Intelligence Support to Emergency Management: A New Paradigm

Jon W. Glassford

Intelligence Support to Emergency Management: A New Paradigm

Abstract:

The Problem: the emergency management discipline does not have a paradigm or model for identifying information required for making decisions; effective techniques for collecting required information; techniques and standards of analyses for making sense of the required information; and standardized techniques for disseminating the resulting analyzed information to those who need it. This process of information identification, collection, analysis, and dissemination is commonly known as the intelligence cycle, and is a key element in many other professions. While most states have emergency operations and fusion centers that list intelligence fusion as one of their primary functions, in reality there is no apparent organized intelligence function at these levels (Steiner, 2009). The lack of an articulated intelligence functional paradigm may contribute to inaccurate and faulty response on the part of emergency management organizations and agencies (Soble & Leeson, 2007). The purpose of this paper is to discuss possible reasons for the lack of an information-processing and analysis model in the emergency management field, and suggests the adoption and modification of the U.S. Army's Intelligence Preparation of the Battlefield as a possible model.

Intelligence is highly charged term, and a lighting rod for controversy. There is a manifest distrust of government and intelligence agencies on the part of many Americans. Some of the reasons for the negative perspectives are based on past misuse and abuses of intelligence by the government. During the 1950's and 60's government military and law enforcement agencies collected information on U.S. citizens for a variety of reasons, mostly due to perceived external threats from the old Soviet Union, or attempting to counter perceived internal threats during the cultural crisis of the 1960's and 1970's. The U.S. Army provided counterintelligence support to the Federal Bureau of Investigation in tracking anti-war protesters (Odom, 2004), and both civilian and military intelligence agencies violated many Americans' civil liberties (Maxwell, 2004). There were many congressional inquiries, such as the Rockfeller Commission report on CIA activities in 1975, and the Church Committee report in 1976 (Maxwell). These violations of American constitutional rights led to the creation of a strict separation of intelligence needed to defend the U.S. from foreign enemies and threats, and intelligence used in law enforcement. This separation is often referred to as the "wall" (Stanton, 2009). Stanton believes the wall is so definitive concerning intelligence support to civil authorities and emergency management efforts that the "unity of effort" paradigm highlighted by homeland security plans and programs is not feasible.

In addition to the concern stemming from legal implications of intelligence support to emergency management, the entertainment media and press reinforced some of the negative perceptions concerning intelligence: that intelligence agencies have no qualms in trampling American rights. Americans get most of their ideas of intelligence from the movies, spy novels, and television. There are dozens of examples: movies such as Ian Fleming's *James Bond* series, Arnold Schwarzenegger in *True Lies,* and actor Matt Damon's the *Jason Bourne* series of

movies; TV shows such *I Spy*, *The Man From U.N.C.L.E.*, and today's *24*; there is the John Le Carre spy novel genre in particular. Most of these depictions focus on one aspect of intelligence, that is, human intelligence in the intelligence community's terms, and a relatively small portion of the overall intelligence community. The first modern novel to really paint a relatively realistic picture of military intelligence was Brigadier General Sir John Hackett's *The Third World War*, a novel concerning war between NATO and the Warsaw Pact written in 1978 (Hackett, 1982). It was followed by the creation of another literary genre, the military techno-thriller, perhaps best known by Tom Clancy's *The Hunt for Red October*, *Red Storm Rising*, and many others. While this genre did a better job of explaining intelligence, it was still focused on entertainment and fantasy. The public forms its ideas and opinions on intelligence from these outlets, however distorted and different from reality they may be.

There is a conspiracy theory community, who believe that the government cannot be trusted, and in fact has developed plans to round up “dissidents” and place them in special detention camps for re-education. According to this fringe element FEMA has set up a string of camps around the country (Keller, 2010). Despite the absurdity of some of these extremist views, they make the evening news, and FEMA is always concerned about controversy.

Academia also has a manifest mistrust of the intelligence community (Lowenthal, 2003). Many in the academic community are distrustful of the lack of openness that is inherent in the intelligence community. The intelligence professional and academic are polar opposites, in that the academic is interested in spreading information; the intelligence professional in collecting and refining it for a specific purpose.

