NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

IMPROVING THE ALL-HAZARDS HOMELAND SECURITY ENTERPRISE THROUGH THE USE OF AN EMERGENCY MANAGEMENT INTELLIGENCE MODEL

by

William N. Schulz

September 2013

Thesis Advisor: Erik Dahl
Second Reader: Christopher Bellavita

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE		Form Approved OMB No. 0704–0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE September 2013	3. REPORT TYPE AND DATES COVERED Master's Thesis

4. TITLE AND SUBTITLE IMPROVING THE ALL-HAZARDS HOMELAND SECURITY ENTERPRISE THROUGH THE USE OF AN EMERGENCY MANAGEMENT INTELLIGENCE MODEL	5. FUNDING NUMBERS
6. AUTHOR(S) William N. Schulz	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943–5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited	12b. DISTRIBUTION CODE A

13. ABSTRACT (maximum 200 words)

As the all-hazards approach takes hold in our national Emergency Management and Homeland Security efforts and continues to seek greater collaboration between these two fields, an area that has yet to be explored to its fullest extent is the utilization of an intelligence process to enhance EM operations. Despite the existence of multiple Federal-level policies that outline the importance of intelligence and information sharing across the all-hazards community, EM is still by-and-large an outsider to the Intelligence Community (IC); the problem is one of both policy and of practice. Formalizing both an intelligence process and EM role culled from best practices of the FBI, U.S. Military, and local law enforcement, and subsequently equipping and training emergency managers in the use of intelligence would be substantially beneficial in all phases of a disaster. Once established, an intelligence process could also help EM augment and integrate into the IC to provide more robust HS capabilities, including a significant role in the State/Local Fusion Centers. This formalized EM Intelligence Cycle (EMIC) lays the groundwork for better EM-IC collaboration, better support to first responders during large-scale events, a more proactive role in preventing future disasters, and a more robust all-hazards community as a whole.

14. SUBJECT TERMS Emergency Management, Intelligence, Intelligence Cycle, All-hazards, Intelligence Preparation of the Battlespace, Intelligence-Led Policing, Natural Disasters, State/Local Fusion Centers	15. NUMBER OF PAGES 105
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UU

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

IMPROVING THE ALL-HAZARDS HOMELAND SECURITY ENTERPRISE THROUGH THE USE OF AN EMERGENCY MANAGEMENT INTELLIGENCE MODEL

William N. Schulz
Assistant Director, Recovery
Arizona Division of Emergency Management
B.S., California Polytechnic State University, San Luis Obispo, 1998
M.A., Azusa Pacific University, 2005

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND DEFENSE AND SECURITY)**

from the

**NAVAL POSTGRADUATE SCHOOL
September 2013**

Author: William N. Schulz

Approved by: Erik Dahl, PhD
Thesis Advisor

Christopher Bellavita, PhD
Second Reader

Mohammed M. Hafez, PhD
Chair, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

As the all-hazards approach takes hold in our national Emergency Management and Homeland Security efforts and continues to seek greater collaboration between these two fields, an area that has yet to be explored to its fullest extent is the utilization of an intelligence process to enhance EM operations. Despite the existence of multiple Federal-level policies that outline the importance of intelligence and information sharing across the all-hazards community, EM is still by-and-large an outsider to the Intelligence Community (IC); the problem is one of both policy and of practice. Formalizing both an intelligence process and EM role culled from best practices of the FBI, U.S. Military, and local law enforcement, and subsequently equipping and training emergency managers in the use of intelligence would be substantially beneficial in all phases of a disaster. Once established, an intelligence process could also help EM augment and integrate into the IC to provide more robust HS capabilities, including a significant role in the State/Local Fusion Centers. This formalized EM Intelligence Cycle (EMIC) lays the groundwork for better EM-IC collaboration, better support to first responders during large-scale events, a more proactive role in preventing future disasters, and a more robust all-hazards community as a whole.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ACAMS	Automated Critical Asset Management System
AO	Area of Operations
CI/KR	Critical Infrastructure/Key Resources
CIP	Critical Infrastructure Protection
COA	Courses of Action
DHS	Department of Homeland Security
DHSI	Department of Homeland Security Intelligence Enterprise
DOJ	Department of Justice
DRF	Disaster Relief Fund
EOC	Emergency Operations Center
EM	Emergency Management
EMIC	Emergency Management Intelligence Cycle
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
GEOINT	Geospatial Intelligence
GIS	Geographic Information Systems
HITRAC	Homeland Infrastructure Threat & Risk Analysis Center
HS	Homeland Security
HSE	Homeland Security Enterprise
HSPD	Homeland Security Presidential Directive
HUMINT	Human Intelligence
I & A	DHS's Office of Intelligence and Analysis
IC	Intelligence Community
ILP	Intelligence-Led Policing
IMINT	Imagery Intelligence
IPB	Intelligence Preparation of the Battlespace
ITACG	Interagency Threat Assessment & Coordination Group
MASINT	Measurement and Signature Intelligence
NIPP	National Infrastructure Protection Plan
NPG	National Preparedness Goal

