We are IntechOpen, the world's leading publisher of Open Access books Built by scientists, for scientists

6,900
Open access books available

186,000
International authors and editors

200M
Downloads

Our authors are among the

154
Countries delivered to

TOP 1%
most cited scientists

12.2%
Contributors from top 500 universities

WEB OF SCIENCE™

Selection of our books indexed in the Book Citation Index in Web of Science™ Core Collection (BKCI)

Interested in publishing with us?
Contact book.department@intechopen.com

Numbers displayed above are based on latest data collected.
For more information visit www.intechopen.com

3

Cyber Security Concerns for Emergency Management

Jessie J. Walker
University of Arkansas at Pine Bluff/Computer Science Unit
USA

1. Introduction

Cyber security has become a matter of national, economic, and societal importance. Present-day attacks on the nation's computer systems do not simply damage an isolated machine or disrupt a single enterprise system. Instead, modern attacks target infrastructure that is integral to the economy, national defense, and daily life. Computer networks have joined food, water, transportation, and energy as critical resources for the functioning of the national economy. When one of these key cyberinfrastructure systems is attacked, the same consequences exist for a natural disaster or terrorist attack. National or local resources must be deployed. Decisions are made to determine where to deploy resources. The question is who makes these decisions? The data required to make and monitor the decisions, and the location of available knowledge to drive them may sometimes be unknown, unavailable, or both.

Indeed, computer networks are the "central nervous system" of our national infrastructure. We are faced with the difficult task of securing our critical cyberinfrastructure from foreign and domestic attacks. In addition, the backbone of emergency management (EM) is a robust cyberinfrastructure. These systems enable emergency management agencies to implement comprehensive approaches to natural disasters, terrorist attacks, and law enforcement issues. There is a general lack of understanding about how to describe and assess the complex and dynamic nature of emergency management tasks in relation to cyber security concerns. Another issue is knowledge integration and how it helps managers improve emergency management task performance. Ever since the first computer virus traversed the Internet, it has been apparent that attacks can spread rapidly. Just as society has benefited from the nearly infinite connections of devices and people through the US cyberinfrastructure, so have malicious parties with the intent of taking advantage of this connectivity to launch destructive attacks.

Surprisingly, very few studies have attempted to tap into the vast knowledge-base of cyber security and emergency management to discover new and relevant theoretical models addressing the two areas. There is also a lack of theories and tools that organizations can use to improve EM success that relate to handling cyber security through effectively managing task complexity and knowledge integration.

This chapter will explore how cyber security concerns related to the uncertainty of emergency management tasks can be addressed for secure EM. In addition, we examine

how cyber situational awareness can exploit the mediating role of knowledge sharing and integration to enhance EM tasks.

2. Emergency management community of practice

Friedman and Wyman (2006) theorized that technology has leveled or "flattened" the global playing field that once existed. This flattening has happened as a result of what they call the "triple convergence" of platform, process and people. When an innovative platform takes hold, processes that use the platform must change. This is especially true in contemporary EM communities. If the right people are available, trained, adept and able to adopt technology and process paradigms, they become the third prong of the triple convergence. EM has witnessed this transformation.

In 2007 in both process and technology utilization, Dr. Wayne Blanchard of the Federal Emergency Management Agency (FEMA)'s Emergency Management Higher Education Project (FMHEP) developed the EM community's strongest set of guiding principles for EM, all of which relied on cyberinfrastructure resources (Abbott, Hetzel, & American Bar Association. Section of State and Local Government Law., 2010; Lansford, 2010; LearningExpress (Organization), 2010). These principles are the governing rules that direct EM activities within each EM tasks directly. They include:

1. Develop comprehensive plans which require all emergency managers to take into account all possible hazards, EM tasks, stakeholders, and anticipate all possible impacts to relevant communities;
2. Develop progressive plans that anticipate future emergencies, disasters and develop preventive, preparatory measures to build disaster-proof and elastic communities that are capable of withstanding any type of disaster or emergency;
3. Develop risk-driven models for emergencies and disasters using well accepted EM principles to assign priorities, personnel, and resources;
4. Develop integrated plans to ensure true uniformity among all segments of the EM community, outside organizations and civilian populations;
5. Develop collaborative plans which create true communities of practices;
6. Develop coordination plans which synchronize the activities among community members;
7. Develop and implement flexible plans that can change with the demands of the environment;
8. Develop a professional community, which integrates technology and science in all segments of EM including communal values, and ethics systems.

All of these activities have created within EM a community of practice. Wenger, McDermott, and Snyder (Wenger, McDermott, & Snyder, 2002) define communities of practice as "groups of people who share a concern, a set of problems, or a passion about a topic, and who deepen their knowledge and expertise in this area by interacting on an ongoing basis." According to these authors, communities of practice operate as "social learning systems" where practitioners connect to solve problems, share ideas, set standards, build tools, and develop relationships with peers and stakeholders. Because they are inherently boundary-crossing entities, communities of practice are a particularly appropriate structural model for cross-agency and cross-sector collaborations within EM. The community of practice in EM is

now expanding somewhat to incorporate cyber security awareness at all levels (Elmagarmid, Samuel, & Ouzzani, 2008).

Although, the EM community has had difficulty, in defining cyber security awareness in terms of EM governing tasks, this challenge is derived from the peculiar aspects of the field of cyber security. The universe of cyber security is an artificially constructed abstraction that is only weakly tied to physical systems. Therefore, there are few a priori constraints on either the attackers or the defenders. Also, one of the most significant challenges in defining cyber security within the context of EM, is the fact that most of the threats associated with cyber security are dynamic in that the nature and agenda of adversaries is continually changing. In addition, the type of attacks encountered evolves over time, partly in response to defensive actions. Cyber security awareness within EM requires understanding of technology concepts, but also shares aspects of many other disciplines such as epidemiology, economics, and social science. All of these analogies are helpful in providing EM cyber security awareness direction for those within the community (Forrest, Hofmeyr, & Somayaji, 1997; Jennex, 2008).

A recent example of an organization attempting to integrate in cyber security awareness into their EM structure is the California Emergency Management Agency (Cal EMA), which has developed a statewide approach which implements cyber security awareness at all levels of the state's EM plans. The new approach places cyber security activities and concerns alongside other disasters that could possibly impact the state's citizens and infrastructure. The plans include efforts to consolidate its cyberinfrastructure resources to secure data for more than 150 agencies. Although, these efforts are not the result forward-thinking EM personnel, but rather the result of the state experiencing thousands of security breaches in 2010, which were documented by the state's technology staff. As a result of these activities the state, began to see the importance of cyber security in the context of its EM needs (Collins, 2011).