The press has a less-than-accurate understanding of intelligence gathering, and often uses the terms spying and espionage as synonyms for intelligence (Dover & Goodman, 2009). These

mental frameworks are distortions of intelligence as a noun and as a focused and systematic effort to understand the dynamics of a problem or issue, which may be the reason why the emergency management community has not picked up on the function. After all, intelligence has become synonymous with failure to stop terrorists here and abroad. There is the popular "connect-the-dot metaphor." This refers to the apparent failure by the intelligence community in failing to link the many bits and pieces of information the law enforcement and intelligence communities had collected about the 9/11 terrorists. If these dots of information had been connected to each other, then a picture would have emerged that would have warned authorities about the impending attack, and law enforcement could have intervened to stop it. Finally, there is the faulty intelligence that led to the U.S. invasion of Iraq and the search for non-existent weapons of mass destruction. And last, but not least, we still haven't found Osama bin Laden.

Another reason for the emergency management community's lack of an intelligence capability is the U.S. Intelligence Community's (IC) focus on countering terrorism as their primary role in emergency management. This is a highly specialized as well as security conscious effort, and the IC is very reluctant to share or disseminate terrorism information to those not in the IC. Reasons for this reluctance range from protection of information sources to security clearance issues.

The common thread to the discussion of mistrust and suspicion of intelligence is the focus on the collection of information about *people*, whether they are domestic or international terrorists, spies, or others that pose a threat to national security. But this focus is just one part of the intelligence community, one aspect that ignores a larger intelligence focus and capability that matches the needs of the emergency management community. Using the iceberg metaphor, there is a tremendous amount of intelligence capability that goes well beyond interest in terrorist,

espionage, and surveillance. The Central Intelligence Agency (CIA) and the National Security Agency (NSA) are the central focus of the media and press. In reality, the majority of American intelligence capabilities are found in the military, and the military intelligence system is much more mundane and less glamorous. It is focused less on terrorism and individual threats, and more on areas such as terrain analysis, weather analysis, enemy or threat organizations, weapons, and tactics, transportation and logistics capabilities, and others. Planning for contingencies and alternate courses of action are essential functions of the military intelligence effort. The U.S. Army's battlefield intelligence model, Intelligence Preparation of the Battlefield, may be modified to serve as a unifying paradigm for local, state, and federal emergency management practitioners.

Emergency management is a comprehensive discipline that covers a myriad of activities. Key elements of effective emergency management involve planning and analysis, which is comprised of the sub-disciplines of mitigation, response, recovery, preparedness, and communications (Haddow, Bullock, & Coppola, 2006). Each of these sub-disciplines has different data and information requirements. Emergency management is also defined as a process of dealing with risk and risk avoidance (Haddow et al., 2006). In order to understand and deal with risk, one must have information concerning the risk. What information is required? Where does it come from? How is it acquired? How is it disseminated? To whom? Each discipline has specialized information needs. This cycle of identifying information requirements, collection, analysis, and dissemination is known as the Intelligence Cycle in the intelligence community. Intelligence is a recognized component of the business community and the law enforcement community. But it is difficult to find any references to emergency management intelligence and intelligence training in support of emergency management. Sobel and Leeson maintain,

"information acquisition and exploitation is a fundamental failure of government's disaster relief management" (Sobel & Leeson, 2007). It appears that there is no systematic effort to manage information within emergency management. This might be a curious development for most people, since many of the communities that support the field such as law enforcement and the military, have robust intelligence programs. As an insider of the U.S. military intelligence community, however, I can attest to the fact that it is a very closed community. This is partly due to the nature of classified information and the "need to know" restrictions regarding access to it, but also due to the fact that is small, somewhat elite, and by definition closed off, from the rest of the military functions. Only those working in operations centers and fusion cells have a good working knowledge of military intelligence. And as fusion cells are developed for the emergency management community, there needs to be some form of intelligence paradigm for it live up to its full capacity.

American emergency management has undergone significant changes since the events of 9/11 and the impact of Hurricane Katrina on the Gulf Coast. One of the results of this change has been the creation of local and state level fusions centers. A fusion center is defined as:

> … an effective and efficient mechanism to exchange information and intelligence, maximize resources, streamline operations, and improve the ability to fight crime and terrorism by merging data from a variety of sources. In addition, fusion centers are a conduit for implementing portions of the National Criminal Intelligence Sharing Plan (NCISP). (US Dept of Justice).

and:

> Fusion centers are the logical touch-points for the Department to access local information and expertise as well as provide them with timely, relevant information and intelligence derived from all-source analysis. The result is a new intelligence discipline and tradecraft that gives us a new, more complete understanding of the threat. The Department provides personnel and tools to the fusion centers to enable the National Fusion Center Network. (DHS Website).

