share resources over a high-speed connection. One of the most common ways for organizations to build this kind of network is to use microwave transmission technology. For example, TV news vans often use microwave antennae to transmit video and sound to the TV studio.

2.2.3 Wide Area Network

A **wide area network (WAN)** spans a much wider geographical region than either a LAN or a MAN, spanning a town, a state, a country, or even the world. Another significant difference is that is a LAN interconnects end systems and a WAN interconnects connecting devices, such as routers. In this respect, a WAN is similar to a MAN. The main difference between a MAN and a WAN is that a WAN is not

Figure 2-2



WAN connecting two LANs.

restricted to a particular geographic region. Figure 2-2 shows a picture of two LANS that are connected via a WAN. The routers in the picture direct the packets received from a host in one LAN to a destination host in the other LAN. The switches direct a packet to a destination within the same LAN as the source.

2.2.4 Personal Area Network

A **personal area network (PAN)** is an interconnection of devices within a short distance from each other, typically less than 10 m. In addition to allowing devices within the PAN to communicate, the PAN can support the transmission of data from the devices to the Internet by identifying one of the devices to be the master that plays the role of the Internet router. A PAN can be wired or wireless. A wired PAN is typically constructed using USB or FireWire connections. For example, you can form a wired PAN by connecting an iPhone to a Mac or Windows machine, gaining access to the Internet through the iPhone via the USB cable. Protocols for wireless PAN (WPAN) include Bluetooth and ZigBee. (Bluetooth and ZigBee are discussed later.)

2.3 The Internet

The **Internet** is a WAN that spans the entire world and interconnects hundreds of millions of computing devices. These devices include desktop machines, laptops, smartphones, high-performance computers known as servers that store and provide data, gaming consoles, and a myriad of other Internet-enabled devices.

The Internet is a **packet switched network**, which means that the data sent from a sender to a receiver is broken into chunks called packets that are transmitted independently and reassembled at the destination. These packets don't necessarily follow the same paths to the destination and therefore can arrive out of order. In addition, no resources are reserved in the path from the source to the destination thus a packet could get dropped at a router if there is no room to store the packet when it arrives. In contrast, in a **circuit switched network** a connection is established between the source and the destination and needed resources along the path are reserved before any data is transmitted. The resources along the path are

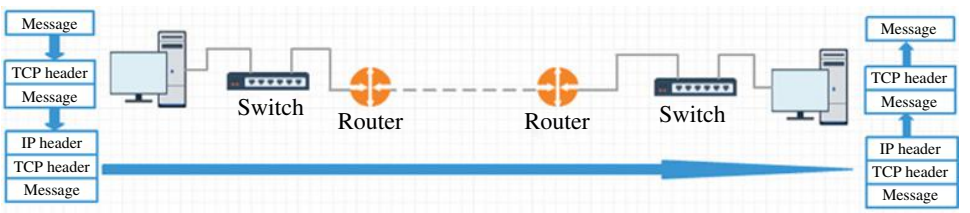
dedicated to the communication until the connection is terminated. Circuit switching is used in the traditional telephone network.

Two principal protocols, the Transmission Control Protocol (TCP) and the Internet Protocol (IP), collectively known as TCP/IP, control the sending and receiving of data across the Internet. The IP protocol specifies the format of the packets that are transmitted and received by end systems. IP packets (also known as datagrams) contain an IP header that contains, among other things, the IP addresses of the source and destination end systems. Routers along the path from the source to the destination use the destination IP address to determine the outgoing communication link upon which the packet is transmitted. A router maintains a forwarding table that maps a range of IP addresses to each communication link. Thus, the IP address and the forwarding table are used for switching. Two types of IP addresses are widely used: IPv4 and IPv6. IPv4 addresses are 32 bits supporting a total of 2^{32} (over 4 billion) devices. With the growth of the Internet, especially with the growing interest in IoT, the number of IPv4 addresses is expected to run out. Thus, IPv6 is being employed to provide more IP addresses. IPv6 addresses are 128 bits supporting 2^{128} addresses, enough to assign every grain of sand an IP address! Because of the near impossibility of an immediate change from IPv4 to IPv6, IPv4 and IPv6 addresses will probably coexist for some time.

The body of the IP packet is called the payload. Typically, the payload is a TCP segment. (The payload could be some other type of packet, but we will only discuss TCP segments.) The TCP protocol defines the format of the TCP segment and provides error-free, in order delivery of the transmitted data. Among other things the TCP header contains a segment number that allows the transmitted data to be put in order at the destination. The TCP header also contains bits, called **checksum** bits, which can be used to determine whether an error was introduced to the segment (the TCP header and/or payload) during transmission. Bit errors are generated by noise on the network. For example, cables that are too close to a noise source, such as lights, can suffer from bit errors. A simple error detection approach is to store an extra parity bit for every 8 bits in the packet. The parity bit is 0 if the number of 1s in the group of 8 bits is even; otherwise, the parity bit is 1. This very simple scheme can successfully detect an odd number of bit errors. (Note: the actual TCP checksum implementation is more sophisticated than this simple scheme.)

