2009

Information Sharing: A Study of Information Attributes and their Relative Significance During Catastrophic Events

Preeti Singh
University of New York at Buffalo

Pranav Singh
State University of New York at Buffalo

Insu Park
University of Memphis

JinKyu Lee
Oklahoma State University

H.Raghav Rao
State University of New York at Buffalo

Chapter XIV
Information Sharing:
A Study of Information Attributes and their Relative Significance During Catastrophic Events

Preeti Singh
University at Buffalo, The State University of New York, USA

Pranav Singh
University at Buffalo, The State University of New York, USA

Insu Park
University at Buffalo, The State University of New York, USA

JinKyu Lee
Oklahoma State University, USA

H. Raghav Rao
University at Buffalo, The State University of New York, USA

ABSTRACT

We live in a digital era where the global community relies on Information Systems to conduct all kinds of operations, including averting or responding to unanticipated risks and disasters. This can only happen when there is a robust information exchange facilitation mechanism in place, which can help in taking quick and legitimate steps in dealing with any kind of emergent situation. Prior literature in the field of information assurance has focused on building defense mechanisms to protect assets and reduce vulnerability to foreign attacks. Nevertheless, information assurance does not simply mean building an impermeable membrane and safeguarding information, but also implies letting information be securely shared, if required, among a set of related groups or organizations that serve a common purpose. This

chapter will revolve around the central pivot of Information Sharing. Further, to study the relative significance of various information dimensions in different disaster situations, content analyses are conducted. The results hence obtained can be used to develop a prioritization framework for different disaster response activities, thus to increase the mitigation efficiency. We will also explore roles played by few existing organizations and technologies across the globe that are actively involved in Information Sharing to mitigate the impact of disasters and extreme events.

INTRODUCTION

Information assurance is the process of ensuring that the right people get the right information at the right time. This term is sometimes used interchangeably with information security but in a broader connotation, it is a superset of information security and also comprise of managing relevance, integrity, accuracy, authentication, confidentiality and other similar attributes of information (Thomas, Ang, Parbati Ray, & Nof, 2001). The main thrust of this chapter is on Information Sharing, which plays a crucial role in mitigating dire consequences of any disaster or threat to our social/business infrastructure. Here we will be analyzing different attributes of information which will also be referred to as information quality dimensions in the sections ahead and will draw some inference on deciding about their priorities during different kinds of disaster. So we will be studying information assurance through the spectrum of Information Sharing during disasters. It is important to note here that the terms disasters, emergency, crisis, calamity and catastrophe, all may have different meanings in their respective fields. However, as a part of this chapter, all these terms refer to the same context and may appear interchangeably. Similarly, information attributes and information quality dimension are both assumed to mean the same.

Information Sharing is a fundamental component of a successful security program. With the high-level of inter-dependent business operations among business partners and automated control systems, organizations can derive value from accessing and sharing appropriate information. Nevertheless, doing the same in a secure fashion is indeed a daunting challenge, since we have to deal with information content that ranges from the simple to the complex (e.g., travel records, weather information, citizenship records, financial information, intelligence reports, military positions and logistical data, map data, etc.) in an interoperable environment that is constantly changing (Phillips, Ting, & Demurjian, 2002). Therefore, it becomes very important to understand the significance of various information attributes during any disaster management operation, because handling information in a way that can facilitate the special information needs of the particular disaster will expedite the relief operations. Our interest is to help disaster management organizations (DMO) prepare a framework for quick and secure Information Sharing that is required in response to a crisis, e.g., natural disaster (earthquake, hurricane), terrorist attacks (biological warfare or explosions), etc.

Background

In the United States, There are approximately 30,000 local governments, 30,000 local fire departments, 18,000 local police departments, 15,000 school districts, and 3,400 county governments (Pelfrey, 2005). Many organizations collaborate together for responding to a major disaster; for example during the disaster response of 9/11 terrorist attacks in New York City, there were 1,607 governmental and non-governmental organizations involved (Kapucu, 2004). Major international volunteer organizations such as the

Red Cross and Voluntary Organizations Active in Disasters (VOAD) also played an important role in mitigating the disaster impact. Incompatible technology can be a serious concern for all of these organizations. During 9/11 response activity, there was a big communication bottleneck created between responders from different organizations of New York City due to incompatible radio systems. The usage of analog radios by the Fire Department failed in the same way as it happened during 1993 World Trade Center attack (Jaeger, et al., 2007). The following excerpt highlights the technological barrier to the Information Sharing during 9/11 attack:

Firefighters, police, and other emergency personnel at the Pentagon and in New York City could not find common radio frequencies to communicate—cell phone networks flooded frequencies and further hindered information flow in the hours following the 9/11 attacks. (Riley, 2003)

The overall coordination and Information Sharing was even more concerning during the response to Hurricane Katrina. Federal, state and local government agencies and private organizations were very inefficient in coordinating and interrelating their activities, lacked an overall operational concept and had no proper system at place to track and share information (Wise, 2006), Secretary of Homeland Security Michael Chertoff told Congress that the response was ''significantly hampered by a lack of information on the ground'' (Chertoff, 2005) and the White House report on the failures of the Katrina response mentioned it as ''inability to connect multiple communication plans and architectures clearly impeded coordination and communication at the federal, state, and local levels'' (WhiteHouse, 2006).

In an emergency, it's generally not possible to know all the answers yourself, but it's quite important to know the resource/entities or collaborating organization that has the answer. Disasters, as we know are mostly unexpected and unavoidable events. Today we are aware of which regions are prone to tornadoes or hurricanes and where the earthquake faults are buried. But what we can never accurately predict, with a comfortable degree of certainty, is what path the hurricane will take, when the earth will shake, how and when terrorists will launch their attack, or where the plane will crash. Yet one thing we surely know is that when a disaster strikes, there will be a pressing need for reliable information exchange to take place. How well we are able to manage that information before, during, and after a disaster can have a direct impact on how well we manage the crisis. So the real essence of Information Sharing is to let the correct information timely reach the appropriate receiver, at the right place and in an understandable format. And this is where the equilibrium gets lost immediately after the disaster. All the information attributes go haywire, unanticipated delays occur, confusion prevails all ultimately resulting in bad emergency response decisions and actions. If a general framework can guide disaster management organizations to focus on more critical information attributes in different types of emergency situations, it will expedite the emergency response operations and will be a boost for disaster management. Previous research in this area focused on describing the emergence and development of the disaster situation under scrutiny, adopting a case study and qualitative analysis approach. While such studies suggest some factors that could influence the performance of disaster management operations in the study context and offer an insight into the particular situation, not many studies have offered objective evidence that certain attributes of information is critical in a disaster response operations.

INFORMATION QUALITY

Intuitively and broadly, "Information Quality" is the degree to which information meets the needs of its users (Gasser & Twidale, 2005). Since differ-

ent people use information for different purposes, it often happens that information which is high quality for one user is low quality for another. For example, when a large-scale wildfire breaks out, information about weather conditions is more relevant for fire crew and evacuation teams than it is for police and Emergency Medical Service (EMS). That's because fire crew may have to use different attack plan to fight against spreading fire, while evacuation team need to determine the best evacuation path depending on the changing direction and strength of the wind. Similarly the information about approximate casualty level might be more important for Emergency Medical Services since they need to dispatch sufficient medical resources to the disaster site, while preserving as much medical resources as possible for other areas. Yet, it is very important that all information that is sent across from one organization/entity to another is of high quality for a successful emergency response.