Stanton discusses the creation and function of state fusion centers (Stanton, 2009). She states that fusion centers are an important element of the national government's effort to identify

and understand global threats, and to develop a unity of effort between the local, state and federal emergency management agencies in countering threats and emergencies. Yet she also notes that there really is no publicly available information on the type, nature, or degree of information or intelligence that is supposed to be shared between the national, state, and local fusion centers. Part of this lack of fusion between the fusion centers is due to the legal "wall" dividing domestic security and intelligence agencies and their responsibilities from those intelligence and security agencies responsible for countering terrorist and other threats from abroad as discussed above. Due to the nature of the security and classification of the intelligence on foreign threats, most of it cannot be passed on to local and state emergency management professionals who do not have the clearances or access to it. Indeed, Stanton's main thrust is that because of the legal wall between domestic security needs and the overseas threats, the goal of a national unity of effort is not possible. This "firewall" between the two groups prevents not only passing of information, but also hinders cross-training and passing on best practices. The efficacy of fusion centers is also questioned by Graphia, who points out that fusion centers have yet to develop effective analytical capabilities. (Graphia, 2010).

The Department of Homeland Security Office of Intelligence and Analysis lists five *analytic thrusts*: (1) threats related to border security, (2) threats of radicalization, (3) threats from particular groups entering the U.S., (4) threats to the Homeland's critical infrastructure and key resources, and (5) weapons of mass destruction and health threats. (DHS Office of Intelligence and Security). The focus of these five analytic thrusts is on people and groups: terrorists and radicals, enemies of the state if you will. What about the other threats facing the homeland? Threats that emergency management professionals must deal with every day include hurricanes, tornadoes, earthquakes, floods, and manmade disasters as well. Each of these threats

and others that cause a crisis or disaster (Mount St. Helens, springs to mind) require a considerable amount of information for effective emergency management. We go back to our initial questions: information for whom? About what?

Information is data that has been structured and manipulated to enhance its meaning (Schoech et al. 2002), and to answer questions. A cursory search through the index of most books on emergency management on library shelves reveals very few references to data (the building blocks of information and basic problem solving), information, intelligence, knowledge management, or decision-making. This appears to me as a significant weakness in emergency management theory and practice. With all of the information requirements one would think should form the foundation of risk and vulnerability assessments, modeling, and basic planning and problem solving, how can we not have whole chapters on information management and knowledge acquisition and development? Managers at all levels must make accurate and timely decisions; but on what information are these decisions based? A literature review of emergency management information requirements turns up very little scholarly research on the topic. Most of the research appears to focus on developing and implementing management information systems, which is the automation of data collection and retrieval (Zhang, Zhou, & Nunamaker Jr, 2002). Only when you change the search parameters to terrorism and counter-terrorism information requirements will you find references to intelligence. And even then, there is a lack of focus on the techniques of information identification, collection, analysis, and dissemination. There are a considerable number of references to dot-connecting, that is, the failure of the intelligence community to connect the dots tying the terrorists of 9/11 together (Anderson, 2004). But exactly how do you accomplish this task? What analytical techniques are available to the

emergency management community to help practitioners conduct risk assessments, and the functions of mitigation, preparedness, response and recovery?

One of the problems we face today is the incredible amount of data and information available. In this day and age of information overload, what Richard S. Wurman refers to as "information anxiety," (Wurman, Leifer, Sume, & Whitehouse, 2001) the ability to collect data and information far outstrips our ability to make sense of it. The amount of data (scattered bits and pieces of facts), and information (semi-structured data) can be overwhelming. Norman states that we are in an era of information explosion, that there is too much information for anyone to assimilate, and much of it is of doubtful quality (Norman, 1993). He goes on to say we tend to collect statistics about those things that are easiest to count or measure, which may not have any connection with what is really important. I believe the emergency management community needs to develop a methodology to manage this flood of data and information.

So what is intelligence? There are many definitions. Intelligence is the capacity to make sense, and take action (Schoech, Fitch, MacFadden and Schkade, 2002). The simplest description is that intelligence is information collected from specific sources and analyzed to answer specific questions by decision-makers. There is a hierarchy of information, beginning with data. For this discussion data is defined as sets of discrete, objective facts. Information is data that has been contexualized (a purpose for which the data was collected), categorized (units of analysis are known), calculated (analyzed mathematically or statistically), corrected (errors removed), and condensed (summarized in a concise form) (Davenport & Prusak, 1998). Data mining is a task that involves sifting through volumes of current and historical data to extract relationships, patterns, sequences, classifications, predictions, and trends that enhance the value of data for workers and stakeholders. The data mining process involves six phases: (1) problem

conceptualization; (2) data collection, selection, storage, and retrieval; (3) data preparation; (4) data modeling; (5) data analysis, model understanding, and model validation; and (6) information visualization and dissemination (Schoech, Quinn, and Rycraft, 2000).