NPR	National Preparedness Report
NSS	National Security Strategy
OCOKA	Observation and fields of fire, Concealment and cover, Obstacles, Key terrain, and Avenues of approach
ODNI	Office of the Director of National Intelligence
OIG	Office of the Inspector General
OSINT	Open Source Intelligence
PPD	Presidential Policy Directive
SIGINT	Signals Intelligence
SLFC	State/Local Fusion Center
USACE	United States Army Corps of Engineers

EXECUTIVE SUMMARY

As the all-hazards approach takes hold in our national Emergency Management and Homeland Security efforts and continues to seek greater collaboration between these two fields, an area that has yet to be explored to its fullest extent is the utilization of an intelligence process to enhance EM operations. Despite the existence of multiple Federal-level policies that outline the importance of intelligence and information sharing across the all-hazards community, EM is still by-and-large an outsider to the Intelligence Community (IC). The problem is one of both policy and of practice; despite the existence of some federal policies, not enough has been explored or fleshed out, and what has been fleshed out is not implemented on any sort of national scale.

Key among these deficiencies is the collection and use of intelligence by the EM community; no formalized method for supporting or utilizing this capability within the EM community currently exists. The lack of familiarity with this overarching and powerful national capability creates a disconnect within the all-hazards community and thereby inhibits collaboration, resource efficiency, and a proactive national posture, concepts vital to the success of the all-hazards approach. Could a refined and well-developed method for intelligence gathering and synthesis within the EM community help strengthen current operations, as well as foster better collaboration with the broader Homeland Security Enterprise (HSE)? Is there a benefit to pushing for EM inclusion into the larger IC, and how best could the EM community support this all-hazards approach to ensure the benefit was mutual to both communities? This thesis addresses these questions, and explores the benefits a formalized intelligence process could have for the EM field, as well as the benefits it brings the all-hazards community as a whole.

By definition, the intelligence process does not necessitate criminal activity; rather, it is simply a well-defined method of information gathering and subsequent analysis. As such, EM intelligence could support a more robust decision-making process within the EM community and the HS community at large. In many ways, the EM field already has a role (albeit a support role) in response operations to all-hazards events, including terrorism, and thus has a vital role in this information gathering/analysis

process. Formalizing this role and subsequently equipping and training emergency managers could be of substantial benefit to jurisdictions in all phases of a disaster. Real world examples of how an EM intelligence process was, or could have been, utilized to bolster EM's current capabilities within each of FEMA's five mission areas further illustrates the potential benefits of a more formal intelligence process.

In order to most effectively develop this intelligence process model and test the hypotheses, the research is two-tiered. The first step is to evaluate key portions of the intelligence processes from various members of the IC through case studies to glean relevant elements and procedures. These best practices come from the military (intelligence preparation of the battlespace), the current U.S. IC (domestically represented by the Federal Bureau of Investigation), and processes currently used by local jurisdictions (intelligence-led policing). These processes have an abundance of open source material available, and there are some clear similarities between the different members of the IC and their methods of analysis, synthesis, and delivery. Through extracting these concepts from those sources, I establish a working model of an intelligence process for EM, including steps, a flow diagram, and other key guiding principles that appear to be essential for success. With key causal factors identified and confirmed, a model developed from the aforementioned principles from the IC is then translated to the EM community.