As can be seen in Figure 2-3 the message that is sent by an application (e.g., a Web browser) is encapsulated first in a TCP header. This encapsulation is performed

Figure 2-3



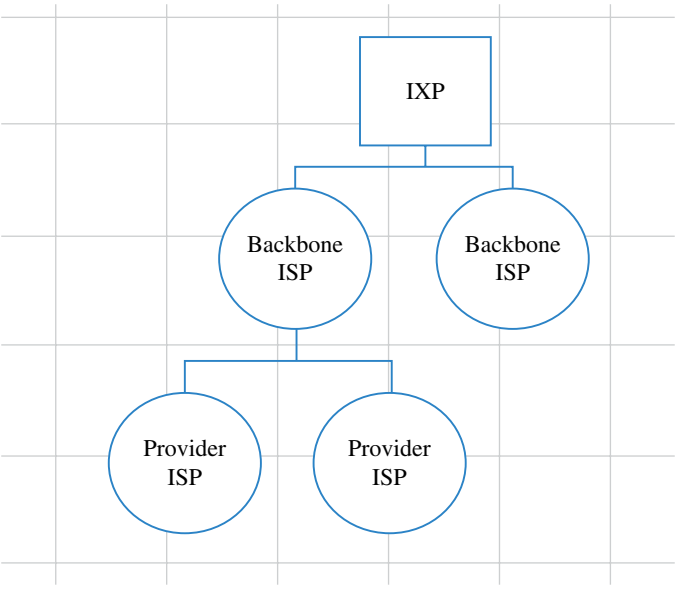
TCP/IP encapsulation/decapsulation.

by transport layer software running on the end system. In fact, for large messages, several TCP segments may be created to transport a single message. Network layer software then encapsulates the TCP segment with an IP header. Routers between the source and the destination examine each IP header in order to choose the appropriate outgoing links. The packet is decapsulated by software at the destination host. Transport layer software reassembles the TCP segments using segment numbers in the TCP headers and the message is delivered to the receiving application (e.g., a Web server).

The backbone of the Internet is a collection of large networks owned by communication companies such as Sprint, Verizon, AT&T, and NTT. These backbone networks are connected to each other at **Internet Exchange Points (IXPs)**, which is a physical infrastructure consisting of one or more network switches and routers to which the backbone networks are directly connected. The networks connected to these IXPs typically have a public peering relationship, meaning that they accept each other's traffic without charge. Provider networks are connected to the backbone networks and pay for the services of the backbone. Customer networks are connected to the provider networks; the customer networks are those that contain end systems that use the Internet. The backbone and provider networks are also known as **Internet Service Providers (ISPs)**. Figure 2-4 illustrates the organization described in this paragraph.

Often an organization desires its own private network (end systems, connecting devices, and links) to ensure that communication across the network remains confidential. However, creating the physical network to support this is very costly. Instead, an organization can create a **virtual private network (VPN)** over the Internet by encrypting data before it is transmitted over the public Internet and

Figure 2-4



Internet backbone.

decrypting it at the destination. The protocol that provides this service is IPSec. IPSec can be used in two modes. In transport mode, IPSec protects the TCP segment by encrypting it and adding to it an IPSec header and trailer. The IP header added to that is not protected by IPSec; thus the source and destination addresses are visible. Only the source and destination hosts are aware that IPSec is being employed. In tunnel mode, IPSec encrypts the entire IP packet and adds a new IP header whose destination address is the router that connects the destination host to the Internet. The router then decrypts the IP packet and delivers it to the destination.

2.4 Communication Technologies

An **access network** physically connects a host or end system to the first router, called the edge router, on its path to another end system. For example, you probably have access to the Internet via your cell phone. How is it that your cell phone connects to a router that can send your request for a particular Web page to the appropriate destination? Beyond the connection to the first router, the **core network** or backbone network is the part of the network that connects the access networks. For example, in Figure 2-2 the two LANs are access networks; the WAN is the core network. This is a very simple example. In fact, the core network can consist of many connecting devices and communication links.

Access and core networks are either **wired** or **wireless**. If the network is wired, data is transmitted across a physical medium such as twisted-pair copper wire. Wireless enables the transmission of data over a distance without requiring wires, cables, or any other electrical conductors. The data is transmitted through the air by using electromagnetic waves like radio frequencies, infrared, and microwaves. The remainder of this section discusses different technologies for creating wired and wireless networks.

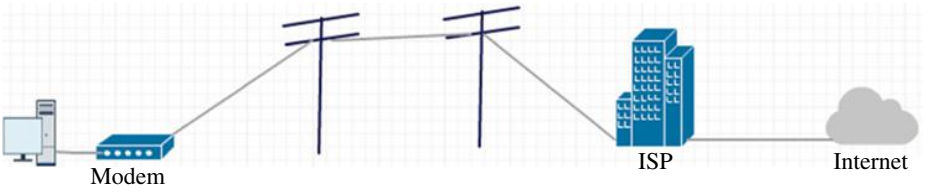
2.4.1 Wired Network Technologies

Dial-up

Before telephone companies and cable companies offered Internet access, access from the home was obtained via Dial-up over traditional twisted-pair copper wire. A computer generates digital signals and the telephone line requires audio; thus a modulator/demodulator (modem) was used to convert digital to audio and vice versa. Software on the computer would explicitly dial the ISP. Unfortunately, dial-up service is very slow and when the computer for the Internet connection is using the phone line, it cannot be used as a regular telephone. Figure 2-5 illustrates how dial-up works. Note that the user is directly dialing the ISP.