Even with this degree of processing, information is still fragmented, and often contained in inarticulate forms (Sobel & Leeson, 2007), and has not yet attained the level of knowledge or intelligence. Intelligence is the "product resulting from the collection, processing, integration, analysis, evaluation and interpretation of available information concerning foreign countries or areas." (Richelson, 1999). U.S. Army Field Manual 2.0 describes intelligence as:

> … the product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations

As stated previously, there are a great many misconceptions about intelligence, ranging from confusion with intelligence as mental capacity (if I had a dime for every time I've heard the old joke about the oxymoron, Military Intelligence) to intelligence as spying. However, the purpose of military intelligence is:

> … to provide commanders and staffs with timely, relevant, accurate, predictive, and tailored intelligence about the enemy and other aspects of the AO. Intelligence supports the planning, preparing, execution, and assessment of operations. The most important role of intelligence is to drive operations by supporting the commander's decisionmaking. (FM 2.0, Intelligence, 2010).

In other word, intelligence is nothing more than conversion of data into information that is collected, analyzed, and disseminated in order to support planning, preparation, and execution of operations. There is no mention of espionage or spying. Intelligence is focused collection of information provided to those who need it to make effective decisions.

Just as emergency management is comprised of sub-disciplines, military intelligence is broken down into intelligence sub-disciplines:

- Signals Intelligence, or SIGINT: Information developed from the interception of communications, such as radios and telephone
- Human Intelligence, or HUMINT: Information derived from people through informant networks, interrogations, debriefings, and elicitation
- Imagery Intelligence, or IMINT: Information derived from imagery, such as satellites and high-altitude aircraft
- Measurement and Signature Intelligence, or MASINT: Information gained from intercepting telemetry and other forms of sensor equipment
- GeoSpatial Intelligence: exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the Earth
- All-Source Intelligence: intelligence products and/or organizations and activities that incorporate all sources of information, most frequently including human resources intelligence, imagery intelligence, measurement and signature intelligence, signals intelligence, and open-source data in the production of finished intelligence
- Open-Source Intelligence: derived from the systematic collection, processing, and analysis of publicly available, relevant information in response to intelligence requirements
- Counterintelligence, responsible for identifying threats from foreign intelligence agents and countering or neutralizing it. (FM 2.0, Intelligence, 2010)

Each of these disciplines have associated career fields. For example, in the discipline of SIGINT there are Voice Interceptors, whose job is to intercept radio conversations of foreign military and government personnel. Imagery Analysts analyze aerial and satellite photos and

images to discern locations of enemy personnel, equipment, and activities. Human Intelligence specialists are Interrogators, Case Officers, and Debriefers. They are the specialists most closely aligned with espionage and spying as depicted in the media and the press, because they provide information from human sources (they also comprise the smallest number with the intelligence disciplines). There are Intelligence Analysts, whose function is to integrate the information and intelligence coming from the specialists to a headquarters, operations center, or task force fusion centers, and determine how all of the information relates to each other, check for relevancy, and produce a variety of intelligence products in the form of reports and various analyses. The information is developed as part of the paradigm known as Intelligence Preparation of the Battlefield, or IPB.

It is possible to make a comparison between the intelligence disciplines of the American intelligence community noted above and emergency management. The Department of Homeland Security has identified 18 Critical Infrastructure Sectors. Below is a partial list (Steiner, 2010):

- Agriculture and Food
- Banking and Finance
- Critical Manufacturing
- Dams
- Energy
- Information Technology
- Public Health and Health Care
- Telecommunications
- Transportation Systems

Each of these sectors could have an emergency management intelligence specialty similar to military intelligence specialties. They would be experts in their field or discipline, providing information and intelligence to a local, state or federal fusion cell or emergency operations center.

One of the key tasks of emergency management is to reduce risk and uncertainty concerning a wide variety of disasters and crises. Risk is the possibility of an incident that can cause harm to people or property that has some known likelihood of happening over a period of time. (Comfort, 1988). The nature of risks is becoming more complicated and dynamic, and standard methods of analysis based on known data fail. And more data and information can actually increase uncertainty and doubt. According to Taleb, "… additional knowledge of the minutiae of daily business can be useless, even actually toxic…" (Taleb, 2007). Taleb posits that the information you give someone, the more hypotheses they will make, and quite possible mistake random noise for information. They become overwhelmed with data and information, what Wurman refers to as *infosmog*. (Wurman et al., 2001).