2.1 Technology-driven emergency management

EM can be defined as a unique set of tasks in which, individuals, organizations, governments and nations attempt to bring order to chaos. Emergencies by their very definition are chaotic events brought on by unforeseen and unpredictable circumstances (Bhavanishankar, Subramaniam, Kumar, & Dugar, 2009; Chen, Sharman, Rao, & Upadhyaya, 2008; Mendon, Jefferson, & Harrald, 2007). These events share a unique set of characteristics, which can be identified by the set of associated tasks and the knowledge, which defines the tasks. Davenport and Prusak (Davenport & Pruask, 1998) define knowledge as an evolving set of data that is a mixture of framed experience, values, contextual information and insights defined by experiences for evaluating and incorporating new experiences and data. Knowledge management is at the core of effective EM. The key to knowledge management within EM is, who possesses the knowledge, where is it located and how to find it. Therefore, a significant portion of EM is how to integrate knowledge management and task behavior. According Murphy and Jennex (Murphy & Jennex, 2006) knowledge management within EM is a practice of selectively applying knowledge from past experiences of decision makers to the current and future activities with the purpose of improving individual or organizational effectiveness in terms of the required EM tasks. Knowledge management and dissemination for modern EM tasks are linked directly and

indirectly by cyberinfrastructure structures which, consists of computer systems, data and information management, advanced instruments, visualization environments, and cyberspace all linked together by software and complex networks (Elmagarmid et al., 2008; Feng & Lee, 2010; Hong & Lindu, 2009). As a result, cyberinfrastructure enables storage and transfer of massive amounts of knowledge to enable planning, resource allocation, personnel deployment, and coordination of emergency situations (Becerra-Fernandez et al., 2008).

Although, most EM focused organizations possess a significant cyber security situational awareness deficit and how it impacts their reliance on cyberinfrastructure resources. These organization's failures in this arena is evident by recent national and international events. For example, the most recent failure of such systems which hampered effective EM included the attack on 9/11 in which law enforcement/rescue agencies were unable to communicate; Hurricane Katrina in which information coordination was limited or nonexistent; and the recent earthquake in Haiti in which the entire country went totally silent, which made EM almost impossible (Asimakopoulou & Bessis, 2010; Chandler & BCP Media., 2005; Hart, Rudman, Flynn, & Council on Foreign Relations. Independent Task Force on Homeland Security Imperatives., 2002).

Recent events on the international stage demonstrate a similar lack of cyber security situational awareness with respect to cyberinfrastructure resources. In January 2009, the Ministry of Defense in the United Kingdom reported that for two-weeks it did not have access to computers systems within the Royal Navy because of a malware attack which had left the system inaccessible to its personnel. During the same period in the United Kingdom, several hospitals suffered a similar attack, and a month later in February, London hospitals lost all network connectivity due to malware infections that occurred at the end of 2008. At the same time in the U.S., the municipal court system in Houston, TX was infected in a similar manner resulting in a suspension of court proceedings and forcing local police officers to suspend arresting individuals for minor offenses (Saurabh Amin, Litrico, Sastry, & Bayen, 2010; Bayer, Kirda, & Kruegel, 2010; Maughan, 2010; Neumann, 2010).

These examples clearly present evidence that cyber security is now critical to the survival of modern society (Hansen & Nissenbaum, 2009). Clearly, cyberinfrastructure is the infrastructure on which modern homeland security activities depend but security attributes of such resources is often vague or un-measurable. For example, small changes at the bit level in data communication systems can have significant and profound implications that are often poorly understood by the general public, communities that depend on such resources. Cyber security approaches have seen very limited success and have become an arms race with adversaries around the globe. Although, not all communities have been participants in this arms race, but have rather sat on the sideline, and played the role of a victim to evolution. EM as a discipline lacks the fundamental concepts, principles or tools to reliably predict or even measure cyber-security as task components of its activities. It is currently difficult to determine the qualitative impact of evolving cyber security concerns (i.e. more secure now or less secure?) much less quantify the improvement on some specific scale within the domain of EM.

The question for EM organizations is how will they handle cyber security situational awareness within the context of the cyberinfrastructure resources they depend on and how will they develop cyber security abstraction models that exploit the knowledge and

experience of sophisticated members of their community as well as provide a framework for discussion of cyber security issues.

2.2 Deterrence and emergency management

Deterrence has proven to be a reliable strategy for ensuring peace with nations, and has been the backbone of international relations since the Cold War of 1946 to 1991 made it an essential element of peace. Deterrence at its core can be defined as preventing an adversary from taking any threatening offensive actions by inducting a set of predefined counter attacks that will convince them they have nothing to gain by the proposed set of actions. However, as the world has changed so have the numerous threats, and the deterrence policies of the past that only countered physical courses of action are no longer as vital to national security as they once were. This is especially true within the sphere of EM, no existing EM plan with in the US contains any type of deterrence policies (Moteff, 2004; Watts, 2003).

As the US continue to infuse society/EM with the world of cyberspace it is essential that we evolve our methods of deterrence and formulate credible threat models that will govern the activities within this new domain. As stated above the US's critical cyberinfrastructure which is the linchpin of EM activities within the US is attacked daily not only from foreign threats but domestic terrorism. The main reason that we find ourselves so vulnerable to such breaches of trust is because we have yet to clearly voice the viable repercussions for those that so choose to impede upon our EM activities beyond standard law enforcement. This highlights a major lack of communication on a local, international scale, and it is upon this lack of consensus that organizations find themselves able to freely commit cyber attacks that can greatly impact EM issues (Harknett, Callaghan, & Kauffman, 2010).

The problem of attribution has plagued cyber security law enforcement ever since the Internet became an accessible form of communication. It prevents victims of cybercrimes from justly placing blame where it should, and thus strips states of the mere ability to even make credible threats of retribution. In essence, when one fights a cyber security attack they are fighting a ghost, and this realization has the power to discredit any proposed counter attacks before they can even be formulated. Knowing this, we've found that when we talk about deterring cyber-attacks in the modern age it is pivotal that we put more emphasis on the aspects of resilience and denial than that of retaliation.

Retaliation can only effectively deter one target group of hackers, and even then its effectiveness is measured based upon the amount of communication and cooperation we receive from international entities. Better security protocols on the other hand can prove their capabilities as soon as they are put into place, and can even abolish the need for threats of retaliation if they are truly impenetrable.

3. Cyber aware emergency management

According to Grant et al (Grant, Venter, & Eloff, 2007), an intrusion within the context of a computer or network system is an act of wrongfully entering, or seizing or taking control of the property of another for malicious purposes. No computer system within our modern society is an island, as a result of an interconnected cyberinfrastructure world where most systems exist in a vast evolving infrastructure of computer network systems. These systems

have brought too much of the world vast amounts of information, access to communities once remote and resources that were the stuff of science fiction. These systems have also become an integral part of our modern civilization just as oil was the defining force of the nineteenth century, computer networks have become the defining force for national defense in the twenty-first century. But just as the shipping lanes brought the plague on the back of rats to thirteenth century Europe, these new cyber resources have brought new threats to the shores of the world.