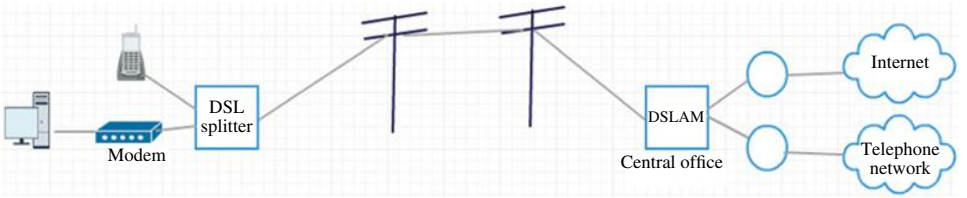
Most Internet users are now able to obtain access to the Internet via a **broadband** service. Broadband services provide a high rate of transmission over a wide range of frequencies. The wide range of frequencies allows a lot of data to be transmitted simultaneously, increasing the data rate (i.e., the number of bits transferred per second).

Figure 2-5



Dial-up.

Figure 2-6



Digital Subscriber Line.

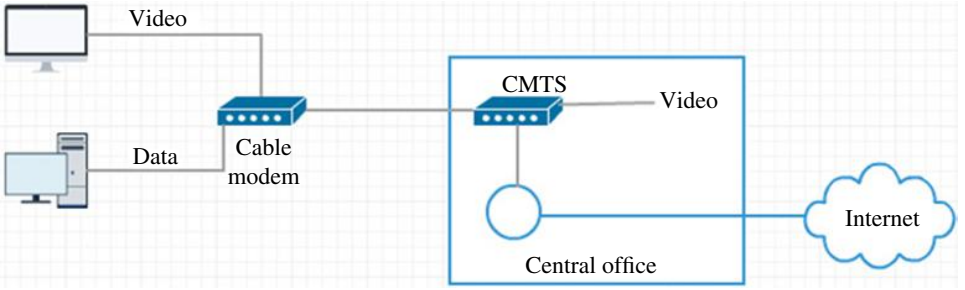
Digital Subscriber Line

Telephone companies developed the Digital Subscriber Line (DSL) to provide higher-speed, broadband, Internet access. DSL allows the telephone line to be simultaneously used for both voice and data by sending the data at a higher frequency. A home's DLS modem takes digital data and translates it to high-frequency tones for transmission over the telephone lines. At the telephone company's central office, a digital subscriber line access multiplexer (DSLAM) converts the analog signals back to digital format and directs voice communication to the telephone network and the data communication to the Internet. At the customer end, a DSL splitter separates the analog signal into the high-frequency data and low-frequency voice and forwards the Internet data to the DSL modem. This process can be seen in Figure 2-6. Note the telephone lines connect to the telephone company's central office, which separates the voice and data.

Cable

Cable companies provide television signals over a coaxial cable, which is a type of wire that consists of a center wire surrounded by insulation and a grounded shield of braided wire. The shield minimizes electrical and radio frequency interference. Cable companies provide customers with Internet access by dividing the coaxial cable bandwidth into three bands: a video band that occupies frequencies from 54 to 550 MHz, a downstream data band (for downloading data from the Internet) that occupies frequencies from 550 to 750 MHz, and an upstream data band (for uploading data to the Internet) that occupies frequencies from 5 to 42 MHz. Similar to a DSL splitter, a cable modem is used at the customer's end that separates the

Figure 2-7



Cable Internet access.

Internet data from the television data. In addition, the cable modem converts the digital computer network data into analog signals for transmission. At the cable provider's end, a cable modem termination system (CMTS) converts the analog signal back to digital format. Figure 2-7 illustrates cable Internet.

Fiber to the X

Fiber to the X where X represents the destination of the fiber is an initiative to replace traditional copper wire used for telephone communications and CATV by optical fiber. Optical fiber is flexible, transparent fiber made from glass or plastic that is used to transmit data in the form of light at a much higher rate than metal wires. In the case of fiber to the home (FTTH), the fiber extends to a box outside of a customer's home. Fiber to the last amplifier (FTTLA), or more commonly called hybrid fiber coax (HFC), is a technique that is used by cable companies to replace coaxial cable by fiber all the way to a neighborhood. Coaxial cable then extends from there to the customer's home. Optical fiber can provide enormous improvements in the rate at which data can be provided to the consumer, potentially gigabits (billions of bits) per second compared to megabits (millions of bits) per second for cable and DSL. However, most FTTH ISPs provide different rate offerings where higher rates cost more money. Much of the core network is implemented by the optical fiber cable owned by major telecommunications companies.

Ethernet

Ethernet is the most common choice for access networks in corporate and university campuses. An Ethernet LAN typically uses twisted-pair copper wire to connect end users to an Ethernet switch, which is in turn connected to an edge router. End systems communicating over Ethernet divide a stream of data into shorter pieces called frames. Each frame contains source and destination MAC addresses which are the addresses given by the manufacturer to network interfaces. An Ethernet switch then outputs a frame onto the appropriate link based upon the MAC address. The frame also contains error-checking bits so that damaged frames can be detected and discarded. Ethernet can provide transmission rates of hundreds of megabits per second.

2.4.2 Long-Range Wireless Network Technologies

This section gives an overview of Worldwide Interoperability for Microwave Access (WiMax), cellular, and satellite technologies that can be used to build a **Wireless Wide Area Network (WWAN)**. A WWAN delivers Internet access to devices in a large area. These devices are typically cell phones or mobile devices, but WWAN cards are also available for laptops.