Comfort lists four approaches emergency management could use in reducing risk and uncertainty: After Action Reviews, Recognition-Primed Decision Making, The Edge of Chaos, and the "Bowtie Model" for an emergency operations center (L. K. Comfort, 2005):

Information from the agencies on the left side of the model goes into the box for processing, and is disseminated to the entities and organizations to the right side of the box for utilization. This model is designed to support learning, update strategies, and adapt to an event more effectively. The model represents how data are integrated, analyzed, and interpreted. This model is strikingly similar to the U.S. Army's Intelligence Cycle model (Field Manual 34-1, 1994), as depicted below:

The intelligence cycle model had been around for many years, and is the foundation of military intelligence. Supervisors determine intelligence requirements; specialists in the field collect

information from their sources; the information is processed and analyzed for meaning, relevance, and validity, and turned into intelligence; the intelligence product (report or briefing) is the disseminated to decision-makers, and the cycle continues for new information, or looking for changes in current intelligence. All of the information that is collected and converted into intelligence is used to accomplish the mission of the organization. If it does not, then it is filed for possible future requirements.

The Army has a well-developed intelligence community of knowledge, including formal military intelligence training for officers and enlisted at all ranks and levels of command. It has a well-established body of knowledge in the form of Military Intelligence Field Manuals (FMs), such as FM 2-0, Intelligence, FM 2-22, Counterintelligence, FM 34-3, Intelligence Analysis, FM 5-33, Terrain Analysis, FM 34-81, Battlefield Weather Effects, FM 2-01, Intelligence Preparation of the Battlefield, and many others. These intelligence manuals are usually unclassified and available to anyone, while others are more sensitive and may reveal military capabilities and techniques the Army doesn't want revealed. The processes and techniques embodied in these manuals can be applied to the emergency management effort.

IPB is a model that bridges the gap between Army Intelligence and the other branches or functions of the Army. IPB was designed to answer the questions of the field commanders and battle captains, to focus only on essential information critical to winning battles, and not trying to know everything occurring on the battlefield. IPB was also designed to use scarce intelligence resources wisely and efficiently. IPB focused not only on the intelligence community, it also took into consideration the format and method of intelligence that best suited the commanders, not the collectors and analysts. It also revised the way commanders conducted planning, so that strategy and tactics were combined with current knowledge of the situation. Finally, IPB created a

common language between the Army's intelligence analysts and its battle captains, a language based on the metaphor of the Situation Map, rich in symbology and easily understood by all military leaders.

The following is a brief description of IPB functions:

- Battlefield Area Evaluation--This evaluation involves assessing the battle area with regard to the overall nature of the friendly and enemy forces and the operating environment. The evaluation involves a general analysis of the weather and terrain of the anticipated battlefield, but leaves the more detailed analysis for later. In essence, this step "sets the stage" for the conflict.
- Terrain Analysis-- The terrain will dictate the method of attack and defense, as well as the type and kind of troops and equipment required. Tanks cannot operate in swamps, flooded areas, or in mountainous area. Airborne troops cannot be dropped in mountainous terrain. Desert sand and dust can clog vehicle filters, as well as provide wide-open fields of fire, or, conversely, provide little or no cover and concealment from enemy fire or

observation. Urban areas offer good cover from fire, but take a greater amount of time to fight through, as well as offer problems with refugees, blocked roads, snipers, etc.

- Weather Analysis-- Weather plays a crucial role in modern warfare. Rain, heat, cold, all contribute significantly to success or failure of military operations. The amount of cloud cover on a given night affects the range of night vision devices; heat and cold affects the operation of equipment as well as the health and capabilities of personnel. Rain can lead to flooding of key terrain, the trafficability of roads, etc. All of the effects of weather must be considered in the planning of any level of battle or campaign.
- Threat Evaluation-- Who and what is the enemy? Are we facing guerrillas or insurgents, or are facing modern mechanized forces? What are their capacities to wage and sustain war? What is the industrial base? What is their level of training? What kind and amount of equipment do they have, and will they use all weapons they have available to them?
- Threat Integration-- Finally, given the effects of the terrain, weather, and threat capabilities, how will the enemy react in given situations or scenarios? What are the Threat's most likely courses of action? What are their most dangerous courses of action? During this stage of IPB, a variety of scenarios are developed that are used to literally "war game" different options or approaches of both enemy and friendly forces. Templates are developed that take into account all of the above factors, as well as how the enemy actually conducts battle, then, how all of these factors will influence the battle. These templates are based on a combination of enemy doctrine and realistic evaluations of terrain, weather, and other factors. Significantly, they are based on the art and science of war. At this point the intelligence officer can develop threat indicators, those signs and clues of where, how, when, and why the threat will strike. He will establish his

reconnaissance and surveillance assets to look for these indicators, and once detected, provide the commander with early warning and time to set counter-strikes or other military options.