As EM has evolved over the last decade so has the notion of knowledge within the context of cyber security awareness, according to Becerra-Fernandez et al (Becerra-Fernandez, Xia, Gudi, & Rocha, 2007) knowledge at the core of EM can be divided into three specific knowledge types:

Context-Specific Knowledge:

Context-specific knowledge, which is defined as a type of knowledge that is temporal in nature centered around a particular set of circumstances.

Technology-Specific Knowledge:

Technology-specific knowledge is centered on a particular technical toolset, which is comprised of rules used to solve a particular problem.

Context/Technology-Specific Knowledge:

Context/technology-specific knowledge, which is a hybrid knowledge that combines a rich set of contextual knowledge while at the same time possessing a significant technical specificity.

This hybrid knowledge represents a tangent point between EM knowledge, tasks, and cyber security situational awareness. Cyber situational awareness is an emerging aspect of cyber security, in which organizations are aware of all cyber assets they are connected to or depend on (Ke, Ming-Tian, & Wen-Yong, 2009; Kellerman, 2010). Emergency management cyber situational awareness requires individuals, organizations to understand how the resources, events, information, individuals actions impact EM tasks both in the near term and future.

Since all EM tasks fall within the following categories: mitigation, preparedness, response and recovery (Dudenhoeffer et al., 2007), each is impacted by cyber situational awareness as listed in figure 1.

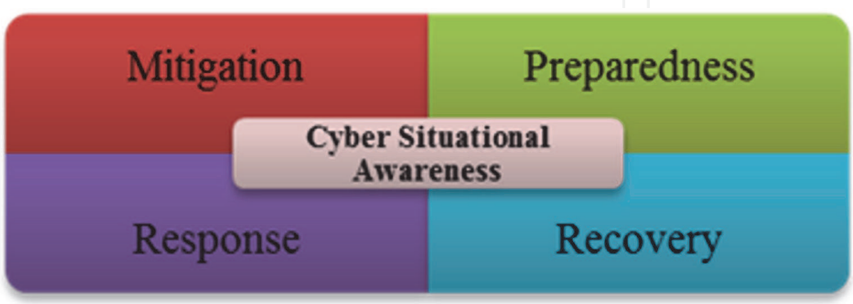


Fig. 1. Cyber Situational Awareness for Emergency Management.

For example, most modern EM tasks needs are met using cyberinfrastructure resources known as Emergency Management Information Systems (EMIS), which support all required tasks of EM. These systems are designed to support interoperability between all required tasks for EM at all segments of the EM community including governmental organizations and civilian populations (Desourdis, 2009; Hong & Lindu, 2009; Moore, 2010). EMIS supports mitigation activities by providing EM personnel the ability to predict, model, and categorize risks using software tools such as geographical information systems (GIS). EMIS allows EM personnel the ability to develop preparedness plans for many types of emergencies modeled on different types of EM scenarios using computer-generated analysis. EMIS provides EM the vast knowledge available in cyberinfrastructure; these services include resource tracking, personnel management, developing and implementing response contingency plans. One of the most significant, support services provided by EMIS to the EM community is the quantification of the true cost of emergencies. Another service includes the development of a uniform community in which remote sensors are connected to provide valuable information to EM personnel to implement future EM mitigation activities (Cohen, 2009). Mitigation tasks are unique within EM, since they are designed to reduce or eliminate risk. Mitigation tasks are either structural or non-structural. Structural tasks typically use technological components in their implementation such as remote wireless sensors or monitoring stations. Non-structural tasks normally include planning techniques such as governmental legislation for land management and development. Mitigation tasks can have the greatest impact on EM since they are designed to prevent emergencies and disasters, according to Rocha et al (Rocha, Becerra-Fernandez, Xia, & Gudi, 2009).

These tasks in an uncertain emergency environment allow planners to close the knowledge gap between specialists in the field and the general population. For example, these tasks and resources are rarely considered when examining cyber security concerns for systems, which are integral to early warning disaster systems and civilian population planning within emergency events such as supervisory control and data acquisition (SCADA) systems (Samia Amin & Goldstein, 2008). Individuals and governmental organizations to ensure resources, personnel, undertake preparedness tasks in the context of EM and infrastructure is ready for any type of emergency that may occur within their boundaries. One of the most important components of preparedness is the development of a communication plan that can be implemented within natural disasters or emergencies. The most recent example of such a failure of preparedness that relates to cyberinfrastructure systems was Hurricane Rita in 2005, one of the most intensive Atlantic hurricanes ever recorded resulting in over 11.3 billion in damage (Davis, Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction (U.S.), United States. Dept. of Defense. Office of the Secretary of Defense., & National Defense Research Institute (U.S.), 2006; Morris, 2009).

The hurricane deaths were the most severe in open unprotected locations such as roadways, because of poorly executed evacuation plans within the affected regions. Many people were trapped on roadways and interstates because of the lack of communication services (i.e., a failure of computer and data networks), inability of EM personnel to communicate important evacuation instructions on roadways and through standard communication channels. Many EM organizations have only recently started to develop preparedness plans that include cyberinfrastructure services as a component of their overall structure (*Disaster*

planning and relief. Part 2, 2010; United States. Federal Emergency Management Agency., United States. Federal Emergency Management Agency. Community Preparedness Division., & Citizen Corps (USA Freedom Corps), 2009). Response is the linchpin of EM. It ensures that the necessary personnel and resources are mobilized when emergencies do occur. These responders include firefighters, police officers, ambulance crews, and in some situations, the National Guard.

These services personnel rely on communication tools, data networks, and computer systems to ensure the correct resources are deployed to the correct location in a timely manner. They also ensure maximum impact is achieved quickly and effectively. As a result of the increased awareness of terrorist-borne threats, such services are becoming increasingly important. An ideal terrorist attack model on a major metropolitan area would be for a terrorist group to deploy a cyber attack against key cyberinfrastructure systems (i.e. communication, and data networks), and then implement a terrorist attack against that community.

The EM community within that metropolitan area would most likely be incapable of offering an effective/coordinated response because of the crippled communication services. Since communication technology is used to coordinate personnel, resources, and analysis of situation awareness within the emergency theater (Freudenburg, 2009; Shaw, Sharma, & Takeuchi, 2009).