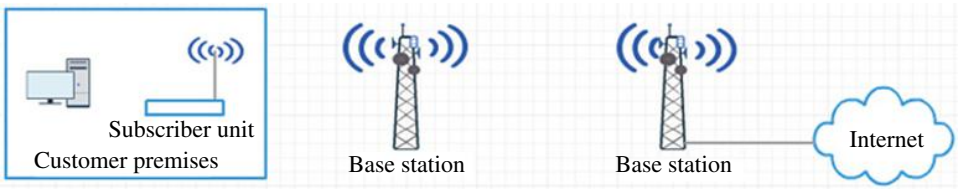
WiMax

WiMax is a wireless technology similar to Wi-Fi but operating at higher speeds and over a wider area designed to replace the use of cable or DSL. WiMax utilizes base stations that have both a transmitter and a receiver and an adaptive antenna system (AAS). The ASS antenna can focus its transmission energy in the direction of a receiver when transmitting and in the direction of the transmitter when receiving. WiMax stations can communicate with each other. A WiMax station might also have a high-bandwidth, wired connection to the Internet. WiMax customers can use a WiMax subscriber unit that connects to the WiMax network and provides Wi-Fi connectivity within the home. Or customers can connect to the WiMax network via a WiMax-enabled computer similar to how computers connect to Wi-Fi. WiMax operates on the same general principles as Wi-Fi; it sends data from one computer to another via radio signals. A computer (either a desktop or a laptop) equipped with WiMax would receive data from the WiMax base station. WiMax is also one of the versions of 4G wireless available in phones as Sprint's 4G technology, although WiMax started out as a way to deliver wireless broadband to homes and businesses. Figure 2-8 illustrates a WiMax network. Note that one of the base stations is connected to the wired Internet.

Cellular

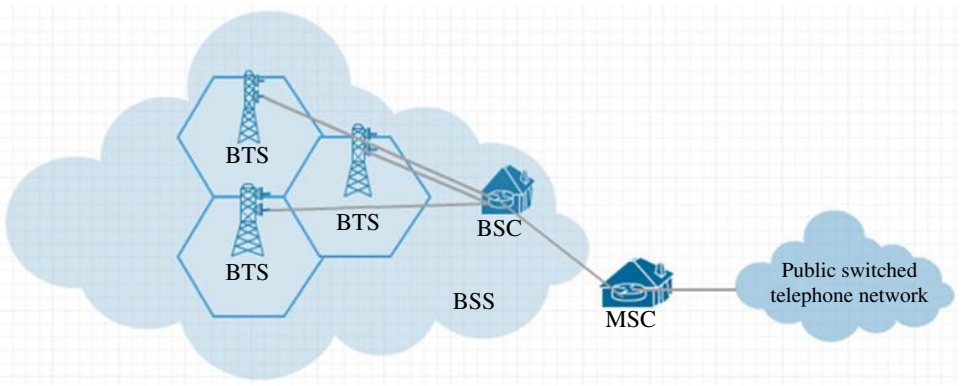
Cellular phone communication works much the same way as other wireless communication. Signals carrying voice, text, and digital data are transmitted via radio waves from one device to another. In the case of cellular networks, the data is transmitted not to a nearby access point as it is with Wi-Fi or directly from device to device as is the case with Bluetooth, but instead data is transmitted to or received from a base transceiver station (BTS) that may be quite far from the cellular phone (Figure 2-9).

Figure 2-8



WiMax network.

Figure 2-9



Cellular network architecture.

The term cellular is derived from the cellular design of the mobile network. The mobile phone network is divided into thousands of overlapping geographic areas called cells. A BTS is stored within each cell that provides service to each mobile device in the cell. The coverage area of the cell depends upon many factors including the transmitting power of the BTS and obstructions within the cell, such as obstructing building. The typical radius of a cell is between 2 and 20 km. A single base station controller (BSC) services tens of BTSs by allocating a radio channel and by handling the handoff of mobile communication from one BTS to another BTS when the signal between the current BTS and mobile device deteriorates. Together the tens of BTSs and the single BSC make up what is called a base station system (BSS). A switching office, called a mobile switching center (MSC), controls the BSS and connects the cellular network to the public switched telephone network.

Cellular technologies can be classified into generations. The 1G systems were analog and supported only voice communication. The 2G systems were designed to support digitized voice in order to provide higher-quality mobile voice communications. In addition, the transmission of digital data rather than analog data allows the frequency spectrum to be used more efficiently; thus the amount of bandwidth, that is, range of frequencies, required to transmit voice communication is smaller. Also, 2G supported the transmission of text messages. The 3G technologies provide both digital data and voice communication. Via 3G technologies, a portable device is automatically connected to the Internet; that is, there is no need to dial a number to connect. The 3G technologies allow someone to talk to anyone in the world with quality that is as good as the traditional television network. In addition, users can stream videos, surf the Internet, play games, participate in video conferences, and more. Unlike 3G technologies, 4G technologies are entirely packet based. This means that all voice and data are carried in IP datagrams. The 4G technologies also provide significantly higher upload and download rates over 3G; thus any app that requires transferring large amounts of data benefits from 4G. The 5G refers to the next generation of the

mobile network technology. In addition to providing faster speeds, 5G networks will also meet the requirements created by the IoT, for example, hundreds of thousands of simultaneous connections to be supported for massive sensor deployments.