The ideal end result is a model that is scalable, functional, easily implemented, and utilized by any level of government. Through this formalized model, the Emergency Management Intelligence Cycle, the groundwork is laid for better support to first responders during large-scale events, a more proactive role in preventing future disasters, and a more robust all-hazards community as a whole. The EMIC also fosters better collaboration with and integration into the IC through the State/Local Fusion Centers and give each state a more comprehensive HS/EM community, able to prepare for, respond to, and recover from disasters of all shapes and sizes.

The thesis concludes with a series of four recommendations that take the EMIC from conceptual stages to full implementation. The recommendations include consideration of cost, personnel, and resources essential to carry this project through to

completion. With the EMIC in place, the all-hazards approach gains a valuable asset towards the goals of greater inter-disciplinary collaboration, maximizing resource efficiency, and a more proactive posture towards incidents that threaten our national safety and security.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

A heartfelt thank you to all who have made this experience possible:

To my wonderful wife, Alison, and epic children, Elijah and Katie–thank you for "loaning" me to Monterey and for the sacrifices you've made to afford me this opportunity; this adventure would never have been possible without your patience and understanding. I love you all.

To my family, Mom, Dad, Jennifer, Phil & Deb, Pat, Uncle Jack, Aunt Jerry, Uncle Carl, Buzz and Ann–thank you for encouraging me to take this challenge on and cheering for me every step of the way; your support has kept me moving forward when the road was difficult.

To my fellow cohort members–thank you for challenging me, putting me in check when I needed it, and inspiring me through your experiences and wisdom; I am eager to see what good things our futures hold.

To my Thesis Advisor, Erik Dahl, and Reader, Chris Bellavita–thank you for your time and insights in shaping this project; this thesis is the result of you both pushing me to think more critically and intelligently.

To the CHDS faculty and Alum (especially Anthony Cox, Jerry Monier, Greg Brunelle, and William Wickers)–thank you for broadening my limited perspective and being a sounding board for ideas; this thesis represents a collaboration and culmination of but a portion of our discussions.

To my agency, the Arizona Division of Emergency Management (ADEM) and Director Wendy Smith-Reeve–thank you for granting me this opportunity and writing my letter of recommendation; your willingness to develop people and not positions makes it a great place to work and I appreciate your leadership over the years.

And finally, to the Recovery Section at ADEM, past and present–thank you for holding down the fort while I was gone; we may play hard, but when it comes to crunch time, you all rise to the challenge and keep the Recovery world spinning.

I. INTRODUCTION

The field of homeland security (HS) as we know it is much like any other field of study offered by institutions of higher learning: it reflects an evolution of theory and research that is as varied as the incidents we encounter. In the crucible of several large-scale terrorist events and natural disasters, our modern homeland security enterprise (HSE) has emerged from the Civil Defense days with a more comprehensive and standardized approach to disaster and incident management.

One of the more recent and profound shifts in the field within the last decade is a blurring of the line between the traditional areas of responsibility of both HS (man-made/terrorist events) and emergency management (natural disasters). This approach, dubbed "all-hazards" by both government and practitioners, seeks to capitalize on similarities in both preparedness and response to both types of incidents, and thereby reduce inefficiencies and redundancies in the use of resources and personnel. The Incident Command System is a good example of this; it is used in field operations by the military, police, and fire teams, and emergency managers have adopted the system for use in governing their Emergency Operations Centers during "all-hazards" incidents.[1]

The subsequent rhetoric and proliferation of this all-hazards concept throughout federal policy has been substantial; the approach is now a staple in emergency management (EM) and responder communities throughout the nation. However, the implementation has not been without significant challenges. Cultural barriers, varying degrees of reluctance and resistance to change, and stove pipes of resources and responsibilities all slow the pace of innovation and collaboration. There is also a glaring deficiency in capabilities between the different disciplines being melded together under the all-hazards umbrella, as the traditional roles that have dictated the use of a certain set of "tools" and skills necessary to conduct operations now overlap. Among these deficiencies is the collection and use of intelligence, as the EM community in particular has no formalized method for supporting or utilizing this capability. The lack of

[1] Federal Emergency Management Agency, "Intelligence/Investigations Function Guidance Document" Version 3 (Draft), February 2008, 2.

familiarity with this overarching capability creates a disconnect within the all-hazards community and thereby inhibits collaboration, a concept vital to the success of this approach. With this is mind, this thesis will attempt to explore the benefits an intelligence process could have for the EM field, as well as the benefits it brings the all-hazards community as a whole.