Post-EM brings the difficult task of restoring the affected area to its previous state through resource and personnel deployment. These tasks focus on rebuilding. The key questions the affected area, EM community must confront is who makes the decisions, how to make them, and how to restore indispensable infrastructure such as power, water, transportation, data, and communication services. Many in the EM community call this time "the window of opportunity", to build better and mitigate future risk associated with disasters or emergencies. These steps are normally the mitigative measures that would be unpopular with citizens such as better building codes, reformatting of existing infrastructure systems such as power grids and transportation systems. This is also the time to deploy important cyber security aware infrastructure systems within cyberinfrastructure systems such as intrusion detection monitors, stronger network security systems and cyber awareness campaigns to the local population (Hong & Lindu, 2009; Howitt, Leonard, & Giles, 2009; Miller, 2009).

4. Emergency management and education (cyber security)

The revolution in EM has occurred, although, most of the EM information-gatekeepers within the classroom have not yet changed their curriculum to reflect this reality. The challenge is not simply a curriculum problem, albeit it is a large and significant issue. Serious modern EM interdisciplinary issues abound, are in fact some of industries, and the US most important challenges (Plant, Arminio, & Thompson, 2011).

Many EM agencies and industries are looking for capable graduates within cyber security and EM experience, find they lack the capability to address the complex and challenging nature of interdisciplinary work, which expands beyond their traditional training in EM (Clement, 2011; Radvanovsky & McDougall, 2010). The scale and variety of the

collaborative, cross-discipline interplay are not represented in traditional EM curricula (Haller, Merrell, Butkovic, & Willke, 2011).

Educational research provides strong evidence that active and collaborative learning environments provides students a much deeper and more integrated understanding of concepts as well as overall retention in courses. Successful sharing of course content, resources enable students in such courses to experience dissimilar teaching styles, which supplements diverse cognitive learning styles such as visual, auditory and kinesthetic (Caldwell, 2011).

For example, most EM programs around the country lack any virtualization tools for cyber security situational awareness. Cyber security is a notoriously challenging subject for students to comprehend. But by making extensive use of tangible artifacts such as cyber security virtualization tools to enhance the learning experience of students and teaching effectiveness of instructors, cyber security concepts could be made accessible to a more diverse student population (Bullen, Abraham, Gallagher, Simon, & Zwieg, 2009).

Furthermore, attacks on critical infrastructure can have devastating consequences these infrastructures are considered to be high-value targets for cyber terrorists. Truly modeling, and effectively demonstrating this within the context of a standard course on cyber or network security or EM training can be problematic, although, with the use of tangible tools such as simulation software, students could more easily understand the complexities of such problems. Students could interact with virtual representations of cities, counties, and nations to demonstrate cyber security attacks, and allow them to deploy solutions in real time. Thereby, enabling the students to examine existing cyber security problems within the domain of EM, which would integrate in the theoretical and practical components. Also, given contemporary students' fondness for multimedia styles of presentation, the virtualization approach would serve as a tool to combat students understanding of the unique problems related to cyber security and EM (Caldelli, Amerini, Picchioni, De Rosa, & Uccheddu, 2009; Pan & Xu, 2010; Smith & Agarwal, 2010).

As in the case above with the intrusion attacks on key critical infrastructure locations such as military installations in the United Kingdom, intrusion attacks are considered to be one of the most common types of cyber security threats facing the EM community (Jamieson, Land, Smith, Stephens, & Winchester, 2009).

5. Emergency management and intrusions

Most practitioners within the EM community wouldn't know what an intrusion is or how to handle such an incident. A recent survey of Intrusion Detection Systems (IDS) indicates that most practitioners are still examining the central question of how to best implement reactive IDS. (Allen, 2000; Arvidson & Carlbark, 2003; Escamilla, 1998; Koziol & Safari Tech Books Online., 2003; Rehman & Safari Tech Books Online., 2003; Valdes & Zamboni, 2006). In a modern cyberinfrastructure world, nodes (e.g. networked computer systems or devices) within a system maybe connected to thousands or millions of other nodes resulting in millions of possible candidates for intrusion attacks from a single or a multistage attack (Liu, Zang, & Yu, 2005). Modern reactive IDS responses to intruders include log-off an offender or modify firewall setting to block network traffic from a malicious source. Although, these approaches do not work with multistage intrusion attacks, in which an intruder will

perform multiple attacks at different points. Most modern reactive IDS are based on the Denning (Denning, 1987) model in which a system monitors a system's log or audit records.

As a result, by the time that an intruder appears in a log or audit record, the event has already taken place, and for this reason, intruders particularly those committing multistage attacks take extraordinary measures to ensure their actions go unrecorded. Snort is the most commonly used IDS used within cyberinfrastructure environments (Chakrabarti, Chakraborty, & Mukhopadhyay, 2010), it can generate thousands of alerts per hour. These include sensor events, which are compared against signatures of common similar attacks, or it may build a database of temporal behavioral patterns. These approaches suffer from a high false-alert rate, which increases the overall workload of most system administrators, which has led to many administrators being weary of using reactive approaches for automatic response. The question for many administrators is when to sound the alarm to law enforcement communities, which may need to be aware of larger attacks such as cyber terrorists (Jones & Michael, 2010; Warren, 2008).

While network-based IDS cover multiple nodes with sensors. These sensors capture, and analyze the content of packets that flow through the network, although, most contemporary IDS are unable to examine encrypted packets or handle large volumes of traffic as in the case of cyberinfrastructure-oriented environments. Moreover, network-based IDSs tend to be poorly placed to detect malicious intruders who act from the inside (Ayd\ et al., 2009).

In contrast host-based IDS are not encumbered by encrypted packets since they monitor all host activities by analyzing each individual application's system calls, logs, and file modifications, while constantly monitoring the host's state. Though one significant fault in most host-based IDS engines design is their reliance on the underlying network to pass them generated events, which can become the target of the intruder, as well as degrading the overall performance of the system on which they reside. The ideal IDS would incorporate automatic protection services, which would be defined by the administrator based on intrusion types and potential impact to the system. This research will focus its efforts on using a host-based IDS Snort.

Most IDS including Snort only examine a subset of all intrusion data including connections, namely those that violate the security policy or triggered an alarm. Which, result in a very limited amount of knowledge contained within the standard log file, such as which machines are present within the network, how were they impacted by the attack. To truly understand intrusion concerns and their impact on critical infrastructure locations, the EM community would need a schema that quantifies attacks and provides a domain independent framework which makes it ideal for quantifying security threats from a universe of known security threats (Umberger & Gheorghe, 2011).