Satellite

A satellite network consists of three types of nodes: satellites, stations, and end hosts, such as satellite phones or satellite modems. The stations communicate directly with the orbiting satellites via radio signals. There are three categories of satellites based upon their orbits, which is the path it travels around the earth. Geostationary earth orbit (GEO) satellites permanently remain 36 000 km over a single spot on the Earth. The huge distance from the ground station to a GEO satellite causes a signification delay in the time that transmitted data takes to propagate from the station to the satellite. In spite of the delay, GEOs satellites are often used in areas without access to DSL or cable-based Internet. Three GEO satellites equidistant from each other can provide full global transmission.

Medium earth orbit (MEO) satellites are located at altitudes between 5000 and 15 000 km. The primary use of these satellites is for navigation, for example for the United States' Global Positioning System (GPS), Russia's Global Global Navigation Satellite System (GLONASS), and Galileo, the Global Navigation Satellite System (GNSS) created by the European Union and European Space Agency. MEO satellites travel overhead at all times, instead of tracking with a fixed point on Earth as GEO satellites do. MEO satellites can provide constant coverage through a constellation of several satellites that are closer to Earth, offering a significantly lower propagation delay than GEO satellites.

Low earth orbit (LEO) satellites have a circular orbit about 500–2000 km above the earth's surface. Because of the smaller altitude, they take much less time (about 90 minutes) to revolve around the earth than MEOs. In addition, LEO satellites change their positions relative to the ground position quickly; thus a large number of satellites are needed if an application requires uninterrupted connectivity. For this reason, LEO satellites are often part of a group of satellites working in concert known as a satellite constellation. Low earth orbiting satellites are less expensive to launch into orbit than geostationary satellites and, due to proximity to the ground, do not require as high a signal strength. LEO satellites communicate with each other as well as with ground stations. The International Space Station, the Space Shuttle, and the Hubble Space Telescope are all in LEO. LEO satellite communication may be used in the future to provide global access to the Internet (Gershgorn, 2015).

Satellite signals are transmitted far above the earth and do not rely on towers. Satellite phones and satellite base stations can receive the signals. Because they do not rely on towers, satellite signals are especially useful in remote areas. In addition, satellites are not damaged by disasters on earth such as earthquakes and thus satellite phones can be an important means for communication in an emergency. However, if a single satellite fails, communication can be lost entirely.

2.4.3 Short-Range Wireless Network Technologies

The technologies described in this section provide short-range connectivity ranging from a few centimeters (Near Field Communication or NFC) to hundreds of kilometers. However, the uses of these technologies tend to be quite different. Wi-Fi technology is typically used to allow end systems access to the Internet, although it can also be used to connect a laptop to a Wi-Fi printer or to share documents between two nearby computers. In general, Wi-Fi is used as a substitute for high-speed cabling, such as Ethernet; thus Wi-Fi is commonly used to build a **Wireless LAN (WLAN)**. Bluetooth technology is typically used to transfer data between two Bluetooth devices, for example, between a mobile phone and a hands-free headset. Like Wi-Fi, Bluetooth can also be used as an access point to the Internet, but provides that access at a much lower rate. Bluetooth, ZigBee, Dash7, RFID, and NFC are all technologies that can be used to build **Wireless Personal Area Networks (WPAN)**. ZigBee and Dash7 both consume less power and have a higher range than Bluetooth and thus are better choices for sensor nodes in smart city applications. RFID and NFC devices are used for extremely short-range data transmission of small packets of data making them suitable for tracking objects, including people and animals. This section describes each of these in more detail.

These technologies can also be used to build a **Wireless Sensor Network (WSN)**. A WSN is a wireless network consisting of a collection of sensors to monitor physical or environmental conditions. Nodes in the WSN system communicate with each other. One node provides wireless connectivity back to the Internet.

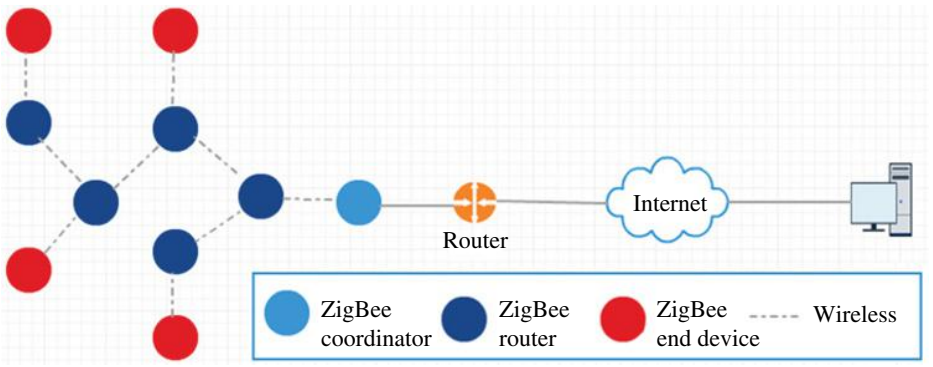
Wi-Fi

WLAN access based on IEEE 802.11 technology is known as Wi-Fi. Wi-Fi provides a low-power form of wireless transmission over short distances. The end system, usually a laptop or a cell phone, must be with a few tens of meters of the wireless router that serves as the access point. Typically, the wireless router is connected to a cable modem or DSL.