A. BACKGROUND

The all-hazards approach was first introduced on a National Policy level with the release of Homeland Security Presidential Directive 8 (HSPD) in 2003.[2] However, it remained largely conceptual until it gained structure with 2011's Presidential Policy Directive 8 (PPD-8), which heavily emphasized the preparedness phase of disaster management, and issued the edict for the development of the National Preparedness Goal (NPG) and National Preparedness System. It also emphasized collaboration towards all-hazards proficiency: "while this directive is intended to galvanize action by the Federal Government, it is also aimed at facilitating an integrated, all-of-Nation, capabilities-based approach to preparedness."[3] PPD-8 also decreed that the Federal Department of Homeland Security (DHS) would begin work on five frameworks, one for each mission area of disaster management (Prevention, Protection, Mitigation, Response, and Recovery), and were to be coordinated under "a unified system with a common terminology and approach, built around basic plans that support the 'all-hazards' approach."[4]

Subsequent to the release of PPD-8, significant progress has been made on the actions required with the release of the National Disaster Recovery Framework (September 2011), the National Prevention Framework (May 2013), the National Mitigation Framework (May 2013), and a second edition of the National Response Framework (May 2013).[5] As part of the development of these frameworks and the

---

2 George W. Bush, Homeland Security Presidential Directive 8, December 2003, 1.

3 Barack Obama, Presidential Policy Directive 8, March 2011, 1.

4 Ibid., 3.

5 Federal Emergency Management Agency, "National Planning Frameworks," www.fema.gov/national-planning-frameworkS.

national proliferation of the all-hazards approach, a Strategic National Risk Assessment was conducted, the results of which "affirmed the need for an all-hazards, capability based approach to preparedness planning."[6] The concept has since worked its way throughout the litany of Federal guidance for agencies involved with all phases of disaster management, solidifying the intent to promulgate the all-hazards approach as the national standard. In fact, the federal rhetoric implies that the implementation is considered fundamentally complete, as identified in the 2012 National Preparedness Report: "The Nation has established the foundation for an integrated, all-hazards planning architecture that considers routine emergencies and catastrophic events."[7]

The approach eventually bled over into the larger HSE, and now resides as part of our overall National Security Strategy (NSS) as issued by the White House. The NSS pledges a more concerted effort to, "integrate homeland security with national security; including seamless coordination among Federal, state, and local governments to prevent, protect against, and respond to threats and natural disasters,"[8] recognizing both the breadth (multiple agencies) and depth (multiple levels of government) that are included in the approach. All-hazards has thus been firmly established at the Federal Policy level as the current way forward for the nation, and much emphasis in both time and resources has been placed on its implementation.

The all-hazards approach, when viewed from a macro level, has three overarching goals:

- Increasing collaboration among HSE partners to maximize capabilities through mission-sharing and broadening cooperation. This is best exemplified by the volumes of national-level policy from multiple federal agencies that now include the all-hazards approach, including the NSS. Among the NSS' goals is "Effectively Managing Emergencies," which strives for "integrating domestic all hazards planning at all levels of government and building key capabilities to respond to emergencies."[9]

---

[6] U.S. Department of Homeland Security, National Preparedness Goal (First Edition), September 2011, 3.

[7] U.S. Department of Homeland Security, National Preparedness Report, March 2012, i.

[8] The White House, National Security Strategy, May 2010, 2.

[9] The White House, NSS, 18.