5.1 Emergency Management and Intrusion Detection

A simple approach EM practitioners could deploy, and has a proven track record is the Boyd's observe-orient decide act (OODA) model (Boyd, 1996). In 1995, a retired Air Force colonel, John Boyd an expert on military strategy, studied dogfights from the Korean, Vietnam wars respectively, and develop a strategy for advanced decision making in situations between numerous adversaries. Boyd's observe-orient decide act (OODA) model was never published in a formal sense in a book or paper, but was presented to influential

politicians, civil servants and military officers, the model is currently implemented in numerous organizations, such as NATO for the monitoring and control of military operations. The model has also, been leveraged in a number of commercial companies. The model offers significant potential within the sphere of intrusion detection/EM, despite the fact it was never published in a formal scientific sense, although it has received significant extensive scientific examination through peer review analysis (Grant et al., 2007). Boyd's model was a cyclic process model of four processes interacting with the surrounding environment.

This model was based on a concept known as *tempo* i.e. that is the decision cycle time, which Boyd believed was the rhythm of the response to events. The rhythm referred to tempo of decision making, according to Boyd "in order to win, we should operate at a faster tempo or rhythm than our adversaries or, better yet, get inside the adversary's Observation-Orientation-Decision-Action loop". However, the OODA model itself does not express his concept of tempo. The four processes of the model are observe, orient, decide, and act.

Observe:

The observe is the process of acquiring information about the environment by interacting with it, sensing it, or receiving messages about it. Observation also receives internal guidance and control from the orient process, as well as feedback from the decide and act processes.

Orient:

The process of orient is the process of representing the world, based on interactive process of implicit cross-referencing, correlations interactions with unfolding circumstances. The orient process forms the way the world is observe, decide, and act i.e. situation awareness.

Decide:

The decide process is the procedure of making choices among hypotheses about the current situation and possible responses to it. Decide is guided by internal feedback from orient, and provides internal feedback to observe.

Act:

The act process is testing the chosen hypothesis by interacting with the environment. Act receives internal guidance and control from the orient process, as well as feed- forward from decide. It provides internal feedback to observe.

The EM community could modify OODA as an environment to develop automatic responses to intrusions in critical infrastructure locations. Therefore, an intrusion attack could be represented as a rational reconstruction model resulting in the OODA-RR in which each node will possess two knowledge bases:

1. One for assessing the situation (Orienting)
2. The other for deciding on the response (Deciding).

The knowledge base for the intrusion response approach could be formed using quantified weights developed by situational rules, which are extracted from national assessments, and the importance of the location i.e. its critical importance to the nation or local community.

Although, some of the challenges of EM security engineering practices include globalization of asset protection, rapid response time requirements, responsiveness to changing network infrastructure environments, and heterogeneous computing platforms. These problems are not easily solved.

A good example of a governmental agency that has taken on similar problems and developed a real tangible solution is the department of defense (DOD). The frontier of cyberinfrastructure protection is of such significance that the DOD, established the U.S. Cyber Command (USCYBERCOM), in 2009, under the US Strategic Command, the USCYBERCOM, which has the unique mission within the DOD of planning, coordinating, synchronizing, activities to direct the operations and defense of DOD cyberinfrastructure resources. As the DOD implements comprehensive cyberinfrastructure protection program, the overarching issue of detecting, protecting against unauthorized access to systems still remains the unresolved issue within all facets of DOD cyberinfrastructure resources (i.e. computer network defense (CND)) (Di Pietro, Mancini, & SpringerLink (Online service), 2008; Krutz & Vines, 2008; Mancini, Pietro, & SpringerLink (Online service), 2008; Volonino, Anzaldua, & Godwin, 2007; Zamboni, Kruegel, & SpringerLink (Online service), 2006)

6. Conclusion

In this book chapter, we discussed several cyber security concerns for the EM community. Each set of EM concern has its own unique implementation concern and characteristics. Many of the EM cyber security concerns listed in this book chapter will demonstrate a clear pattern of duplication of cyber security concerns for the entire EM community. Most EM researchers agree that there is no real killer solution to integrate in cyber situational awareness for the EM community but instead there is a real need for standards to be integrated into the EM paradigm as it currently stands. This will be evident from the cyber security concerns described in this chapter. Hence this lack of coherent knowledge offers many opportunities for further research into how to guide EM community to a framework that integrates in cyber situational awareness and develops an appreciation for cyber security concerns for each particular task within the domain of EM. Therefore, many solutions must be brought to bear on the problem.

6.1 Education

In the United States, critical infrastructure is particularly difficult to secure with standard security approaches because it is massive, distributed, and interdependent and often needs to be accessible to diverse populations. Further complicating cyber security issues in the United States, is the multiple public and private entities now collaborating to build, run and maintain this critical infrastructure. Because of these numerous threats the UShas become aware of the urgent need to educate a computing/communication security, EM capable workforce quickly, and effectively to confront these growing threats. The current cyber security/EM workforce does not reflect the unique diversity of the US, many segments of the population have been left on the sideline in this new cyber war.

The EM community of practice, which currently exists, must embrace the changing role of cyber security as a key component or task within their community. Many new cyber security and EM programs do not practice curriculum reuse or curriculum sharing. A much

deeper examination of the issue demonstrates little evidence that curricular innovations are ever adopted rapidly or widely outside of their home institution or local discipline on any consistent basis. The researchers Verscoustre and McLean (Vercoustre & McLean, 2005) offers some key potential obstacles in implementing reuse, including locating the material, discovering what material is included, understanding the instructional structure and content needed to support or supplement the material and the arduous process of incorporating the content into one's course and the program curriculum. This approach must change within the homeland security disciplines.

6.2 Communal tools

Homeland security today depends as never before upon ease of access to data, associated sophisticated tools and applications, to enable asset protect, training, law enforcement.. Homeland security officers, emergency managers, police, fire departments, national security agencies who once worked in local, isolated silos now collaborate routinely and on a global scale. Specialized instruments that were spread across multiple locations can now fit into a single location connected via cyberinfrastructure resources. Set within this evolving cyberinfrastructure, networks have become the primary artery connecting homeland security individuals to each other and to the data so critical to their work. Going forward, such networks are likely to evolve to become "data mediums" where data can be positioned to serve an ever-changing tool for homeland security. The current structures of cyber security threat ensure they must be address by many facets of homeland security.

When the Internet was created, the end-to-end principle was adopted based on the assumption that the end users (mostly engineers and researchers at the time) were willing to behave cooperatively and with trust of one another. Security was not considered important to the designers. The Internet protocols and architecture were designed from the perspective of functionality. To support emerging applications, the intermediate network was a purely transparent carrier optimized for *best-effort* packet forwarding. Today, however, the Internet is operated in an untrustworthy world and any device connected to it can become a victim. As a result law enforcement individuals must have the tools to model, and predict possible threads before they happen (i.e. robust and intelligent network infrastructure). It is mandatory to detect and counteract attacks inside the core infrastructure. For example, within homeland security and EM community, it is important to make the distinction between infrastructure security and information security. Individuals steal information all of the time from agencies and industries, with types of intrusions. While when individuals target cyberinfrastructure, they are mainly targeting the availability, reliability, and stability of the network fabric.