Quality Dimensions

Information quality as such, unfortunately, is difficult to observe, capture or measure. Information quality dimensions are the means by which we can measure quality of Information (H. Miller, 1996). Several researchers have identified the dimensions of information quality with as many as 15 dimensions identified by Strong et al. in 2002. In another research project, a literature review was conducted to find out the list of most common information quality dimensions (Parker, 2006). In that study, papers dealing with all quality dimensions and published during the years 1996-2005 were examined and the frequency of each dimension was calculated across those publications. In this chapter, we adopt the nine common information quality dimensions identified by the previous study (Parker, 2006). They are discussed briefly below:

Timeliness

Timeliness is the degree to which information is up-to-date. It can be seen in an objective fashion, meaning that information represents the current state of the real world. Timeliness can also be seen as task-dependent, meaning that the information is timely enough to be used for a specific task. It is one of the most important quality dimensions for handling disasters, because providing new information instantly is a major success factor of preventing a disaster or mitigating its effect. Information must be timely, and not "stale". Stale information is what has become outdated and has been replaced by new information. The implications of untimely/stale information during a disaster can be considerable. Not only does it lead to the expending of valuable time in processing that information, but it also prevents the appropriate response needed by the actual situation. To enable coordination and synchronization of multiple operations, information has to be up to date. Quoting an e-mail sent by a White House Homeland Security Council officer during the Katrina response:

... sending us very stale sit rep info that has already been updated (earlier) by the HSOC is not as helpful. Is there a way to coordinate the info flow so we don't waste time receiving such old data and you folks don't waste time sending us stuff? (Christopher & Robert, 2002)

Also, Timeliness and Accuracy go hand in hand. When a situation changes dynamically, any situational information that is not timely is not accurate.

Security

Security has been identified as another important information quality dimension. If information

is not secure, it can be easily intercepted by any intelligent opponent (e.g., terrorists, criminals) and used in a harmful manner. For example, if there is a huge fire that needs to draw police, medical and fire responders from surrounding areas, and if a criminal comes to know this, (s)he can take undue advantage of this information: (S)He can identify which area lacks police force and commit a crime in that area. This information quality dimension is especially important when there exists an active and strategic opponent (e.g., in a terrorist attack situation), as the degree of damage that can be done by information leakage in such cases can be extremely higher. Two aspects of information security include protecting information from intentional and unintentional human acts (information security) and protecting information from disasters (disaster recovery planning). Cyber security relies on logical barriers such as data encryption, passwords and transaction authentication, along with human vigilance. Disaster recovery planning involves protecting information and ensuring appropriate back-up and alternate processing procedures are in place (H. Miller, 1996).

Accessibility

For information to be utilized in an effective manner, it must be accessible. Accessibility implies the degree to which information is available, easily obtainable or quickly retrievable when needed. But this availability of information to the users is generally within the constraints of policy and confidentiality. Knowledge of the existence of information, its availability, and the tools necessary to acquire it are key attributes of access (Fuerth, 1997). It enables Information Sharing, giving an impression as if resources were centralized. When coupled with timeliness, it permits synchronization of interdependent activities. Accessibility is an important issue in a disaster situation as it often happens that all means of communication get disrupted in a disaster. For example, during Hurricane Katrina, the communication infrastructure was completely devastated in many parts of the affected area, and the responders had very tough time in coordinating their emergency response operations (D. R. Miller, 2006).

... It got to the point that people were literally writing messages on paper, putting them in bottles and dropping them from helicopters to other people on the ground. (WhiteHouse, 2006)

The disaster management organizations should identify the technical and other barriers limiting the access to information during disasters and make a cooperative effort to surmount them.

Completeness

Completeness is the degree to which information is not missing. Incomplete information can be hazardous. However, complete information for one person may be incomplete for another. For example, emergency medical services, FBI and Fire crew, all may be interested in the weather conditions around the disaster site, but each may require different levels of detail. Just as information of which precision exceeds a recipient's processing capability may be too accurate, information may also be too complete. During a disaster, it's also an adverse situation that the amount of information generated is so much that processing it all in a timely fashion becomes infeasible. At the same time, in a disaster response, if information is incomplete, it becomes difficult for the responders to accurately assess the situation and hence they are unable to respond effectively. The following excerpt illustrates this situation:

.....Each data set was examined to evaluate the completeness of records as a useful indicator of quality. The mere recording of the occurrence of a disaster with no other information on it makes the record essentially unusable for analyses. (Debarati & Below, 2000)

Accuracy

Accuracy is the degree of correctness and precision with which information in an automated system represents states of the real world. It is a very important quality dimension that on which many early information quality studies have focused (Alexander, 1999; Katerattanakul & Siau, 1999; Strong, Lee, & Wang, 1997). Within information production processes inside organizations, accuracy can be improved by implementing institutional procedures, like having information double checked by two independent people, or by installing technical means, like calibrating sensors or verifying shipping address information received through a website against an address database. The concept of accuracy implies the assumption that information can be captured in an objective fashion. Thus, accuracy is not applicable to subjective information, like destructive impact, public perception or political views. Inaccurate information may be worse than no information at all. Example, if a fire crew does not know the type and extent of situation at a disaster site, they will at least try to extract more information. However, if they have been given inaccurate information, they may respond with inappropriate strategy, which may lead to loss of innocent lives. Similarly, inaccurate information about the death toll in a disaster can lead to pandemonium in public.

Coherence

Coherent information is what "gels" or blends with itself consistently. Incoherent information can lead to confusion and panic during a disaster. This can lead to wastage of valuable time as well as resources. Coherence implies that two or more values do not conflict with each other. Information generated during a disaster is likely to be inconsistent as multiple information providers, which might use different procedures to capture information, have different levels of knowledge and different views of the world. Since most people are exposed to information through a number of media and from various sources, it must be consistent in order to be credible. Inconsistent information tends to confuse people and allows them to discount some or all of it. For example:

numerous organizations--state agencies, the Red Cross, school authorities, and media outlets--in California met in the immediate aftermath of the Loma Prieta quake just to discuss and agree upon the wording all of them would use for the "Drop, Cover, and Hold!" message.(Sarah et al, 1999)

Relevance

Relevancy is the extent to which information is applicable and helpful for the task at hand. Information must be relevant as per the demands of situation, i.e., it must address the needs of the end user to whom it is being transmitted. For example, when a user calls a 911 operator to tell about an emergency, he might tell irrelevant details out of panic. The operator must analyze what information should be sent across to the responders and ask relevant questions to complete the information. The key component for information quality is whether the information addresses its user's needs. If not, then the user will find the information inadequate regardless of how well the information rates along other dimensions mentioned in this chapter.

Validity

Information should be valid in the sense that it must be true and verified; it must satisfy the set standards related to other dimensions such as accuracy, timeliness, completeness and security. The most common form of information validation is auditing. Auditing can uncover mistakes and is a good way to measure the quality of information (Whitehouse, 2006). Validity is a resultant rather than a causal dimension of information quality.

This means that even though some information may be classified as being highly 'valid', it still may fall under poor quality information if other crucial dimensions like accuracy, timeliness etc. is absent (H. Miller, 1996).

.....When indicators possess high degree of reliability and validity, the data and information they generate is more useful in continuously improving performance. Conversely, indicators that are unreliable and invalid produce confusing, irrelevant and useless data and information while consuming precious resources..... (O'Leary, 2004)

Format

Information must be in such a format that it is uncomplicated and easily understood by the end user. This is especially true in a disaster situation as minimum time must be wasted between information processing and actual response. Information format refers to how the information is presented to the user. Two key components of information format are its underlying form and its context for interpretation, which is sometimes referred to as its frame (H. Miller, 1996). The appropriate format for information depends on the information's recipient and the information's use. For example, while giving demographic details or statistics of any past event, multi-color pie charts may be a better format than putting numbers. Moreover, during disaster management, if there is a commonly agreed upon format for exchange of information between two organizations, say Fire department and 911 operators, it aids understandability and expedites the response. Since there might be huge data to handle, it's always better to keep them formatted instead of letting them go haywire.