- Reducing inefficiencies in resource utilization, primarily through efforts such as the regionalization of assets, whereby equipment and technical specialists are shared across a region rather than filling the capability for each and every jurisdiction. (For example, a set of four geographically close towns sharing a regional bomb squad, as opposed to each town housing their own squad at quadruple the cost.) Federal agencies have already taken this approach, as evidenced by the National Infrastructure Protection Program (NIPP) supporting an all-hazard approach to Critical Infrastructure/Key Resource (CI/KR) protection.[10] The NIPP thus recognizes that risk assessments to a building for a man-made event have significant overlaps with a similar assessment for a natural disaster.
- Enhancing and improving the national posture in all phases of disaster management, be it man-made or natural. From the National Strategy for Homeland Security: "An effective all-hazards response effort must begin with a strong foundation based on clear roles and responsibilities across all levels of government and the private and non-profit sectors, strengthened doctrine to guide our national response, a joint planning process to improve response capabilities, and advance readiness activities to better prepare for an impending or emergent event."[11]

Although these goals are not stated explicitly in federal guidance, the concepts in my estimation are readily identifiable and explain the substantial shift in policy and approach being undertaken from a federal level. The HSE is attempting to be shrewder, smarter, and better prepared.

B. PROBLEM IDENTIFIED

A key tenet of the all-hazards approach is collaboration across the multiple partners and levels of government involved in incident management, including the sharing of critical information and intelligence through new and established channels to strengthen all members of the HSE. Primarily situated in the prevention and protection phases of the National Preparedness System, intelligence and information sharing are part of the "all-hazards approach to National Preparedness,"[12] and are outlined as follows in the NPG:

---

[10] U.S. Homeland Security Council, National Strategy for Homeland Security, October 2007, 26.

[11] U.S. HS Council, 32.

[12] DHS, NPG, 2.

"Intelligence and Information Sharing–Provide timely, accurate, and actionable information resulting from the planning, direction, collection, exploitation, processing, analysis, production, dissemination, evaluation, and feedback of available information concerning threats to the United States, its people, property, or interests; the development, proliferation, or use of WMDs; or any other matter bearing on U.S. national or homeland security by Federal, state, local, and other stakeholders. Information sharing is the ability to exchange intelligence, information, data, or knowledge among Federal, state, local, or private sector entities, as appropriate.

- Anticipate and identify emerging and/or imminent threats through the intelligence cycle.
- Share relevant, timely, and actionable information and analysis with Federal, state, local, private sector, and international partners and develop and disseminate appropriate classified/unclassified products.
- Ensure Federal, state, local, and private sector partners possess or have access to a mechanism to submit terrorism-related information and/or suspicious activity reports to law enforcement."[13]

Intelligence and Information Sharing are identified as a core capability that spans the prevention and protection missions, which is understandable given that the intent is to use these capabilities to interdict an event before it happens. As such, the definition above still leans towards the prevention of a terrorist attack, as seen in Item 3. However, true to all-hazards form, the capability does not limit the capability, or preclude the use, of intelligence in events outside the criminal realm, i.e., natural disasters. In fact, it can be asserted that while the timing of an event may be relatively unpredictable, the effects of a natural disaster are not as random as we currently view them. This concept will be discussed more in Chapter V.

On a state and local level, this intelligence function would traditionally be held by local law enforcement, or in many large metropolitan areas in the U.S., the State/Local Fusion Centers (SLFC). Along with all other capabilities identified in the NPG, SLFCs are directed to adopt the all-hazards approach through the collection and dissemination of

[13] Ibid., 6.

intelligence to all community partners. Additionally, "fusion centers position law enforcement, public safety, *emergency management*, fire service, public health, critical infrastructure protection, and private security personnel to understand local implications of national intelligence."[14]

Despite the existence of multiple Federal-level policies that outline the importance of intelligence and information sharing across the all-hazards community, EM is still by-and-large an outsider to the Intelligence Community (IC). The problem is one of both policy and of practice; despite the existence of the aforementioned policy, not enough has been explored or fleshed out, and what has been fleshed out is not implemented on any sort of national scale. First identified as a weakness by the 9/11 Commission, the Weapons of Mass Destruction Commission,[15] and President George Bush,[16] progress towards the ideal end state has seen minimal success. In fact, the National Preparedness Report (NPR) of 2012 found that of the seven areas identified as "national strengths," the only one to not be assessed in the top 10 capabilities from a State perspective was the Intelligence and Information Sharing capability.[17] The 2013 NPR showed minimal improvement, with this capability barely cracking the top 10;[18] however, this "improvement" is questionable given the reliance on a SLFC self-assessment tool that limits consideration of how robust a statewide intelligence capability is outside of the SLFCs.[19] Seemingly strong from a national level, the policy has not made its way into the State level and below, which is detrimental to our EM and first responder communities who are the most heavily involved in day-to-day operations.