As presented above in section 5.1, an individual could deploy a simple intrusion attack by flooding a server with data, which simply exhausts certain critical resources, such as bandwidth. The attacker does not even need to understand the fundamentals of the system. But when the attacker (s) targets large groups of systems with the goal taking down key infrastructure assets, the results can have large-scale societal implications. The EM community should adopt more nontraditional educational models to expose students within both the cyber security and EM communities to each other's disciplines. Both communities could benefit from the direct use of virtualization teaching tools such as visualization. By utilizing the proposed instructional model the traditional whiteboard classrooms could be

replaced by active communal learning environments. These environments could incorporate practical/interdisciplinary computer security theories, principles, and EM tasks, which enable students to examine existing problems in innovative and unique ways, thereby, allowing them to become active participants in the learning process. As a consequence, the students' work could become a part of the learning experience of the class, and an enriching component of teaching. As well as, allow student to consider new innovative approaches to problems.

6.3 Emergency Management and The Road Ahead

There are some cases where knowledge can only be gained through trial and error. Though this method is not very efficient, it has proven itself to be one of the most effective ways to obtain useful information. However, where there is information of a sensitive nature involved, the defending actor is often reluctant to welcome would-be cyber terrorists to assault their systems. The use of the trial and error method often results in failure. This is very unappealing to many within the EM community, as failure to protect one's system can have catastrophic consequences. It then becomes necessary to create a safe environment to test one's system security against a large quantity of various types of attack. With the risks accompanying failure abolished, every iteration of the attack simulation may produce beneficial data regardless of whether or not the defenses were successful in thwarting the attack.

The defender would be well equipped, and able to react to the exploits of the actors in several different ways, with the goal of slowing and eventually stopping the attack.

Resilience:

- The first line of defense will be a sturdy firewall, and a steady stream of updates and patches. This alone will hinder actors to a limited degree.
- The resilience of any system is one of the most important aspects of system security. It acts as a preventive measure against recreational actors possessing all levels of skill and quantities of resources, and non-state organizational actors may find an especially resilient system to be a devastating deterrent.
- The patches and updates will either be automatic or applied by an administrator.

Denial:

- Denial of service can be a very effective means of deterring an actor. The repeated termination of a connection may force an attack to an abrupt end. The defender will possess the means to cause such interruptions.
- Denial is the next best thing to possessing a resilient system. Actors operating with but a few terminals may find their efforts to be in vain once they have been denied on all fronts.
- An actor with multiple terminals or networks may circumvent the denial, but the denial can also be repeated.
- This methods holds to be most effective against recreational hackers, who usually only have one viable connection to the Internet, and non-state hackers, who may have more than one connection but are still hindered by limited resources.

Retaliation:

- Retaliation should only be used as a last resort, and even then, it should be used with extreme caution. Attacking the actor may stop the attack, but the dilemma of attribution makes this method highly unreliable.
- Retaliation may serve a purpose in dealing with state actors. State actors have something to protect, and may think twice about taking aggressive action if they know that they stand to lose more than they gain.
- The use of retaliation will be readily available to the defender, but the risk of misattribution will also be present in some fashion.

Speaking candidly, it is crucial that we place greater efforts into research and development while also taking the initiative to thoroughly educate the public on the issues regarding future security of the modern society as these issues relate to EM.

7. References

Abbott, E. B., Hetzel, O. J., & American Bar Association. Section of State and Local Government Law. (2010). *Homeland security and emergency management : a legal guide for state and local governments* (2nd ed.). Chicago, IL: Section of State and Local Government Law, American Bar Association.

Allen, J., Christie, A., Fithen, W., McHugh, J., Pickel, J., and Stoner, E. (2000). *State of the Practice of Intrusion Detection Technologies*. Pittsburgh: Carnegie Mellon University.

Amin, S., & Goldstein, M. P. (2008). *Data against natural disasters : establishing effective systems for relief, recovery, and reconstruction*. Washington DC: World Bank.

Amin, S., Litrico, X., Sastry, S. S., & Bayen, A. M. (2010). *Stealthy deception attacks on water SCADA systems*. Paper presented at the Proceedings of the 13th ACM international conference on Hybrid systems: computation and control.

Arvidson, M., & Carlbark, M. (2003). *Intrusion Detection Systems -- Technologies, weaknesses and trends*. Linköping University, Stockholm.

Asimakopoulou, E., & Bessis, N. (2010). *Advanced ICTs for disaster management and threat detection : collaborative and distributed frameworks*. Hershey, PA: Information Science Reference.

Ayd\, M. A., \#305, Zaim, A. H., G\, K., \#246, & Ceylan, k. (2009). A hybrid intrusion detection system design for computer network security. *Comput. Electr. Eng., 35*(3), 517-526.

Bayer, U., Kirda, E., & Kruegel, C. (2010). *Improving the efficiency of dynamic malware analysis*. Paper presented at the Proceedings of the 2010 ACM Symposium on Applied Computing.

Becerra-Fernandez, I., Madey, G., Prietula, M., Rodriguez, D., Valerdi, R., & Wright, T. (2008). *Design and Development of a Virtual Emergency Operations Center for Disaster Management Research, Training, and Discovery*. Paper presented at the Proceedings of the Proceedings of the 41st Annual Hawaii International Conference on System Sciences.

Becerra-Fernandez, I., Xia, W., Gudi, A., & Rocha, J. (2007). *Task Characteristics, Knowledge Sharing and Integration, and Emergency Management Performance: Research Agenda and*

Challenges. Paper presented at the 16th International Conference on Management of Technology.

Bhavanishankar, R., Subramaniam, C., Kumar, M., & Dugar, D. (2009). *A context aware approach to emergency management systems*. Paper presented at the Proceedings of the 2009 International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly.

Boyd, J. (1996). *The Essence of Winning and Losing*: Unpublished lecture notes.

Bullen, C. V., Abraham, T., Gallagher, K., Simon, J. C., & Zwieg, P. (2009). IT workforce trends: Implications for curriculum and hiring. *Communications of the Association for Information Systems, 24*(1), 9.

Caldelli, R., Amerini, I., Picchioni, F., De Rosa, A., & Uccheddu, F. (2009). Multimedia forensic techniques for acquisition device identification and digital image authentication. *Handbook of Research on Computational Forensics, Digital Crime and Investigation: Methods and Solutions*.

Caldwell, S. L. (2011). *Critical Infrastructure Protection: Update to National Infrastructure Protection Plan Includes Increased Emphasis on Risk Management and Resilience*: DIANE Publishing.