For each disaster, too many database and software have been developed and designed and millions of money has been expended. These projects are substantially costly and the main problem are the existing of many parallel sub-systems and activities and repeat labor works in different database format which have to be created for each hazard management systems. Such methodology will be so complicated due to implementation of different platform, different database format, and different program languages and so on. This will make all projects costly and non-efficient. (Assilzadeh & Mansor S.B., 2004)

DISASTER TYPES

Disasters may be natural or man-made. Natural disasters include earthquake, natural fires, volcanoes, tsunami, hurricane, landslide, flood, drought, and so on. Man-made disasters include bio/chemical/radiation/fire emergencies caused by human error or by strategic opponents (e.g., terrorists) and so on. Whatever may be the disaster type, it needs adequate and timely response by several government agencies that interact and exchange information with each other to combat the disaster. In order to make the study more manageable, in current context, we limit our scope to hurricanes, earthquakes, and terrorist attacks.

Disaster Cases Analyzed

We have focused on the below disasters:

1. Katrina Hurricane: It was the third most intense United States (U.S.) land-falling hurricane on record based on central pressure. The catastrophic damage and loss of life inflicted by this hurricane is an estimated 1,353 direct fatalities and 275,000 homes damaged or destroyed. Total economic losses could be greater than $100 billion (Groumann, Houston, & Lawrimore, 2005).
2. Indian Ocean Earthquake (and resulting Tsunami): It originated with an epicenter off the west cost of Sumatra, Indonesia on December 26, 2004. It killed an estimated

350,000 people and caused losses worth US $4.45 billion (Athukorala & Resosudarmo, 2005)

3. 9/11 Attacks: It occurred on September 11, 2001 when a series of suicide bombings using hijacked commercial air-liners hit several strategic US locations. The attacks killed more than 2,600 people (9/11 Commission report, 2005) and caused economic losses in NYC worth US $83-$95 billion (Thompson, 2002).
4. Anthrax Attacks: During the fall of 2001, mail packages containing large numbers of Bacil lus anthracis spores were sent to people at several locations in the US. 22 people got seriously infected and five of them died. As many as 30,000 people in the U.S. Postal Service (USPS) initiated preventive antibiotic treatment (Alibek, Lobanova, & Popov, 2005).

We selected the above mentioned four cases for our research because they not only caused loss of human life and capital, but also grabbed widespread public and media attention in the recent past. Out of these, Tsunami and Hurricane Katrina are natural disasters and 9/11 attacks and Anthrax attacks are man-made. Therefore, our findings will also help in distinguishing the relative significance of information quality dimensions during disaster management in both of these kinds of disasters.

Before we proceed with content analysis, let us make a few statements about expected relationships between the above mentioned information quality dimensions and one or more types of the disasters examined in the content analysis. Security will be obviously more important in the two terrorist attacks (9/11 and Anthrax attacks) than in the other two disasters, because strategic opponents are present. Accessibility will be more important in disasters where communication infrastructure is damaged. Therefore, we can expect that media articles about larger-scale disasters like Katrina and Tsunami would put more weight on the accessibility dimension, compared with other types of disasters of which damages were isolated within a relatively small geographical area (e.g., a city) or did not disrupt telecommunication networks. Timeliness will be more important when the threat situation in a disaster develops dynamically and at a fast phase. Thus, logically, media reports about 9/11 and the Tsunami should emphasize timeliness more than reports about the Anthrax attack.

CONTENT ANALYSIS

In order to be able to quantify the information quality attributes so that they can be compared to determine their relative importance in a disaster situation, we used a semantic content analysis approach. Content analysis is a research method by means of which the presence of certain words or concepts within a given text can be determined (Busch, et al., 2005). Holsti (1969) broadly defines content analysis as, "any technique for making inferences by objectively and systematically identifying specified characteristics of messages". This tool can be used to predict the content and meaning of the text or article under consideration.

In our research, we used CATPAC as content analysis software. CATPAC is a self-organizing artificial neural network computer program that has been optimized to read and analyze large amounts of text (Kim, Song, Braynov, & Rao, 2005). This program identifies the most frequently occurring concepts in a given text which can be interpreted as a measure of importance, attention, or emphasis of that concept (Krippendorff, 1980).

Document Corpus Construction

Since we wanted to predict the importance of information quality dimensions *during* a disaster response, we collected several journal articles and

news items relating to emergency response of each disaster event under scrutiny. The articles were collected from comprehensive databases such as Academic Search Premier, MasterFILE Premier, InfoTrac Newspapers, LexisNexis Academic, and Factiva. After a manual inspection to assure relevance, we selected 50 media and journal articles to conduct a semantic content analysis. The list of these articles has been included in Appendix A at the end of this chapter.

Semantic Analysis to Identify Keywords

We created a list of keywords (Table 1) which represent each quality dimension (*semantically equivalent categories*). We included several synonyms while creating the list of keywords for each dimension, considering the fact that authors may use synonyms for stylistic reasons throughout a document – if only a single word is used to do content analysis, it can lead us to underestimate the importance of a concept (Weber, 1990). For example, an author might use the word 'available' or 'reachable' or 'accessible' while talking about the 'accessibility' aspect of information, and so, we need to consider all three words while doing a content analysis. Similarly, the author might use the word 'inaccessible' or 'unavailable' and still be talking about 'accessibility' (rather, *in*accessibility) aspect of information. As a result, our list of keywords includes both synonyms as well as antonyms to represent a quality dimension. While we understand the limitation that every keyword in each category may not represent that category equally well, there is no well-defined procedure to assign the *weight* of each word (Stemler, 2001). Consequently, we proceeded with our research under the assumption that all keywords for an information quality dimension (i.e., category) are of equal 'weight'.

Table 1. Keywords

Information Quality Dimension	Keywords
Timeliness	timeliness, delay, delays, time, timely, timelines, immediate, immediately, late, early, prompt, slow, fast, speed, waiting, prolonged, expedite, expedited
Security	safe, unsafe, secure, security, threat, threats, threaten, risk, risks, violence, crime, criminal, lawlessness, terrorism, terrorist, protection, protect, protected
Accessibility	accessible, inaccessible, communication, communicate, communicating, reach, reached, coordination, coordinate
Completeness	incomplete, complete, adequate, inadequate, unknown, unaware, insufficient, integrity, wholeness, entirety
Accuracy	accurate, inaccurate, accurately, confirmed, uncertainty, uncertain, rely, reliable, relied, wrong, false
Coherence	coherent, inconsistent, ambiguous, confusion, conflicting, uniform, concrete, consistent
Relevance	relevant, irrelevant, useless, useful, lengthy, redundant, applicable, applicability, cogency, pertinence
Validity	valid, validated, invalid, obsolete, outdated, substantiate, substantiated, unsubstantiated, credible, warrant, warranted, unwarranted
Format	standardized, complex, complexity, complicated, meaningful, unclear

Frequency Analysis

We then conducted a content analysis of the articles using CATPAC and summed up the frequency of words for each dimension, with frequency counts determining the relative concern of each dimension. Also, in order to ensure that we did not miss any high frequency keyword that could possibly represent an information quality dimension, we reviewed all high frequency words in content analysis results. Any word that we found was highly correlated and semantically similar to an existing keyword was added to our list, and then the results were revised accordingly.

Total number of content bearing words for the four disaster cases came out to be:

1. Hurricane Katrina: 4062
2. Tsunami (Indian Ocean Earthquake): 778
3. 9/11 Attacks: 4995
4. Anthrax Attacks: 4082

Since most of the articles analyzed in this study were published in the US, we can see that the total number of content bearing words in Tsunami is relatively less than those in the other cases. Nevertheless, the total word count will not have any impact in determining relative importance because we are measuring the hit density of keywords belonging to different information quality dimensions within a particular disaster.

Filtering Ambiguous Words

Simple frequency of words may not actually represent the importance of each dimension as words can have multiple meanings or appear in multiple contexts. For example the word "uniform" can have a noun meaning "clothing", an adjective meaning "evenly spaced", or an adverb meaning "provide with uniform". In order to resolve the ambiguity in the context in which the words appeared, we used the Key Word In Context (KWIC) search to test for the consistency of word usage. We used HyperRESEARCH to pull up the sentences in which the keywords were used to perform a validation of our results (Stemler, 2001). HyperRESEARCH is a software package that assists collection and analysis of qualitative data. We reduced the word count wherever we found that the context where the word appeared was not 'information' or 'information quality' related.