Bluetooth is a popular technology for building a WPAN known as a piconet. A piconet consists of a master device, up to seven active slave devices, and up to 255 inactive (parked) slave devices. The master device can bring an inactive device into active status at any time, after an active device is parked. The slave devices do not communicate with each other or with the Internet. All communication is through the master device. A simple example of a piconet is a fitness-monitoring device connected to a cell phone via the Bluetooth connection.

ZigBee defines technology for building a WPAN that is simpler and less expensive than Bluetooth. The ZigBee specification defines a radio protocol for communication among low-cost, low-power devices at a lower rate of transmission than Bluetooth devices. ZigBee has been successfully used in devices for control such as for lighting, irrigation, aerial vehicle (AV) systems, industrial equipment, security systems, and patient monitoring. For example, a ZigBee device can be

Figure 2-10



ZigBee wireless sensor network.

used to monitor a patient's blood pressure and heart rate and communicate the information to the hospital.

ZigBee devices are typically arranged in a mesh network where the connection is spread out among wireless nodes that can communicate with each other across a large area. The mesh network boosts data transmission range (up to 65 000 nodes can be on a single network) and provides greater fault tolerance if a node fails.

ZigBee nodes can be coordinators, routers, and end devices. Coordinators are comparable to Bluetooth master nodes and establish the network and store information like security keys that are used to encrypt transmitted data. ZigBee coordinators form the network by determining the PAN ID and the channel used for communication. Routers and end devices join the network. Routers act as intermediate nodes and relay data from other devices. End devices are low-power gadgets that can communicate with coordinators and routers but cannot transmit data to other end devices. End devices sleep most of the time in order to conserve batteries. Figure 2-10 illustrates a ZigBee WSN. The ZigBee end devices would contain sensors for things such as light, sound, temperature, pressure, gas, and so on.

Dash7

Dash7 is a long-range, low-power wireless communications standard for applications requiring modest bandwidth like sensor readings or providing the coordinates for location-based advertising. Dash7 excels at connecting things that move. Unlike Wi-Fi and Bluetooth, the "instant-on" capability of Dash7 allows connections with passing cars, buses, or people jogging. In addition, Dash7 operates at 433 MHz, which is a frequency that allows penetration through walls and supports ranges up to many kilometers. Like Bluetooth and ZigBee, Dash7 defines technology that can be used to build a WPAN where devices communicate in a master–slave relationship. However, Dash7 devices have a higher range and longer battery life.

Radio-Frequency Identification Systems

Radio-Frequency Identification (RFID) is a communication technology to uniquely identify tagged objects by transmitting radio signals. An RFID system consists of tags, a reader, and a database. The reader decodes the data stored in the tag and the data is transferred to the database for processing. RFID systems are widely used in manufacturing for tracking parts, in shipping, and in payment systems such as for toll roads. They are also being used in emergency management as described later.

RFID tags are either active or passive. Active RFID tags contain their own power source (i.e., a battery), giving them the ability to broadcast their tag. A reader within 100 m will be able to read the tag. Passive RFID tags do not have their own power source. Instead, the electromagnetic energy transmitted from an RFID reader causes the tag to activate. Because the radio waves must be strong enough to power the tags, the read range is smaller than it is for active tags. In particular, the reader must be within 25 m of the passive tag to activate and read the tag.

Near Field Communication

NFC is used in mobile devices for very short-range (10 cm or less) communication. Unlike RFID systems where an RFID device is either a tag or a reader, NFC is bidirectional; thus it is possible to share information between devices. The predominant current application of NFC is the digital wallet. A smartphone equipped with NFC can be used as a substitute for a credit card and can also be used to provide identification. In addition, since NFC communication is bidirectional, it can be used to share data (pictures, videos, contact information) between devices. Like RFID systems, NFC devices can be used for asset management; for example, in emergency response, NFC devices can be used to track people, animals, medical equipment, and so on.

2.5 The Internet and Emergency Management

In 2015, 67% of American homes had broadband Internet access (Horrigan and Duggan, 2015). This has slightly decreased from 2013 as more adults are using smartphones to access the Internet. About 13% of American adults reported in 2015 that their smartphone is the only device that they use to access the Internet; this is up from 8% in 2013. Overall access to the Internet continues to grow. Some 80% of American adults reported having either a smartphone or a home broadband subscription in 2015, compared with 78% who said this in 2013.

Being able to access the Internet has forever changed how news is produced and consumed. In the past, communication between newscasters and news consumers was one to many. Now, anyone with a phone and/or an Internet connection can contribute to the media conversation by calling into a talk show or posting to one of many available social media sites such as Facebook and Twitter.

In fact, the Internet enables government entities to serve as their own news bureaus. For example, during Hurricane Sandy, the New York Office of Emergency Management used Twitter and Facebook to provide hourly updates about evacuations, shelters, aid, and storm conditions. The Boston Police Department (BPD) used social media immediately after the Boston Marathon bombing to let people know what had occurred. The use of social media, in particular Twitter and Facebook, allowed the BPD to correct misinformation that was being spread by professional media outlets and social media sites. The public and professional news organizations alike soon realized that the most accurate information about the bombing was available on official BPD social media accounts. It is becoming increasingly more common that social media networks are a primary source of information for rescue authorities and victims following a natural or man-made disaster (Besaleva and Weaver, 2016).