Chakrabarti, S., Chakraborty, M., & Mukhopadhyay, I. (2010). *Study of snort-based IDS*. Paper presented at the Proceedings of the International Conference and Workshop on Emerging Trends in Technology.

Chandler, R. C., & BCP Media. (2005). *Crisis communication planning : sustaining effective corporate communication during disasters, emergencies, and critical events*. St. Louis, Mo.?: Richard L. Arnold.

Chen, R., Sharman, R., Rao, H. R., & Upadhyaya, S. J. (2008). Coordination in emergency response management. *Commun. ACM, 51*(5), 66-73.

Clement, K. E. (2011). The Essentials of Emergency Management and Homeland Security Graduate Education Programs: Design, Development, and Future. *Journal of Homeland Security and Emergency Management, 8*(2), 12.

Cohen, N. (2009). *Emergency communications : enhancing the safety network*. Hauppauge, N.Y.: Nova Science Publishers.

Collins, H. (2011). California May Incorporate Cyber-Readiness into State Emergency Plan. *Emergency Management*

Davenport, T., & Pruask, L. (1998). *Working Knowledge: How Organizations Manage What They Know*. Boston: Harvard Business Press.

Davis, L. M., Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction (U.S.), United States. Dept. of Defense. Office of the Secretary of Defense., & National Defense Research Institute (U.S.). (2006). *Combating terrorism : how prepared are state and local response organizations?* Santa Monica, CA: RAND National Defense Research Institute.

Denning, D. E. (1987). An Intrusion -Detection Model. *IEEE Transactions on Software Engineering, 23*(12), 800 - 807

Desourdis, R. I. (2009). *Achieving interoperability in critical IT and communication systems*. Boston: Artech House.

Di Pietro, R., Mancini, L. V., & SpringerLink (Online service). (2008). Intrusion detection systemspp. xiii, 249 p.). Available from http://eresources.lib.unc.edu/external_db/external_database_auth.html?A=P%7CF=N%7CID=24%7CREL=AAL%7CURL=http://libproxy.lib.unc.edu/login?url=http://dx.doi.org/10.1007/978-0-387-77265-3

Disaster planning and relief. Part 2. (2010). New Delhi

Washington, D.C.: Library of Congress Office;

Library of Congress Photoduplication Service.

Dudenhoeffer, D. D., Permann, M. R., Woolsey, S., Timpany, R., Miller, C., McDermott, A., et al. (2007). *Interdependency modeling and emergency response*. Paper presented at the Proceedings of the 2007 summer computer simulation conference.

Elmagarmid, A. K., Samuel, A., & Ouzzani, M. (2008). Community-Cyberinfrastructure-Enabled Discovery in Science and Engineering. *Computing in Science & Engineering, 10*(5), 46-53.

Escamilla, T. (1998). *Intrusion detection : network security beyond the firewall*. New York: John Wiley.

Feng, Y.-H., & Lee, C. J. (2010, 20-23 April 2010). *Exploring Development of Service-Oriented Architecture for Next Generation Emergency Management System.* Paper presented at the Advanced Information Networking and Applications Workshops (WAINA), 2010 IEEE 24th International Conference on.

Forrest, S., Hofmeyr, S. A., & Somayaji, A. (1997). Computer immunology. *Commun. ACM, 40*(10), 88-96.

Freudenburg, W. R. (2009). *Catastrophe in the making : the engineering of Katrina and the disasters of tomorrow*. Washington, DC: Island Press/Shearwater Books.

Grant, T. J., Venter, H. S., & Eloff, J. H. P. (2007). *Simulating adversarial interactions between intruders and system administrators using OODA-RR*. Paper presented at the Proceedings of the 2007 annual research conference of the South African institute of computer scientists and information technologists on IT research in developing countries.

Haller, J., Merrell, S. A., Butkovic, M. J., & Willke, B. J. (2011). Best Practices for National Cyber Security: Building a National Computer Security Incident Management Capability, Version 2.0.

Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen School. *International Studies Quarterly, 53*(4), 1155-1175.

Harknett, R. J., Callaghan, J. P., & Kauffman, R. (2010). Leaving Deterrence Behind: War-Fighting and National Cybersecurity. *Journal of Homeland Security and Emergency Management, 7*(1), 22.

Hart, G., Rudman, W. B., Flynn, S. E., & Council on Foreign Relations. Independent Task Force on Homeland Security Imperatives. (2002). America still unprepared, America still in danger Available from http://www.cfr.org/publication.html?id=5099

Hong, T., & Lindu, Z. (2009, 19-21 May 2009). *Knowledge Management System of Intercity Emergency Decision Making*. Paper presented at the Software Engineering, 2009. WCSE '09. WRI World Congress on.

Howitt, A. M., Leonard, H. B., & Giles, D. (2009). *Managing crises : responses to large-scale emergencies*. Washington D.C.: CQ Press.

Jamieson, R., Land, L., Smith, S., Stephens, G., & Winchester, D. (2009). CRITICAL INFRASTRUCTURE INFOMATION SECURITY: IMPACTS OF IDENTITY AND RELATED CRIMES.

Jennex, M. E. (2008). Cyber War Defense: Systems Development with Integrated Security. *Cyber Warfare and Cyber Terrorism*, 241-253.

Jones, M., & Michael, K. (2010). Cyber terrorists'a real threat'.

Ke, T., Ming-Tian, Z., & Wen-Yong, W. (2009, 25-28 July 2009). *Insider cyber threat situational awareness framwork using dynamic Bayesian networks.* Paper presented at the Computer Science & Education, 2009. ICCSE '09. 4th International Conference on.

Kellerman, T. (2010). Cyber-Threat Proliferation: Today's Truly Pervasive Global Epidemic. *Security & Privacy, IEEE, 8*(3), 70-73.

Koziol, J., & Safari Tech Books Online. (2003). Intrusion detection with Snortpp. xx, 340 p.). Available from http://ezproxy.library.arizona.edu/login?url=http://proquest.safaribooksonline.com/?uiCode=uariz&xmlId=157870281X

Krutz, R. L., & Vines, R. D. (2008). *The CEH prep guide : the comprehensive guide to certified ethical hacking*. Indianapolis, IN: Wiley.

Lansford, T. (2010). *Fostering community resilience : homeland security and Hurricane Katrina*. Burlington, VT: Ashgate.

LearningExpress (Organization). (2010). *Becoming a homeland security professional*. New York: LearningExpress.

Liu, P., Zang, W., & Yu, M. (2005). Incentive-based modeling and inference of attacker intent, objectives, and strategies. *ACM Trans. Inf. Syst. Secur., 8*(1), 78-118.