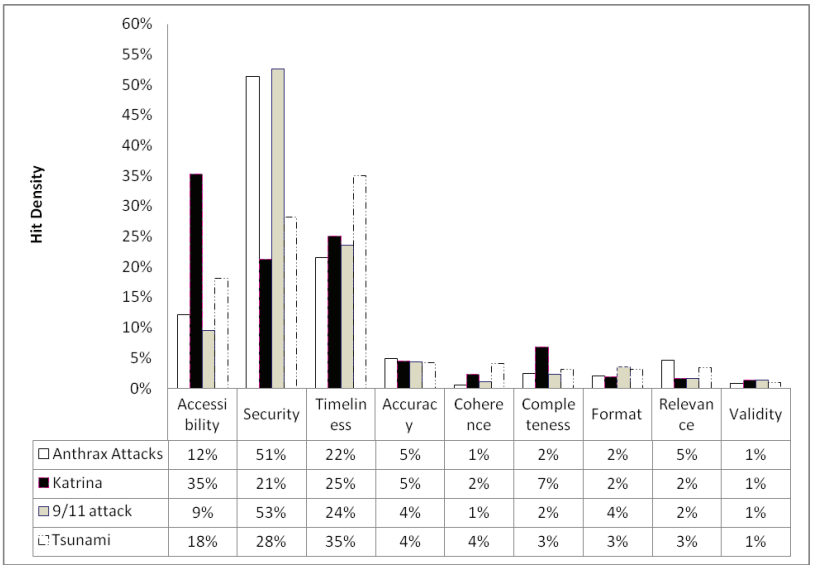
Hit Density

Since the length of articles varied, the absolute number of keywords appearing in the corpus thus did not represent the actual relevance of each dimension. Therefore, we calculated the '*hit-density*' of keywords corresponding to each information attribute. The hit density is a ratio of the number of hits divided by the number of content-bearing words in an article (Efthimiadis, 1993). Here we define the term 'hits' as the number of words corresponding to the quality attribute under consideration, and 'number of content bearing words' as the total number of words that represent *all* quality attributes for a given disaster situation. For example, the number of words associated with the dimension 'accessibility' for the disaster Katrina was 1,431, while the total number of words obtained by summing up word count for *all* dimensions for disaster Katrina was 4062. The hit density is 1,431/4,062, i.e., 35. Accordingly, a hit density index that represents the importance of an information quality dimension can be compared with those of other dimensions within a disaster as well as across all disaster cases. The results of hit density analysis are graphically represented in Figure 1 to facilitate sense making and easy reading of the results.

From the hit density analysis results, we can observe several interesting differences within and across different types of disasters.

1. Security is, by far, the most important issue in terrorist attacks (i.e., Anthrax and 9/11at-

Figure 1. Hit density analysis



	Accessibility	Security	Timeliness	Accuracy	Coherence	Completeness	Format	Relevance	Validity
Anthrax Attacks	12%	51%	22%	5%	1%	2%	2%	5%	1%
Katrina	35%	21%	25%	5%	2%	7%	2%	2%	1%
9/11 attack	9%	53%	24%	4%	1%	2%	4%	2%	1%
Tsunami	18%	28%	35%	4%	4%	3%	3%	3%	1%

tacks), while it still remains as the 2nd and 3rd important dimension in Tsunami and Katrina cases respectively. We can induce from this result that existence of an active intelligent opponent (e.g., terrorist) can force stakeholders (e.g., emergency responders, potential victims) to maintain a high-level of information security during emergency response operations. If information is insecure, it could easily be intercepted and misused to spread more terrorism. However, even when there is no immediate threat from intelligent opponents, security seems to remain as an important concern to many stakeholders (e.g., victims, the public, government agencies, non-government relief organizations), because a large-scale disaster will inevitably involves exchange of sensitive information across different organizations with different security requirements.

2. Timeliness was the most important issue in the Tsunami case (35%) and the 2nd most important issue, with almost equal levels (22-25%), for the other cases. It is obvious that if information does not reach the responders in time, they will not be able to respond before irrevocable and serious damages have already been done. One possible explanation of the relatively high level of the hit density in the Tsunami case may be the time lag between the earthquake and the strikes of tsunami at different regions, because effective and timely warning might allow potential victims to evacuate or minimize the damages. In addition, the extremely higher number of casualty, as the death toll (350,000) suggests, could require timely responses to save valuable, yet perishing lives.
3. Accessibility was the most important issue in Katrina (35%), and the 3rd most important issue in all the other cases (9-18%). However, the gap between Katrina and the other cases are quite obvious, unlike the timeliness dimension. We suspect that the unexpected scale of damages on the once-reliable communication infrastructure could cause the surge of emphasis on accessibility. Also, the number and the variety of organizations involved in the relatively long recovery period, together with the level of bureaucracy imposed by the hierarchical

structure of the US disaster management agencies could result in accessibility issues among different stakeholders.

4. All the other dimensions (i.e., accuracy, coherence, completeness, format, relevance, and validity) are much less emphasized (mostly below 5%), regardless of the types of disaster, than the three most important dimensions (i.e., accessibility, security, timeliness). While it is still much lower than the other dimensions, the hit density of completeness in the Katrina case is distinctively higher than those in the other disasters. This may also result from disruption of communication and transportation systems, as well as reliance on archival systems that became unavailable by the impact of the disaster. One important point to make clear is that the low levels of these dimensions do not necessarily mean these are not important dimensions. We assume that published articles reflect the current issues in the respective context. Therefore, we can consider the three most important dimensions (i.e., accessibility, security, and timeliness) as the ones that became the center of hot discourse because we have misunderstood their impacts, resulting in mis-configured disaster management systems.

From the results of the comparative analyses of information quality dimensions in different disaster situations, we can conclude that these dimensions hold varying significance across different disasters. We can also infer some factors that might influence the differences in the importance levels of the three most important dimensions. Therefore, it is recommended that information be exchanged between different organizations on the basis of the circumstances and resulting relative significance of these information quality dimensions. The prioritization process which can be created utilizing these results will certainly help the emergency response operation to focus on the information quality dimension which matters the most and thus will reduce the impact of disaster significantly by expediting the relief operations. Moreover, this will save time and resources which get dissipated dealing with less significant dimensions and thus can be utilized in the right direction to respond to the disaster in a better way.

In the previous sections, we discussed the important attributes of information. Taking the information security aspect a step further, let us continue our research to analyze the aspects of information assurance. We will perform content analysis to explore the relative significance of different dimensions of information assurance to provide us with more valuable conclusions which can be utilized to build a prioritization framework in mitigating disaster impacts.

Information Assurance

Information assurance is often used interchangeably with information security. But in specific terms, information assurance can be defined as information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes provision for restoration of information systems by incorporating protection, detection and reaction capabilities (Maconachy, V., Schou, Ragsdale, & Welch, 2001). At the heart of Information assurance is the provisioning of five security services: *Availability, Integrity, Authentication, Confidentiality, and Non-Repudiation* which we are considering as the five important dimensions of information assurance.

1. *Availability* can be defined as timely, reliable access to data and information services for authorized users. It means that the information, the computing systems used to process the information, and the security controls used to protect the information

are all available and functioning correctly when the information is needed. Often it is viewed as a function, which is not entirely security related. Availability is equated with information system operations such as redundant communication channels, back-up power and off-site capabilities to handle crisis. Availability is the utility part of security services. There may be times during the course of operations that demand system availability at the expense of the other security services. The decision to abandon the other security services is a risk mitigation decision often driven by threats and vulnerabilities that fall beyond the system security parameters. Broadcasting a decision or some critical information at the time of disaster, to handle a life-threatening condition may override concerns to do so in a totally secure fashion (Maconachy, et al., 2001).