- Time. The last, crucial element in IPB is time. IPB adds the dimension of time in the development of templates. An estimated time frame is given for each enemy move. This allows friendly forces to develop timelines for gathering their own forces in time to effectively counter enemy moves at the time and place of their choosing.

IPB and Emergency Management

If we redefine the elements of IPB with terms more compatible with emergency management, the utility of the model begins to emerge. Battlefield Area Evaluation can be renamed as Regional Analysis. This can be used by local, state and federal analysts to describe the particular area or region under analysis: the Gulf Coast and hurricanes, or flood plains along the Mississippi, earthquake zones in California. What is the nature of the region? How many people live there? What are the critical infrastructure concerns? What businesses or critical industries exist in the region? Haddow et al discuss the need to conduct social and economic risk factors:

- Education
- Culture
- Health and welfare
- Local government
- Values, laws, and beliefs

Analysis of these factors would be conducted in the Regional Analysis phase.

Terrain Analysis. What is the nature of the terrain? Flat, hilly, swampy, mountainous, and desert? How does the terrain affect the people and society? How have they adapted to it? What aspects of the terrain would intensify or mitigate man-made or natural disasters and crises? As an

example, southern Florida has a limited transportation system for mass evacuations in the event of a hurricane. People are channled onto only a few interstate highways. What would the impact be of the loss of key bridges during the evacuation? The road networks into and out of New Orleans were compromised during Hurricane Katrina due to wind and the flood surge, forcing a premature halt to evacuation of the citizenry.

Weather Analysis. How does the weather affect disasters of a given region? Besides the known risk of tornadoes, floods, blizzards, and hurricanes, what would be the effect of heat or cold on a chemical or nuclear plant disaster? What are the wind patterns for a given time of year, and how would they disperse toxic fumes, chemicals, or radiation? Or the use of chemical or biological agents?

Threat Evaluation. Threats can be natural as well as man-made. In evaluating threat, we need to consider the most likely course of action of a threat, the least likely course of action, and the most dangerous course of action. The analysis of threats and their courses of action can be developed as a standard template, but would have to be adjusted to meet current conditions and situations. We develop plans for coping with disasters, but every disaster is unique to the time and circumstances.

Threat Integration. Threat integration is the process that brings together Regional Analysis, Terrain, Weather, and Threat Analysis to develop a clear picture of the possible threat courses of action, their impact on the region or community, the identification of indicators of the threat courses of action, with a concomitant reconnaissance and surveillance system to predict when, where, and how the threat will strike.

Instead of Intelligence Preparation of the Battlefield, we now have Intelligence Preparation of the Homeland.

Even if intelligence tailored for emergency management was provided to practitioners, there are still barriers to using it effectively. Intelligence is knowledge, and knowledge is often seen as a source of power and influence. The discussion above highlights the many misperceptions of intelligence that exist not only among the American public, but also among those who should have a better grasp of the field and its capabilities. How can one expect emergency management specialists to be cognizant of the benefit of intelligence if their perception or knowledge is based on these distortions and misperceptions? They don't know that they don't know. They have little or no experience in the intelligence community, and so cannot adopt many of the practices.

Organizations and agencies that vie for scarce emergency management funding may be reluctant to share knowledge (intelligence) in the belief that it would give them a competitive funding edge over other agencies. There are legitimate reasons for not disseminating intelligence, especially if its release might jeopardize the source of the information, and hence dry it up. There are other barriers to effectively sharing intelligence, such as a lack of common standards and practices, divided management, and the inherent complexity and secrecy of intelligence (Maxwell, 2004, p. 464-465). Training is an issue. People have to be taught how to recognize intelligence, how to use it, and how to share it, and how to report or disseminate to those who need it in a manner they can use. Intelligence analysts have to have well-developed critical thinking skills (Moore, 2007). But this last barrier is something that could be easily addressed through training and practical applications. It should not be difficult to arrange U.S. Army military intelligence trainers to conduct specialized training for emergency management personnel in basic intelligence collection, analysis, reporting and disseminating intelligence, and other topics.