Mancini, L. V., Pietro, R., & SpringerLink (Online service). (2008). Intrusion Detection Systems, Advances in Information Security, 38. Available from http://eresources.lib.unc.edu/external_db/external_database_auth.html?A=P%7CF=N%7CID=24%7CREL=AAL%7CURL=http://libproxy.lib.unc.edu/login?url=http://dx.doi.org/10.1007/978-0-387-77265-3

Maughan, D. (2010). The need for a national cybersecurity research and development agenda. *Commun. ACM, 53*(2), 29-31.

Mendon, D., Jefferson, T., & Harrald, J. (2007). Collaborative adhocracies and mix-and-match technologies in emergency management. *Commun. ACM, 50*(3), 44-49.

Miller, D. A. (2009). *Disaster response*. Detroit: Greenhaven Press.

Moore, M. (2010). *Bridging the gap : developing a tool to support local civilian and military disaster preparedness*. Santa Monica, CA: RAND.

Morris, J. (2009). *Disaster planning*. Detroit: Greenhaven Press.

Moteff, J. (2004). *Critical infrastructure and key assets: definition and identification*.

Murphy, T., & Jennex, M. (2006). Knowledge Management, Emergency Response, and Hurricane Katrina. *INTERNATIONAL JOURNAL OF INTELLIGENT CONTROL AND SYSTEMS, 11*(4), 199-208.

Neumann, P. G. (2010). Risks to the public. *SIGSOFT Softw. Eng. Notes, 35*(3), 24-32.

Pan, R., & Xu, C. (2010). *Research on Decision of Cyber Security Investment Based on Evolutionary Game Model*.

Plant, J. F., Arminio, T., & Thompson, P. (2011). A Matrix Approach to Homeland Security Professional Education. *Journal of Homeland Security and Emergency Management, 8*(2), 8.

Radvanovsky, R., & McDougall, A. (2010). *Critical infrastructure: homeland security and emergency preparedness*: CRC.

Rehman, R. U., & Safari Tech Books Online. (2003). Intrusion detection systems with Snort advanced IDS techniques using Snort, Apache, MySQL, PHP, and ACID, Bruce Perens' Open source series.pp. xii, 263 p.). Available from http://ezproxy.library.arizona.edu/login?url=http://proquest.safaribooksonline.com/?uiCode=uariz&xmlId=0131407333

Rocha, J., Becerra-Fernandez, Xia, W., & Gudi, A. P. (2009, Aug 2009). *Dealing with Task Uncertainty in Disaster Management: The Role of Knowledge Sharing for Exploration and Exploitation.* Paper presented at the Amerias Conference on Information Systems, San Francisco, California

Shaw, R., Sharma, A., & Takeuchi, Y. (2009). *Indigenous knowledge and disaster risk reduction : from practice to policy*. New York: Nova Science Publishers.

Smith, C. L., & Agarwal, R. (2010). Practicing Safe Computing: A Multimedia Empirical Examination of Home Computer User Security Behavioral Intentions. *Management Information Systems Quarterly, 34*(3), 613-643.

Umberger, H., & Gheorghe, A. (2011). Cyber Security: Threat Identification, Risk and Vulnerability Assessment. *Energy Security*, 247-269.

United States. Federal Emergency Management Agency., United States. Federal Emergency Management Agency. Community Preparedness Division., & Citizen Corps (USA Freedom Corps). (2009). *Personal preparedness in America : findings from the Citizen Corps national survey*. Washingotn, D.C.: Community Preparedness Division, FEMA.

Valdes, A., & Zamboni, D. (2006). *Recent advances in intrusion detection : 8th international symposium, RAID 2005, Seattle, WA, USA, September 7-9, 2005 : revised papers*. Berlin ; New York: Springer.

Vercoustre, A.-m., & McLean, A. (2005). Reusing Educational Material for Teaching and Learning: Current Approaches and Directions. *International Journal on E-learning (IJEL), a special issue on Technologies for Electronic Documents, 4*(1), 57-68.

Volonino, L., Anzaldua, R., & Godwin, J. (2007). *Computer forensics : principles and practices*. Upper Saddle River, N.J.: Pearson/Prentice Hall.

Warren, M. (2008). Hackers and cyber terrorists. *Encyclopedia of information ethics and security*, 304.

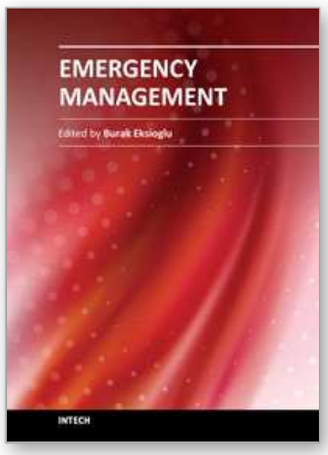
Watts, D. (2003). *Security & vulnerability in electric power systems*.

Wenger, E., McDermott, R., & Snyder, W. M. (2002). *Cultivating Communities of Practice: A Guide to Managing Knowledge*. Cambridge, MA: Harvard Business School Press.

Zamboni, D., Kruegel, C., & SpringerLink (Online service). (2006). Recent advances in intrusion detection 9th international symposium, RAID 2006, Hamburg, Germany, September 20-22, 2006 : proceedings, Lecture notes in computer science,pp. xii, 330 p.). Available from http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=4219

IntechOpen

IntechOpen



Emergency Management
Edited by Dr. Burak Eksioglu

ISBN 978-953-307-989-9
Hard cover, 90 pages
Publisher InTech
Published online 27, January, 2012
Published in print edition January, 2012

After the large-scale disasters that we have witnessed in the recent past, it has become apparent that complex and coordinated emergency management systems are required for efficient and effective relief efforts. Such management systems can only be developed by involving many scientists and practitioners from multiple fields. Thus, this book on emergency management discusses various issues, such as the impact of human behavior, development of hardware and software architectures, cyber security concerns, dynamic process of guiding evacuees and routing vehicles, supply allocation, and vehicle routing problems in preparing for, and responding to large scale emergencies. The book is designed to be useful to students, researchers and engineers in all academic areas, but particularly for those in the fields of computer science, operations research, and human factor. We also hope that this book will become a useful reference for practitioners.

How to reference
In order to correctly reference this scholarly work, feel free to copy and paste the following:

Jessie J. Walker (2012). Cyber Security Concerns for Emergency Management, Emergency Management, Dr. Burak Eksioglu (Ed.), ISBN: 978-953-307-989-9, InTech, Available from: http://www.intechopen.com/books/emergency-management/cyber-security-concerns-for-emergency-management

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821

© 2012 The Author(s). Licensee IntechOpen. This is an open access article distributed under the terms of the Creative Commons Attribution 3.0 License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

IntechOpen

IntechOpen