2. *Integrity* is "the quality of an information system reflecting logical correctness and reliability of an operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data." (Lohse et al, 2003). It means that data cannot be created, changed, or deleted without authorization. In a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information. Data integrity is a matter of degrees of trust. Integrity must include the elements of accuracy, relevancy, and completeness. Data and system integrity implies robustness.
3. *Authentication* is a security service, "designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorizations to receive specific categories of information" (Maconachy, et al., 2001). Authentication provides a foundation for many security services by ensuring that data, transactions, communications or documents (electronic or physical) are not exposed to unauthorized entities thereby giving them a chance to tamper or misuse them.
4. *Confidentiality* is "the assurance that information is not disclosed to unauthorized persons, processes or devises" (Maconachy, et al., 2001). The application of this security service implies information labeling and need-to-know imperatives are aspects of the system security policy. Information that is considered to be confidential in nature must only be accessed, used, copied, or disclosed by persons who have been authorized to do so, and only when there is a genuine need to do so. A breach of confidentiality occurs when information that is considered to be confidential in nature has been, or may have been, accessed, used, copied, or disclosed to, or by, someone who was not authorized to have access to the information.
5. *Non-Repudiation* refers to the assurance that "the sender of the data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data" (Fry, 2001). Non-repudiation has ramifications for electronic commerce as well as battlefield orders. Electronic commerce uses technology such as digital signatures and encryption to establish authenticity and non-repudiation.

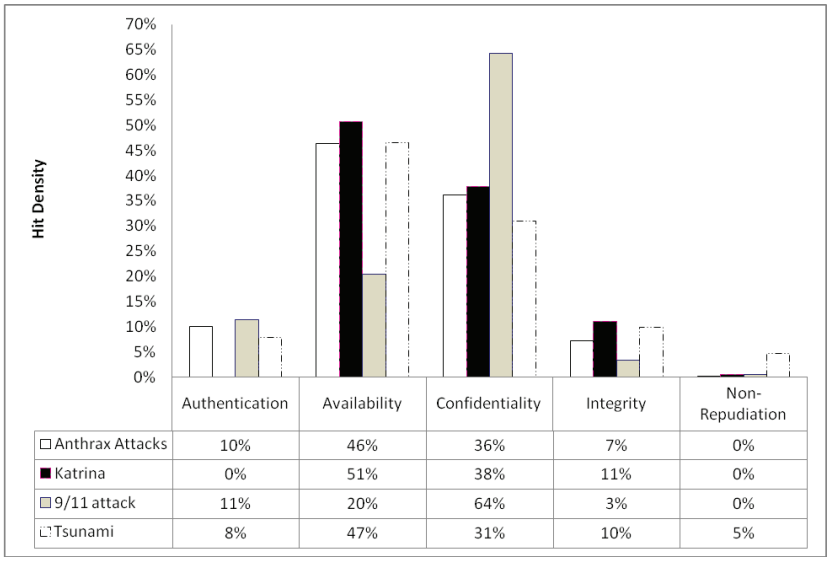
Now let us do the content analysis of above five mentioned dimensions by using the keywords described below in Table 2, across all the four disasters. Our research approach is the same as we did in the previous content analysis.

After doing content analysis across all the four disasters, we calculated the hit density, as done in the previous section, and plotted them on the bar chart as shown below in Figure 2:

Table 2. Content analysis keywords

Information assurance attributes	Keywords
Availability	Available, accessibility, accessible, inaccessible, communication, communicate, communicating, reach, reached, unavailable, availability, unavailability
Integrity	Completeness, wholeness, relevance, accuracy, incomplete, complete, adequate, inadequate, insufficient, Tamper, tampering, repudiate, manipulate, integrity
Authentication	Valid, genuine, certify, attest, evidence, validity, authenticity, authenticate, authenticated, authenticates, manifest, manifestation, authentication
Confidentiality	Privacy, secret, secrecy, private, classified, confidential, confidentially, conceal, concealed, covert, covertly, unacknowledged, confidentiality
Non-Repudiation	Reject, disown, renounce, repudiate, encryption, decryption, time-stamp, time-stamped, signature, unfair, disclaimer, disclaim, repudiation, non-repudiation

Figure 2. Hit density analysis



	Authentication	Availability	Confidentiality	Integrity	Non-Repudiation
Anthrax Attacks	10%	46%	36%	7%	0%
Katrina	0%	51%	38%	11%	0%
9/11 attack	11%	20%	64%	3%	0%
Tsunami	8%	47%	31%	10%	5%

From the result of the above content analysis, we can draw the following conclusions:

1. *Confidentiality* was the dominant concern in 9/11 attack (64%), while it was the 2nd most important issue in the other disasters (31-38%). Interestingly, this attribute was not as much emphasized in the other terrorist attack case (i.e., anthrax attacks) as it was in 9/11. This difference between the two types of terrorist attack cases may come from the nature of attack. In 9/11, the attack was carried within a relatively short period of time, and nothing was clear at the point of attack, from which the US intelligence community had to figure out what really happened and how to handle the situation, before the public is informed of what the

public needs to know. On the other hand, the anthrax case involved multiple attacks that aimed at seemingly random targets. Therefore, the public, as a group of individuals who may become a victim of the next attack had to be informed, educated, and mobilized, in order to minimize the impact of the attacks and maximize the chance to catch the attacker by encouraging bottom-up information flow for terrorist investigation tips, in the anthrax case. Therefore, it's very important to assure confidentiality of any information that has a potential to have a negative consequence, should the information fall in the hands of active opponents, while confidentiality should give a way to availability (or some other attributes) if the situation requires cooperation from other relief agencies or the public.

2. In contrast to confidentiality, *Availability* was a more important attribute in the Anthrax attack (46%), Katrina (51%), and Tsunami (47%) cases. It took 20% of the content-bearing words in the 9/11 case, which is a smaller portion, but still the 2nd important dimension. This may reflect issues like inconsistent access control for inter-organizational Information Sharing, lack of redundancy in communication links, absence of good backup practice, and improper business continuity planning for disaster management operations. The results show that confidentiality and availability are two most critical information quality dimensions, together taking a major portion (79 -89%) of the content-bearing information security words in the four disaster cases. The hit densities of *Authentication*, *Integrity,* and *Non-Repudiation* were relatively low, suggesting that these dimensions were less of concern in the studied disasters. Non-repudiation appears especially irrelevant to the disaster management situation.

The results obtained can be utilized by government and non-government disaster management organizations to align their relief operations more effectively, by devising special mechanism to take care of every mentioned information attribute as per their significance. There are different organizations which are involved in different types and stages of disaster management operations. Among other information assurance attributes, they tend to focus on availability and confidentiality of information. The results suggest that availability is the most important information assurance dimension in the disaster management context, unless the situation requires confidentiality (e.g., information about the situation may benefit strategic opponents), in which case confidentiality may become the dominant dimension of information assurance quality over the usual golden rule of "availability goes first".

In Appendix B, we will touch upon a few of organizations and technologies that can help disaster management organizations achieve appropriate levels of availability and confidentiality for information assurance, while accommodating relevant information quality dimensions (e.g., accessibility, security, timeliness), in a disaster response situation. By utilizing these organizational and technological supports, relief agencies, esp. those who often participate in large-scale, multi-agency disaster management operations, will be able to better prepare for and improve their performance in different types of disasters.