The Internet has changed the hierarchical nature of information flow in an emergency situation. In the past, information flow in emergency management was top-down. Local officials would learn details about an emergency from their superiors if they needed to; likewise, community members would learn details from local officials. The Internet has changed the flow of information since the Internet is typically the source of information in an emergency and the information becomes available to all simultaneously. Misinformation and the misinterpretation of information on the Internet is a problem. However, for emergency management, the ability to communicate widely and quickly outweighs possible drawbacks.

The Internet is not immune to communication failures that occur during disasters but can sometimes stay intact or be repaired more quickly than other forms of communication. The most common cause of failure is physical damage to devices and network infrastructure (Richards, 2015). For example, hurricane force winds, floods, and seismic activity can potentially damage cell towers, power lines, and optical fiber cables. Damage to a cell tower will disrupt an area's wireless communication. A cell tower is expensive and time-consuming to repair and also requires getting a crew to the devastated area. Optical fiber cables can be even more challenging to repair because the cables are underground, making it more difficult to find the location of the damage and requiring excavation to pinpoint and repair the damage. Wireless links are also susceptible to disruption by heavy rain, snow, or fog.

Satellite-based emergency communication devices are typically the most reliable devices in an emergency situation because satellite communication is not affected by any localized conditions such as floods, power outages, fires, earthquakes, hurricanes, tornadoes, or other disasters. In addition, satellite coverage is universal. However, satellite phones are expensive and not widely used by the general public. In addition, if a single satellite fails, communication can be completely disabled and impossible to repair quickly.

In the absence of physical damage, the network infrastructure may still be unusable due to the volume of network traffic generated by those impacted by the disaster. When a disaster occurs, the network becomes inundated by videos and photos of the damage, friends and family attempting to communicate with loved

ones in the impacted area, and communications between emergency personnel. Network nodes that receive data from many downstream networks, for example, a DSLAM device that receives DSL traffic from many customers, are often the failure points for congested network. If the network becomes too congested, messages can be lost entirely.

Communication failures are less likely when there is more than one type of path between the source and destination of the communication. This way if one path is destroyed during a disaster, the other path may still be intact. For example, if a customer has both broadband Internet access via DSL or cable and Internet access via the cellular network then if a break occurs in underground cables, the customer may still be able to access the Internet via the wireless link. However, this solution relies on the customer to purchase the needed redundancy. Indeed, the Pew Research Center found that the number of homes in the United States with broadband Internet access has slightly decreased in recent years as more adults are using only their smartphones to access the Internet (Horrigan and Duggan, 2015).

Broadband ISPs can provide more stability to their customers by complementing their own existing cable links with wireless links. The backup wireless solution must be as reliable and at least as high capacity as the wired connection, otherwise it too may be ineffective if the primary connection fails.

In an emergency situation in which communication has been destroyed, an ad hoc network can be quickly created to restore cellular communication (Richards, 2015). **Cellular on Wheels (COW) and Cellular on Light Trucks (COLT)** can be transported into an area to temporarily provide cellular service. A COW consists of networking equipment on a flat-bed trailer that has to be hooked to a truck tractor. A COLT is a self-contained truck that provides cellular and possibly Wi-Fi and portable charging stations for mobile devices. COLTs are used more often in the event of a natural disaster, as their independent operation can make them easier to deploy. As one example, COWs were deployed in the aftermath of Hurricane Katrina to provide critical phone service to rescue and recovery workers when the area's cellular networks were otherwise disabled.

FOR EXAMPLE

In October 2012, Hurricane Sandy devastated New York City, killing more than 100 people, crippling public transportation, cutting power to over 8 million homes, damaging infrastructure, and destroying entire communities. However, during that time AT&T, one of the country's leading network carriers, suffered no network problems (Bell, 2012). AT&T accomplished this impressive feat by sending COLTs and COWs to New York City, Long Island, and various locations in New Jersey. The trailers contained the exact same equipment as an AT&T central office, including their own power supply, and thus could be parked in a parking lot to become the central office. These mobile cellular towers were set up to provide cellular network access to Sandy victims.

2.6 IoT and Emergency Management

The **IoT** is a massive network of often battery-powered devices, estimated to reach 30 billion by 2020 (ABIResearch, 2013). These devices may connect to each other through the Internet, but more frequently they talk directly to each other through Bluetooth, ZigBee, or other wireless standards. Beyond this networking-oriented definition, IoT can be seen as a technology that enables decentralized systems of cooperating cyber–physical **Smart Objects** (SOs) which are physical objects, augmented with sensing/actuating, processing, storing, and networking capabilities. SOs may cooperate with other SOs and exchange information with human users and other computing devices.

The integration of SOs, people, physical environments, and computing devices is often called a **Cyber–Physical System (CPS)**. These include systems such as Smart Cities, Smart Grids, Smart Factories, Smart Buildings, Smart Homes, and Smart Cars. The terms CPS and IoT are often used interchangeably. However, IoT is more generally used to refer to the technology employed to provide connectivity to devices. IoT technology enables the development of a CPS, such as a Smart Car, that is, a car that could receive real-time traffic alerts and respond to them possibly without user intervention.