In addition to the lack of inclusion in the IC, EM has lagged far behind in establishing a process and function for the collection and use of intelligence. While

---

14 DHS, NPR-2012, 12.

15 Office of the Director of National Intelligence, "United States Intelligence Community Information Sharing Strategy," (February 2008), 3.

16 George W. Bush, "Using 21st Century Technology to Defend the Homeland," available from http://www.whitehouse.gov/homeland/21st-technology.html.

17 DHS, NPR-2012, ii.

18 U.S. Department of Homeland Security, National Preparedness Report, March 2013, 8.

19 Ibid., 19.

counter-terrorism experts have long used well-refined method of intelligence gathering and analysis, EM lacks the training and tools to broaden its understanding and role in the IC as more than just a consumer of whatever intelligence products are dictated to be pertinent for their review. EM should be a sensor, consumer, and producer of intelligence, and if truly integrated, would prove to be a mutually beneficial partner with the IC.

C. IMPACT ON CURRENT OPERATIONS

Because EM is not included in the IC and does not have a formalized process for Intelligence collection and processing, all three of the all-hazard goals identified above are negatively impacted.

- Collaboration is limited and capabilities are not maximized, most clearly evidenced by the lack of State Emergency Operations Center (EOC) and SLFC relationship. Here again we see the existence of national policy that is largely ignored at the State level and below. A joint DHS/Department of Justice report from 2012 found that, "more than 83% of the (SLFC) locations visited were either unaware of or did not utilize federal guidance for Fusion Center and Emergency Operations Center interaction provided in Comprehensive Preparedness Guide 502."[20] This lack of collaboration is largely unexplained and somewhat ironic, as both the EOC and the SLFC are by nature collaborative, bringing multiple jurisdictions and resources together for a common goal. Yet the majority of these champions of partnership do not work together despite a significant overlap in responsibilities and capabilities. A key connection between state level assets and partners is thereby missing, a piece that limits a common operating picture during events that are under the purview of both entities. This is further exacerbated by a lack of common language and understanding of intelligence, and therefore the connection to maximize capabilities is impeded.
- Resource utilization is not currently optimized, either, as there is a clear overlap of responsibilities between the IC and emergency managers and seemingly little effort to eliminate the redundancies. For example, the area of CI/KR risk analysis and protection is a common theme to both the IC and EM. While the IC looks at the facilities from a terrorist angle as they conduct Critical Infrastructure Protection (CIP) assessments, EM personnel are also required to assess the same facilities and aid them through the phases of mitigation, preparation, response, and recovery

[20] U.S. Department of Homeland Security Office of Inspector General, *Relationships Between Fusion Centers and Emergency Operations Centers*, December 2011, 1.

during an event of significance. How much more effort would be required to conduct these simultaneously, or at least share the information as a foundation for the EM assessments (or vice versa)? Time, effort, and expertise are wasted in the duplicitous assessment of these facilities. Systems such as the Automated Critical Asset Management System (ACAMS)[21] are housed in either the SLFC or EOC, with the same entity being designated as the point of contact and thereby controlling access to the system. For example, in a large metropolitan city this responsibility is seated with the SLFC; no personnel at the State EOC have been given access. Although ACAMS isn't a law enforcement/fire service specific program, the use of ACAMS is tied to the Terrorism Liaison Officer (TLO) program and since the SLFC has "taken the approach that emergency managers aren't included in the TLO program,"[22] access to this particular State's ACAMS has neither been offered nor granted to the EOC. This same redundancy can be found in the area of Hazardous Materials Tier II reporting as the information is collected by state EM or the SLFC yet is not stored in a shared database where both agencies may access and update any information. The United States "cannot afford to protect all things from all threats and hazards; therefore, critical decisions must be made about how to invest limited resources to achieve the greatest results."[23] One of the easiest decisions would be to eliminate the stovepipes that prevent intelligence being gathered by and shared amongst "need-to-know" partners and reducing duplicitous data gathering efforts.