In summary, the emergency management community lacks a methodology for the identification, collection, analysis, and dissemination of information and intelligence. While information systems have been developed that can store and retrieve vast amounts of data and information, that capability does not provide the focused information and analysis that creates the required intelligence. The reasons for the lack of a working emergency management intelligence system include an incorrect focus by the national intelligence and security agencies on terrorism as the primary threat vice a more practical concern with other forms of man-made and natural threats; and the misperception by Americans, to include professionals from all walks of life, on the complete U.S. intelligence community capabilities and methodologies. The armed forces intelligence community, specifically the U.S. Army military intelligence community, has a rich body of knowledge and practice that can be adapted to meet the information and intelligence needs of emergency management.

Sources

Alexander, D. (2002). *Principles of emergency planning and management*. New York: Oxford University Press.

http://books.google.com/books?id=iLqMSDgecHQC&printsec=frontcoverAnderson, T. (2004). Homeland security-from small clues to big picture. *Security management. 48*(6), 52.

Andrienko, N., & Andrienko, G. (2007). A Framework for Decision-Centred Visualisation in Civil Crisis Management. In *Location Based Services and TeleCartography*, Lecture Notes in Geoinformation and Cartography (pp. 461-477). Springer Berlin Heidelberg. Retrieved from http://dx.doi.org/10.1007/978-3-540-36728-4_33

Bazerman, M. H., & Watkins, M. (2004). *Predictable surprises: the disasters you should have seen coming, and how to prevent them*. Leadership for the common good. Boston: Harvard Business School Press.

Burstein, F., Holsapple, C., Walle, B., & Turoff, M. (2008). Decision Support for Emergency Situations. In *Handbook on Decision Support Systems 2*, International Handbooks on Information Systems (pp. 39-63). Springer Berlin Heidelberg. Retrieved from http://dx.doi.org/10.1007/978-3-540-48716-6_3

Comfort, L. K. (2005). Risk, Security, and Disaster Management. *Annual review of political science. 8*, 335-356.

Comfort, L. K. (1988). *Managing disaster: strategies and policy perspectives*. Duke Press policy studies. Durham: Duke University Press.

Copeland, T. E. (2007). *Fool me twice: intelligence failure and mass casualty terrorism*. Boston: Martinus Nijhoff.

Daton, D., & , R. (n.d.). Emerald | Disaster Prevention and Management | Disaster stress: an emergency management perspective. Retrieved September 9, 2010, from http://www.emeraldinsight.com/journals.htm?articleid=870958&show=html

Davenport, T. H., & Prusak, L. (1998). *Working knowledge: how organizations manage what they know*. Boston, Mass: Harvard Business School Press.

Department of Homeland Security | Office of Intelligence and Analysis. (n.d.). Retrieved September 25, 2010, from http://www.dhs.gov/xabout/structure/gc_1220886590914.shtm

Department Of The Army Washington DC. (1994). Intelligence and Electronic Warfare Operations. Retrieved from http://handle.dtic.mil/100.2/ADA394229

Dover, R., & Goodman, M. S. (2009). *Spinning intelligence: why intelligence needs the media, why the media needs intelligence*. New York: Columbia University Press.

Fusion Centers and Intelligence Sharing. (n.d.). Retrieved September 25, 2010, from http://www.it.ojp.gov/default.aspx?area=nationalInitiatives&page=1181

GI Science, Disasters, and Emergency Management .pdf. (n.d.). Intelligence and Security Informatics for Homeland Security Information Communication Transportation.pdf. (n.d.).

Fuld, L. M. (1985). *Competitor intelligence: how to get it, how to use it*. New York: Wiley.

Fuld, L. M. (1995). *The new competitor intelligence: the complete resource for finding, analyzing, and using information about your competitors*. New York: J. Wiley.

Graphia, R. D. (2010). An exploratory study of the perceived utility and effectiveness of state fusion centers. Retrieved from http://hdl.rutgers.edu/1782.2/rucore10002600001.ETD.000052951

Hackett, J. W. (1982). *The Third World War: the untold story*. New York: Macmillan.

Haddow, G. D., Bullock, J. A., & Coppola, D. P. (2006). *Introduction to emergency management*. Butterworth-Heinemann homeland security series. Boston: Elsevier/Butterworth-Heinemann.