CONCLUSION

In a disaster, every moment counts. A single minute saved can save a large number of lives, and thus it is very important to utilize time in the most efficient manner during the disaster response operations. Unfortunately, the situation often goes haywire immediately after the disaster, and the relief operations do not necessarily go in the

planned manner, giving rise to chaos all around and thus information quality suffers. There exists an urgent need for a prioritization framework on the basis of which information quality dimensions can be weighed and their relative significance used to orient the emergency response operations. In this chapter, we have reviewed nine information quality dimensions, which led us to deduce relative significance of some of the information attributes across different disaster types. Based on the results of our content analyses, this chapter provides empirical evidence that effective disaster management requires a right mix of information quality dimensions to be achieved in their communication, depending on the particular circumstances of the disaster. We also discussed several key organizations and technologies that can promote information assurance in disaster management and improve various aspects of information quality.

The results of our analysis suggest that security is one of the most important information quality dimensions for all types of disaster management, but a much higher level of information security must be provided when an active intelligent opponent (e.g., terrorist) may take advantage of the information about the situation. Timeliness is another very important attribute for all disaster types, but it may gain weight when there is a time lag between a sign of potential damage (e.g., ocean earthquake, request for an ambulance) and actual strike of the disaster (tsunami reaching a coastline, death of a life), during which potential victims or emergency responders can be prepared to minimize the impact. Disaster responders should pay more attention to accessibility if they need to respond to a disaster that affected a large geographical area. Interestingly, all the other dimensions included in our analysis did not receive much attention in the four disaster cases.

The chapter further analyzed 5 sub-dimensions of the information security dimension, one of the three hottest issues in the current disaster management communications. The results that we have obtained thus can be used by public and private sector disaster management organizations to create an *information dissemination prioritization framework* when responding in an emergency situation. Such a framework will aid decision-making when communicating information across organizations during a disaster. For example, agencies will know when to wait for information to get 'complete' while it is still 'secure,' and when to ensure that information is 'secure' while it is still 'complete,' and so forth.

While mostly in tandem with our predictions, the results of the content analyses also call for more research in this area. For example, a follow-up study may identify different dimensions of disasters (e.g., geographical and time span of the impact/recovery, number of involved responders/relief agencies, changes in the casualty at each phases of the disaster), which will allow more systematic analysis of possible relationships between information attributes and disaster attributes. Similarly, research on organizational attributes of disaster management organizations is highly likely to improve our understanding on the relative importance of information attributes. Also, the importance of various information quality dimensions can be measured on a single reference frame, which will allow direct comparison of the absolute value of the attributes. From a citizen-centric view point, analyzing personal web blogs or comments on first responder websites to understand the relative value of G2C (Government to Citizens) disaster communications will also be a meaningful research avenue. As such, we believe that our findings and discussions in this chapter can provide a fertile ground for future studies in the field of disaster management and information security.

ACKNOWLEDGMENT

This research has been supported by NSF under grant # IIS-0733388 and IIS-0809186. The usual disclaimer applies.

REFERENCES

Alexander, J., & Tate M (1999). *Web wisdom: How to evaluate and create information on the web*. Mahwah, NJ: Erlbaum.

Alibek, K., Lobanova, C., & Popov, S. (2005). *Bioterrorism and Infectious Agents: A New Dilemma for the 21st Century* .

Assilzadeh, H., & Mansor S. B. (2004). *Natural Disaster Data and Information Management System*. Paper presented at the XXth ISPRS Congress, Istanbul, Turkey.

Athukorala, P. C., & Resosudarmo, B. P. (2005). *The Indian Ocean Tsunami: Economic Impact, Disaster Management and Lessons*. Paper presented at the Asian Economic Panel Conference.

Busch, C., Maret, P. S. D., Flynn, T., Kellum, R., Le, S., Meyers, B., et al. (2005). *Content analysis.* : Writing@CSU. Colorado State University Department of English. Retrieved [Date] from http://writing.colostate.edu/guides/research/content/.

Chertoff, M. (2005). *Statement before the Senate Committee on Homeland Security and Governmental Affairs*. Department of Homeland Security: Second Stage Review.

Christopher, C., & Robert, B. (2002). *Disaster: Hurricane Katrina and the Failure of Homeland Security*. Macmillan Publishers.

Debarati, G. S. (2000). *The quality and accuracy of disaster data: A comparative analysis of three global data sets*. A study by the Provention Consortium.

Efthimiadis, E. N. (1993). *A User-Centered Evaluation of Ranking Algorithms for Interactive Query Expansion*. Paper presented at the ACM SIGIR, Pittsburgh, PA.

Fry, S. A. (2001). *Information assurance and Computer Network Defense*. Chairman of Joint Chiefs of Staff Instruction.

Fuerth, L. (1997). *Disaster Information Task Force Report*. The Global Disaster Information Network.

Gasser, L., & Twidale M. (2005). *Information Quality Discussions*. Graduate School of Library and Information Science, University of Illinois at Urbana-Champaign.

Groumann, A., Houston, T., & Lawrimore, J. (2005). *Hurricane Katrina: A climatic perspective*: US Department of commerce

Holsti, O. R. (1969). *Content analysis for the Social Sciences and Humanities*. Reading, MA.

Jaeger, P. T., Fleischmann, K. R., Preece, J., Shneiderman, B., Wu, P. F., & Qu., Y. (2007). *Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science*, *5*.

Kapucu, N. (2004). Interagency communication networks during emergencies: Boundary spanners in multiagency coordination. *American Review of Public Administration, 36*, 207-225.

Katerattanakul, P., & Siau, K. (1999). *Measuring information quality of web sites: Development of an instrument.* . Paper presented at the the 20th international conference on Information Systems., Charlotte, North Carolina, USA.

Kim, D. J., Song, Y. I., Braynov, S. B., & Rao, H. R. (2005). A multidimensional trust formation model in B-to-C e-commerce: A conceptual framework and content analyses of academia/practitioner perspectives *Decision Support Systems, 40*(2), 143-165.

Krippendorff, K. (1980). *Content analysis: An introduction to its methodology*. Beverly Hills, CA: Sage.

Lohse, E. S., Schou, C., Sammons, D., & Schlader, R. (2003). *Management, Research and Information Distribution in a Confidential, Controlled Environment*. Information Data Archives Idaho State University.

Maconachy, V. W., Schou, C. D., Ragsdale, D., & Welch, D. (2001). *A Model for Information assurance: An Integrated Approach*. Paper presented at the 2nd Annual IEEE Systems, Man and Cybernetics Information assurance Workshop.

Miller, D. R. (2006). *Hurricane Katrina: Communications & Infrastructure impacts, Threats at our threshold*. National Defense University.

Miller, H. (1996). *The Multiple Dimensions of Information Quality Information Systems Management, 13*(2), 79-82.

O'Leary, M. (2004). *Measuring Disaster Preparedness: A Practical Guide to Indicator Development and Application*: iUniverse.

Parker, M. B., Moleshe, V., De la Harpe, R., & Wills, G. B. (2006). *An evaluation of Information quality frameworks for the World Wide Web.* Paper presented at the 8th Annual Conference on WWW Applications, Bloemfontein, Free State Province, South Africa.

Pelfrey, W. V. (2005). The cycle of preparedness: Establishing a framework to prepare for terrorist threats. *Journal of Homeland Security and Emergency Management, 2*(1), 1-21.

Phillips, C. E. Jr., Ting, T. C., & Demurjian, S. A. (2002). *Information Sharing and security in dynamic coalitions*. Paper presented at the Proceedings of the seventh ACM symposium on Access control models and technologies.

Riley, B. (2003). Information Sharing in Homeland Security and Homeland Defense: How the Department of Defense Is Helping. *Journal of Homeland Security*.

Sarah, N., Paula, G., Greene, M., Lemersal, E., & Mileti, D. (1999). *Public Education for Earthquake Hazards*. Natural Hazards informer.

Stemler, S. (2001). An overview of content analysis. Practical Assessment. *Research & Evaluation, 7*(17).

Strong, D., Lee, Y., & Wang, R. (1997). Data Quality in context. *Communications of the ACM, 40*(5), 103-110.

Thomas, B., Ang, C. B., Parbati Ray, & Nof, S. Y. (2001). *Information assurance in Networked Enterprises: Definition, Requirements, and Experimental Results*. CERIAS Tech Report 2001-34.