- Intelligence is a key piece of prevention and protection (as mentioned in the NPG); because EM is not a member of the IC and does not currently have a process for gathering, analyzing, and using intelligence, a key capability is missing that is "central to the process of preparedness. They (collaboration and information sharing)…are predicate elements that enable agencies, jurisdictions, and organizations to effectively perform the other elements of prevention."[24] Attempts have been made over the years to mitigate and prepare for natural disasters, but these efforts have been overshadowed by the incessant focus on response capabilities. The result is that EM maintains a reactive posture, rather than a proactive one as evidenced by "the default position of most responder agencies, as suggested by the label 'response' to an event."[25] This posture is most

21 U.S. Department of Homeland Security, *Automated Critical Asset Management System (ACAMS)*, http://www.dhs.gov/automated-critical-asset-management-system-acams.

22 Personal communication with State EM Operations Section.

23 William O. Jenkins (2007), Testimony before the Subcommittee on Homeland Security, House Committee on Appropriations (GAO Report No. GAO-07–386T), 1–2.

24 William V. Pelfrey, The Cycle of Preparedness: Establishing a Framework to Prepare for Terrorist Threats, Journal of Homeland Security and Emergency Management, 2 (1, Article 5), 9.

25 Ibid., 1.

accurately depicted in Federal spending on the various phases of EM: in FY2013, State & Local Programs (covering all 4 phases) were budgeted $654M; the Disaster Relief Fund (overwhelmingly focused on response and recovery, with minimal funds given to mitigation and preparedness) was slated for $6.088B.[26] This funding, at first glance, could reflect a solid foundation in preparedness, thereby allowing for an emphasis on recovery. However, this is not the case, and is more accurately identified as the inability of the EM community to swing the pendulum to the preparedness and mitigation phases. Intelligence, and the use of, is critical to that swing.

- The lack of intelligence is detrimental to routine EOC operations, as well. Without the ability to analyze and synthesize the volumes of information coming into the EOC during an activation, data is not culled and consolidated outside of situation reports. Information alone is not intelligence; you need some mechanism to process the information into some sort of usable, actionable format. Information sharing alone leads to subjective interpretations, not a much more critical Common Operating Picture. Additionally, instruments critical to preparedness and protection, such as risk assessments, are not utilized or incorporated into EOC decision-making during events.

D. RESEARCH QUESTION

As this all-hazards approach takes hold and continues to blend the best of the two sub-fields (HS and EM), an area that has yet to be explored to its fullest extent is the utilization of an intelligence process to enhance EM operations. Could a refined and well-developed method for intelligence gathering and synthesis within the EM community help strengthen current operations, as well as foster better collaboration with the broader HSE? Is there a benefit to pushing for EM inclusion into the larger IC, and how best could the EM community support this all-hazards approach to ensure the benefit was mutual to both communities?

The question this thesis will attempt to answer is: *Is there a role for an intelligence process within the emergency management field? If so, what role could it play, what would the process look like, and how best could it be implemented to improve the all-hazards homeland security enterprise?*

[26] Federal Emergency Management Agency, The State of FEMA, 2012, 38.

E. ASSUMPTIONS AND HYPOTHESES

By definition, the intelligence process does not necessitate criminal activity; rather, it is simply a well-defined method of information gathering and subsequent analysis. As such, EM intelligence could support a more robust decision-making process within the EM community and the HS community at large. In many ways, the EM field already has a role (albeit a support role) in the response operations to all-hazards events, including terrorism, and thus has a vital role in this information gathering/analysis process. Formalizing this role and subsequently equipping and training emergency managers could be of substantial benefit to jurisdictions in all phases of a disaster.

Once established, an EM intelligence process could also help augment and integrate into the IC to provide more robust HS capabilities. EM has a significant amount of information that would be of use to the IC that is not currently shared (i.e., HazMat Facilities), and could also provide situational awareness during large-scale events for factors that aren't readily discernible in the field (i.e., weather forecast, locations of critical infrastructure). This integration into the IC would include greater collaboration with the SLFC to give each state a more comprehensive HS community, able to prepare for, respond to, and recover from disasters of all shapes and sizes.

My hypothesis is that the establishment, refinement, and consistent use of an intelligence process could swing the EM pendulum from the reactive to the proactive. Borrowed from best practices in the current IC, and adapted to ensure a process that better reflects the all-hazards goal, the potential benefits include: decreased in response time by pre-positioning resources; enhanced situational awareness; and the inevitable reduction of recovery costs due to advanced information gathering, processing, and addressing vulnerabilities before they were affected.