Hernandez, J. Z., & Serrano, J. M. (2001). Knowledge-based models for emergency management systems. *Expert Systems with Applications*, *20*(2), 173-186. DOI: 10.1016/S0957-4174(00)00057-9

Keller, L. Fear of FEMA | Southern Poverty Law Center. (n.d.). Retrieved September 25, 2010, from http://www.splcenter.org/get-informed/intelligence-report/browse-all-issues/2010/spring/fear-of-fema

Khalsa, S. K. (2005). Forecasting Terrorism: Indicators and Proven Analytic Techniques. In *Intelligence and Security Informatics*, Lecture Notes in Computer Science (Vol. 3495, pp. 561-566). Springer Berlin / Heidelberg. Retrieved from http://dx.doi.org/10.1007/11427995_59

Norman, D. A. (1993). *Things that make us smart: defending human attributes in the age of the machine*. Reading, Mass.: Addison-Wesley Pub. Co.

Odom, W. E. (2004). *Fixing intelligence: for a more secure America*. Yale University Press.

Perry, R. W., & Lindell, M. K. (2003). Preparedness for Emergency Response: Guidelines for the Emergency Planning Process. *Disasters*, *27*(4), 336-350. Retrieved from http://dx.doi.org/10.1111/j.0361-3666.2003.00237.x

Richelson, J. (2008). *The US intelligence community*. Boulder, Colo.: Westview Press.

Schaafstal, A. M., Johnston, J. H., & Oser, R. L.Training teams for emergency management. *Computers in Human Behavior*, *17*(5-6), 615-626. DOI: 10.1016/S0747-5632(01)00026-7

Scheps, S. (2008). *Business intelligence for dummies*. Hoboken, NJ: Wiley.

Sobel, R. S., & Leeson, P. T. (2007). The Use of Knowledge in Natural-Disaster Relief Management. *Independent Review -Oakland-*, *11*(4), 519-532.

Stanton, L. (2009). *The Civilian-Military Divide: Obstacles to the Integration of Intelligence in the United States*. ABC-CLIO.

Steiner, J. (2010, September 25). Improving Homeland Security at the State Level — Central Intelligence Agency. Retrieved September 3, 2010, from https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol.-53-no.-3/improving-homeland-security-at-the-state-level.html

Otis, P. (2003). The intelligence pro and the professor: toward an alchemy of applied arts and sciences. In Swenson, R. G., & Center for Strategic Intelligence Research (U.S.). *Bringing intelligence about: practitioners reflect on best practices*. Washington, D.C.: Joint Military Intelligence College, Center for Strategic Intelligence Research.

Steiner, J. (2010, September 25). Improving Homeland Security at the State Level — Central Intelligence Agency. Retrieved September 3, 2010, from https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol.-53-no.-3/improving-homeland-security-at-the-state-level.html

Taleb, N. (2007). *The black swan: the impact of the highly improbable*. New York: Random House.

Turoff, M., Chumer, M., Hiltz, S. R., Hendela, A., Konopka, J., & Yao, X. (2006). Gaming Emergency Preparedness. In *Proceedings of the 39th Annual Hawaii International*

Conference on System Sciences - Volume 02 (p. 38). IEEE Computer Society. Retrieved from http://portal.acm.org/citation.cfm?id=1109515#

United States. Dept. of the Army. (1983). *IPB: intelligence preparation of the battlefield.* Washington, D.C.: Dept. of the Army.

United States. Dept. of the Army. (1992). *Collection management.* Washington, D.C.: Headquarters, Dept. of the Army: G.P.O.

United States. Dept. of the Army. United States Army Intelligence Center & School. (1980). *Intelligence analyst*. Washington: Dept. of the Army.

Wilmeth, J. L. (2004). *US Military Support to Homeland Security* [Monograph]. School of Advanced Military Studies, Fort Leavenworth, KS.

Waugh, W. L. (2003). Terrorism, Homeland Security and the National Emergency Management Network. *Public Organization Review, 3*(4), 373-385. Retrieved from http://dx.doi.org/10.1023/B:PORJ.0000004815.29497.e5

Wurman, R. S. (1989). *Information anxiety*. New York: Doubleday.

Wurman, R. S., Leifer, L., Sume, D., & Whitehouse, K. (2001). *Information anxiety 2*. Indianapolis, Ind.: Que.

Wybo, J. L., & Kowalski, K. M.Command centers and emergency management support. *Safety Science, 30*(1-2), 131-138. doi:doi: DOI: 10.1016/S0925-7535(98)00041-1

Zhang, D., Zhou, L., & Nunamaker Jr, J. F. (2002). a knowledge management framework for the support of decision making in humanitarian assistance/disaster relief. *Knowledge and Information Systems*, *4*(3), 370-385. Retrieved from http://dx.doi.org/10.1007/s101150200012