FOR EXAMPLE

In May 2016, Juniper Research named Singapore the "Global Smart City—2016." The Singapore Smart City is empowered by an immense collection of sensors and cameras that are deployed across the city to monitor everything including the cleanliness of public spaces, crowd density, and the movements of registered vehicles. Sensor data is being fed into a system known as Virtual Singapore that is being built by the government's National Research Foundation with assistance from private–sector companies, universities, and other governmental departments. In addition to receiving sensor data, the system maintains a map that includes the exact dimensions of buildings, placement of windows, and the types of construction materials used.

At this point, applications for the data are being envisioned and developed including applications that:

- reroute buses based on where riders are gathering
- collect information about the bumpiness of bus rides from riders' cell phones to determine where road repairs need to be done
- detect smoking in prohibited areas
- automatically charge tolls based upon the movement of the registered vehicle
- provide parking information through an online map
- monitor the movements of elderly people in their homes to detect a potential emergency
- inform volunteers that can perform CPR of someone who has suffered from a cardiac arrest who is within 400 m of their location

To enable the development of applications, the Singapore government has created an initiative called "Smart Nation." This initiative seeks to engender a people-centric approach to creating applications by rallying citizens, industries, research institutions, and the government to participate in their creation. The government facilitates the development by sharing the extensive real-time public domain data collected via the vast network of sensors and cameras.

More precisely, IoT is the combination of billions of IP-enabled devices, RFID tags, WSNs, mobile apps, and cloud computing. **Cloud computing** refers to the practice of using servers that can be accessed via the Internet to store, process, and access data. A server is a computer that provides computing resources or data to other computers. If those two computers communicate via the Internet, then it is employing cloud computing and the server is located in what is called the cloud. For example, wireless sensor data can be sent to the cloud for storage and processing. Emergency personnel can then have access to the processed data via a mobile app.

WSNs are of particular importance to the field of emergency management since sensors can be used to detect environmental parameters that may indicate an emergency situation (Benkhelifa et al., 2014). For example, changes in atmosphere and temperature can be used to detect a forest or building fire. The presence of a toxic gas may indicate an explosion. Vibrations may indicate an earthquake. In addition, during rescue and recovery, the number of Bluetooth devices in the area can be used to estimate the number of victims. If a company uses an RFID system or NFC for tracking entrance into a building, that data can be used to determine the number of people in a building in the event of a disaster.

One of the key tasks of emergency management is tagging/tracking and RFID systems can support this important task. An urgent problem at the emergency scene is the overwhelming number of victims that must be monitored, tracked, and managed by first responders and volunteers. In addition, the equipment deployed at the emergency scene, as well as other resources to support victims, needs to be managed and distributed appropriately. The process of managing humans and other objects during emergencies is composed of the following tasks (Ahmed, 2015):

- Marking or tagging of humans and objects
- Using tags to track humans/objects
- Using tags for object management before, during, and after emergencies.

In particular, RFID systems can be used to identify an object within a group of similar objects and to provide real-time information about that object's position.

FOR EXAMPLE

Hurricane Katrina exposed a number of problems dealing with the evacuation of citizens. In 2005, when Katrina loomed in the Gulf, most New Orleanians did leave town, but more than 100 000 residents were left behind. Many of those that stayed lacked a car and money for transportation or had no one outside of the city that they could turn to for shelter. In addition, some residents, not having Internet access, relied on television for information about the storm. Television stations were slower at informing viewers how bad the storm would be. Still others were disabled or suffering from a chronic disease, which made evacuation more difficult. The city failed to inform its most vulnerable residents about the seriousness of the impending storm and they failed to facilitate their evacuation.

Many of the evacuees of Hurricane Katrina were moved to Texas. Unfortunately, Hurricane Rita hit some of the areas to which Hurricane Katrina victims were evacuated, causing those victims to be evacuated again. It became very difficult for emergency personnel to keep track of who was being evacuated and where they were being evacuated. Many of the victims of the storm were separated from their families including a large number of parents separated from their children. Special needs people were particularly vulnerable. It sometimes took weeks for families to find their loved ones.

After experiencing the evacuation mishaps of hurricanes Katrina and Rita, Texas Governor Rick Perry spearheaded a program that uses RFID, GPS, and bar code technology to automate the evacuation process of elderly, sick, disabled, or able-bodied individuals or families who have no access to transportation during an emergency. Evacuees meet at embarkation centers, which are located in towns and cities. At these centers, adults and children are issued wristbands and pets receive special tags affixed to their collars. Each wristband and tag contains a bar code and/or an RFID. The IDs issued to the pets and children are associated in a back-end database with those of their guardians. Assets, such as medical equipment, are also tagged. Bar code scanners or RFID readers are used to read the wristbands of evacuees boarding buses at the various embarkation centers. GPS receivers inside of buses are used to track the location of the bus and the evacuees inside of them. When evacuees leave the bus, a bar code scanner or RFID reader is used to read tags of evacuees and the database is updated to indicate who disembarked at that site.

WSNs, **Unmanned Aerial Vehicles (UAVs)**, and **Unmanned Ground Vehicles (UGVs)** can be used for disaster preparedness, damage assessment, and disaster response and recovery (Erdelj and Natalizio, 2016). WSNs and UAVs can be used for structural and environmental monitoring to provide information to forecast an impending disaster. For example, sensors can be used to detect slope movement that can predict a landslide (Frigerio et al., 2014). However, to enable disaster preparedness often a WSN is deployed to an inhospitable location that can cause a