Thompson, W. J. (2002). *One Year Later: The fiscal impact of 9/11 on New York city*. Comptroller, City of New York.

Weber, R. P. (1990). *Basic Content analysis* (2nd ed.). Newbury Park, CA.

WhiteHouse (2006). *The Federal Response to Hurricane Katrina: Lessons Learned*. Washington, D.C.: White House Report on Katrina,.

Wise, C. R. (2006). Organizing for homeland security after Katrina: Is adaptive management what's missing? *Public Administration Review, 66*, 302-318.

APPENDIX A: DOCUMENT CORPUS

HURRICANE KATRINA:

1. Agency, F. E. M. (2006). *DHS/FEMA Initial Response Hotwash: Hurricane Katrina in Louisiana,* . Baton Rouge, Louisiana: Federal Emergency Management Agency
2. Chua, A., Kaynak, S., Foo S. (2007). An Analysis of the Delayed Response to Hurricane Katrina Through the Lens of Knowledge Management. *Journal Of The American Society For Information Science And Technology, 58*(3), 391-403.
3. Edition, N. M. (Writer) (2004). Report Offers Post-Katrina Emergency response Recommendations: National Public Radio
4. Eosco, G. M., & Hooke, W. H. (2006). Coping with Hurricanes: It's not just about the Emergency response…, . *American Meteorological Society.*
5. In Wikipedia, T. F. E. (2008). Criticism of government response to Hurricane Katrina. , from http://en.wikipedia.org/w/index.php?title=Criticism_of_government_response_to_Hurricane_Katrina&oldid=222561822
6. Marchi, B. D. (2007). Not just a matter of knowledge. The Katrina debacle. *Environmental Hazards, 7*(2), 141-149.
7. Piper, P., & Ramos, M. (2006). A Failure to Communicate: Politics, Scam and Information Flow during Hurricane Katrina, Searcher: . *The magazine for database professionals, www.infotoday.com/searcher/jun*.
8. Representatives, U. S. H. o. (2006). *A failure of Initiative*: the Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina.
9. Rojek, J., & Smith, M. R. (2007). Law Enforcement Lessons Learned from Hurricane Katrina, . *Review of Policy Research, 24*(6), 589-608(520).
10. Shane, S., & Shanker, T. (2005). When Storm Hit, National Guard Was Deluged Too. *The New York Times*,
11. Stephan, K. D. (2007). We've got to talk: Emergency Communications and Engineering Ethics. *IEEE Technology and Society Magazine*.
12. Striedl, P., Crosson, J., & Farr, L. (2006). *Observations of Hurricane Katrina: Lessons Learned*: Association of Contingency Planners (ACP)
13. Treaster, J. B., Sontag D. (2005). Despair and Lawlessness Grip New Orleans as Thousands Remain Stranded in Squalor. *The New York Times*,
14. Venkataraman, S., Benger, W., Long, A., Jeong, B., & Renambot, L. (2006). Visualizing Hurricane Katrina: large data management, rendering and display challenges, Conference on Computer Graphics and Interactive Techniques in Australasia and Southeast Asia. *Graphite,* 209-212.

9/11 ATTACKS:

1. Carpenter, T. G. (2005). Missed Opportunities: The 9/11 Commission Report and US Foreign Policy. *Mediterranean Quarterly 16*(1), 52-61.
2. Jenkins-Smith, C., H., & Herron, K. G. (2005). United States Public Response to Terrorism: Fault Lines or Bedrock?, Review of Policy Research, . *22, 5*, 599-623(525).
3. Johnson, C. W. (2005). *Applying the lessons of the attack on the World Trade Center, 11th September 2001, to the design and use of interactive evacuation simulations.* . Paper presented at the *Conference on Human Factors in Computing Systems*, Portland, Oregon.
4. Kwan M-P, L. J. (2005). Emergency response After 9/11: The Potential of Real-Time 3D GIS for Quick Emergency response in Micro-Spatial Environments. *Computers, Environment, and Urban Systems, 29* (93-113).
5. Rashbaum, W. K. (2002). Commissioners Seek Closer Ties For Fire Dept. And the Police. *The New York Times*,
6. Report, T.-C. (2004). *Final Report of the National Commission on Terrorist Attacks Upon the United States* Official Government Edition.
7. Risen, J., & Johnston, D. (2002). F.B.I. Account Outlines Activities Of Hijackers Before 9/11 Attacks. *The New York Times*
8. Shenon, P. (2004). 9/11 Panel Set To Detail Flaws In Air Defenses. *The New York Times*,
9. Shenon, P., & Flynn, K. (2004). 9/11 Panel Has a Question: Why Wasn't the City Prepared? *The New York Times*,
10. Shenon, P., Flynn, K. (2004). Panel Criticizes New York Action In Sept. 11 Attack. *The New York Times*,
11. Staff Statement(2004), The National Commission On Terrorist Attacks Upon The United States, Threats And Responses In 2001
12. Wang, H. M. (2003). *Contingency planning: emergency preparedness for terrorist attacks.* Paper presented at the *Proceedings of IEEE 37th Annual 2003 International Carnahan Conference on Security Technology.*

TSUNAMI DISASTER:

1. Athukorala, P.-C., & Resosudarmo, B. P. (2005). *The Indian Ocean Tsunami: Economic Impact, Disaster Management and Lessons.* Paper presented at the Asian Economic Panel Conference.
2. Britton, N. (2007). *Lessons from ADB's Indian Ocean Tsunami Experience.* Paper presented at the Small Group Workshop on Preparing for Large Scale Emergencies.
3. Darcy, J. (2005). *The Indian Ocean Tsunami Crisis: Humanitarian Dimensions*: Humanitarian Policy Group.
4. *The December 2004 tsunami* (2007). (No. Online: http://ec.europa.eu/environment/civil/tsunami.htm): European Civil Protection
5. Dickson, D. (2005). Tsunami Disaster: A Failure in Science Communication. *SciDev.Net News*,
6. Dorsett, D. J. (2005). *Tsunami! Information Sharing in the wake of destruction*.
7. Fehr, I. e. a. (2004). Indian Ocean Tsunami Report. *Risk Management Solutions Publications*, Online: www.rms.com/Publications/IndianOceanTsunamiReport.pdf
8. Fidler, D. P. (2005). Disaster Relief And Governance After The Indian Ocean Tsunami: What Role For International Law? *Melbourne Journal of International Law, 6*.
9. Grünewald, F., Boyer, B., Maury, H., & Pascal, P. (2007). *Indian Ocean Tsunami 2004 : 10 Lessons Learnt From The Humanitarian Response Funded By The French State*: Groupe URD, French Ministry of Affairs
10. *IUCN* (2007). *Coastal Ecosystems*: International Union for Conservation of Nature and Natural Resources Newsletter.
11. Jefferys, A., Simha, V., Samuel, K., Kottegoda, S., & Eskeland, L. (2005). Sharing information for tsunami recovery in South Asia. The International Federation of Red Cross and Red Crescent Societies.
12. Leoni, B. (2005). *10 lessons learned from the South Asia tsunami of 26*: International Strategy for Disaster Reduction (ISDR).
13. Wattegama, C. (2007). A Tale of Two Tsunamis: What Went Wrong in Each Case *Daily Mirror*,

ANTHRAX ATTACKS:

1. Ackerman , G. A., & Moran , K. S. (2006). *Bioterrorism and Threat Assessment*. Sweden The Weapons of Mass Destruction Commission.
2. Bravata, D. M. e. a. (2002). *Bioterrorism Preparedness and Response: Use of Information Technologies and Decision Support Systems*: Agency for Healthcare Research and Quality Publication.
3. Chapman, J. (2005). *Countering Bioterrorism: How can Europe and the United States work together?* Paper presented at the the fourth meeting of the New Defence Agenda's Bioterrorism Reporting Group co-organised
4. Davis, R. (2001). Bioterrorism. *USA Today*
5. Editor Letters (2003) Bioterrorism Response, Science, Vol 300
6. Eisenstein, M., & Houghton, B. K. (2000). *Bioterrorism: Homeland Defense: The Next Steps.* Paper presented at the Executive Summary of the Rand Symposium Proceedings
7. Kaplan, E. H., Craft, D. L., & Wein, L. M. (2003). Analyzing bioterror response logistics: the case of smallpox. *Mathematical Biosciences 185*, 33-72.
8. Kress, M. (2006). Policies for biodefense revisited: The prioritized vaccination process for smallpox. *Ann Oper Res 148*, 5-23
9. Kun, L. G., & Bray, D. A. (2002). Information Infrastructure Tools for Bioterrorism Preparedness. *IEEE Engineering In Medicine And Biology*
10. Lee, B. Y. (2007). The Role of Internists During Epidemics, Outbreaks, and Bioterrorist Attacks. *Society of General Internal Medicine 22*, 131-136
11. Mackby, J. (2006). *Strategic Study On Bioterrorism*: Center for Strategic and International Studies (CSIS) Publication
12. Sharp, R. J., & Roberts , A. G. (2006). Review Anthrax: the challenges for decontamination. *Journal of Chemical Technology and Biotechnology, 81*, 1612-1625.

APPENDIX B: ORGANIZATIONAL AND TECHNOLOGICAL RESOURCES

United States Computer Emergency Readiness Team (US-CERT)

A partnership between Department of Homeland Security (DHS) and public and private sector organizations, US-CERT is charged with improving cyber security preparedness and response in the United States. Through US-CERT, companies can access valuable educational resources, find up-to-date security information and receive security alerts. Individual companies are encouraged to register with them to receive alerts, warnings and other cyber security related information that is relevant to company-specific technology.

Cyberspace is a combination of distinct information infrastructures, including government and business operations, emergency preparedness communications, and critical digital and process control systems. Protecting these systems is very important to the resilience and reliability of the Nation's critical infrastructures and key resources and, therefore, to its economic and national security. US-CERT has a very important responsibility to analyze and reduce cyber threats and vulnerabilities, disseminate cyber threat warning information, and coordinate incident response activities. They collaborate with other organizations like Federal agencies, the research community, private sector, state and local governments, and international organizations. By coordinating with different incident response centers using both classified and unclassified systems, US-CERT disseminates reasoned, critical and actionable cyber-security information to the public. (DHS Cyber Security, 2006)

The different collaboration efforts of US-CERT include:

- **US-CERT Web Portal:** Provides a secure web-based collaborative system to share sensitive cyber-related information with government and industry members. And secondly it provides the government, private sector, and public with information needed to improve US-CERT's ability to protect information systems and infrastructures; includes information on current activity, events, resources, publications, and affiliates.
- **National Cyber Alert System:** Delivers targeted, timely, and actionable information to Americans, educating them on how to secure their own computer systems.
- **National Cyber Response Coordination Group:** Established in partnership with the Department of Defense and the Department of Justice; serves as the federal government's principal interagency mechanism to coordinate efforts to respond to and recover from cyber incidents of national significance.
- **Government Forum of Incident Response and Security Teams (GFIRST):** Embodies a community of more than 50 incident response teams from various federal agencies working together to secure the federal government.
- **US-CERT Einstein Program:** Involves an automated process for collecting, correlating, analyzing, and sharing computer security information across the federal government to improve our Nation's cyber situational awareness.
- **Internet Health Service:** Provides information about Internet activity to federal government agencies throughout the GFIRST community.

After the calamity caused by Hurricane Katrina, Department of Homeland Security (DHS) realized that many critical infrastructure control systems were shutdown, damaged, or destroyed. Hence

they provided assistance to owners and operators in rebuilding and securely restarting those sensitive control systems. In order to assist control system owners, vendors, operators, and service providers in bringing control systems, and the sensitive processes and functions they monitor and manage, back into operation as safely and as securely as possible under the circumstances, the DHS US-CERT Control Systems Security Center (CSSC) compiled a set of items to consider when restarting and rebuilding control systems. (US-CERT, 2005)

CEO COM LINK for Business Roundtable CEOs

The Critical Emergency Operations Communications Link (CEO COM LINK[SM]) is a secure telephone communications system that will enable the nation's top CEOs to enhance the protection of America's employees, communities and infrastructure by communicating with leading government officials and each other about a threat or during national crises. This communication system links each of the Business Roundtable's 150 CEOS with the federal government to coordinate communication and facilitate effective response in times of crisis. Rapidly linking the private and public sectors during crisis can dramatically improve collaboration and effectiveness in enhancing homeland security.

The CEO COM LINK, developed by Business Roundtable, is an essential tool that enables this collaboration prior to, during, and in the aftermath of a significant national crisis. CEOs are alerted that the system is being activated and dial in to a secure conference call number. Each caller goes through a multi-step authentication process to ensure that only authorized participants are on the call. The calls also would allow CEOs to ask questions or share information with government leaders and with each other. Business rules have been established to govern calls and handle sensitive information (BRT, 2003).

Security is of utmost importance to ensure the confidentiality and integrity of information being shared. A critical security component is authentication. Each CEO is issued a means of authentication (e.g., voiceprints, caller ID), so a caller's identity can be verified. Because the private sector owns or operates 90 percent of our nation's critical infrastructures – including airlines, railroads, financial markets, telecommunications services and information services – CEO leadership in combating terrorist threats is critical to America's security. A timely and effective exchange of information between government and the private sector – and among business leaders – is critical for our nation's ability to detect additional threats, maintain homeland security, and respond effectively to threats or disasters.

Government Emergency Telecommunications Service (GETS)

GETS is a White House directed emergency phone service provided by the National Communications System through the Department of Homeland Security. GETS provides emergency access and priority processing in local and long distance in the Public Switched Telephone Network (PSTN). It provides Federal, State and local government National Security and Emergency Preparedness (NS/EP) users with a ubiquitous switched voice and voice-band data communications service and is used during periods of natural or man-made disasters or emergencies that cause congestion or network outages.

Different imperatives of GETS are:

- ***Access Authorization*:** GETS access control is accomplished through the use of Personal Identification Numbers (PINs) to ensure only authorized users gain access to GETS features and protect against fraud.

- ***Enhanced Routing*:** GETS calls use extensive enhancements to the PSTN's robust network of interconnecting paths between switches. With these enhancements to the grid of multiple switch connections, GETS calls can still be connected without any disruptions even when numerous switch failures occur in the PSTN.
- ***Priority Treatment*:** GETS allows that a high probability call identifier can be carried across the signaling network and used to trigger priority features such as trunk queuing and trunk reservation for designated emergency management communications.

European Network and Information Security Agency (ENISA)

The objective of ENISA is to improve network and information security in the European Union. The agency has to contribute to the development of a culture of network and information security for the benefit of the citizens, consumers, enterprises and public sector organizations of the European Union, and consequently will contribute to the smooth functioning of the EU Internal Market.

Different tasks done by ENISA are:

- Collect appropriate information to analyze current and emerging network and information security risks and provide the results of the analysis to Member States and the Commission;
- Provide advice and, if appropriate, assistance within its objectives to the European Parliament, the Commission and other competent bodies;
- Enhance cooperation between the different players in the sector (e.g., by organizing collaboration links between enterprises and universities) and facilitating cooperation between the Commission and the Member States in the development of common methodologies to prevent security problems;
- Contribute to awareness raising and the availability of rapid, objective and comprehensive information on network and information security issues for all users. This can be achieved by promoting exchanges of best current practice, including methods of alerting users;
- Assist the Commission and the Member States in their dialogue with industry to address security related problems in hardware and software products;
- Track the development of standards for security products and services and promote risk assessment activities;
- Contribute to Community efforts to cooperate with third countries and international organizations to promote a global common approach to security issues.