F. METHOD

The goal of this thesis is to determine whether or not intelligence has a role in EM and if a well-defined intelligence process for EM can contribute to the all-hazards community. If the evidence suggests there is a role for intelligence in EM, then the next step is to develop a model for the use of an intelligence process within the EM

community. In order to most effectively develop this intelligence process model and test the hypotheses, my research is two-tiered. The first step is to evaluate key portions of the intelligence processes from various members of the IC through case studies to glean relevant elements and procedures. These best practices come from the military (intelligence preparation of the battlespace), the current U.S. IC (domestically represented by the Federal Bureau of Investigation), and processes currently used by local jurisdictions (intelligence-led policing). These processes have an abundance of open source material available, and there are some clear similarities between the different members of the IC and their methods of analysis, synthesis, and delivery. Through extracting these concepts from those sources, I establish a working model of an intelligence process for EM, including steps, a flow diagram, and any other key guiding principles that appear to be essential for success. If key causal factors can be identified and confirmed, a model developed from the aforementioned principles from the IC could be translated to the EM community.

The ideal end result will be a model that is scalable, functional, easily implemented, and utilized by any level of government. Groundwork would then be laid for better collaboration with the current IC by the EM community, better support to first responders during large-scale events, a more proactive role in preventing future disasters, and a more robust all-hazards community as a whole.

G. CHAPTER OUTLINE

This thesis discusses the use of intelligence in EM, including how the EM community can best collaborate with the IC to best support and improve the all-hazards approach to incidents. Chapter II reviews current literature on the current uses of intelligence in the EM community, including a brief discussion of the term "intelligence" to help narrow the focus of the subsequent chapters. The review also looks at the current EM-SLFC relationship and identifies both gaps and opportunities moving forward.

Chapter III addresses the first portion of the research question, determining whether there is a need and role for an intelligence process within EM. The role of such a

process is compared against the five mission areas of FEMA, and includes a real-life example of how EM intelligence was, or could have been used, during an incident.

Chapter IV discusses current models of the use of intelligence from three different perspectives: the U.S. Military's Intelligence Preparation of the Battlespace process; the Federal IC's intelligence process, focusing primarily on the Federal Bureau of Investigation (FBI); and finally local jurisdiction's use of intelligence-led policing tactics. A summary of transferrable concepts relevant to the EM community concludes each section of the chapter.

Chapter V presents a model of the use of intelligence of EM based on the best practices from the previous chapter. It also includes discussion of field application and provides examples of how a proposed Emergency Management Intelligence Cycle could be utilized to enhance the overall all-hazards community.

Chapter VI discusses conclusions and recommendations for integrating the EM intelligence model into the existing EM community, as well as offering suggestions for overcoming identified obstacles. This chapter summarizes the overall key findings of the thesis and serves as concluding statements regarding the material.

II. LITERATURE REVIEW

A. INTRODUCTION

The purpose of this review is to summarize current literature that addresses the definition of intelligence, the intelligence process, and areas of applicability to the EM field. Because this subject is specific to governmental EM and HSE, the scope of the literature reviewed was primarily limited to governmental documents, including government agencies outside DHS that have established intelligence-gathering processes. The review of academic writings was added when warranted and available. The literature can be broken down into: 1) literature that focuses on definitions of intelligence and the intelligence process; 2) literature that addresses the use (or potential use) of intelligence within the EM community; and 3) literature that looks at the EOC-SLFC relationship, the primary source of current interaction between the EM and IC.

B. DEFINITIONS OF INTELLIGENCE AND THE INTELLIGENCE PROCESS

1. Intelligence

The concept of intelligence is not new to the homeland security enterprise as evidenced by DHS' inclusion in the IC, as identified by the Office of the Director of National Intelligence's (ODNI) identified IC.[27] However, the lack of its clear application to the world of EM necessitates some consideration, and thus establishing commonalities amongst the sources will provide a working definition to frame the remainder of this review. The base definition used is that of the U.S. Department of Defense from 1998: "the product resulting from the collection, processing, integration, analysis, evaluation and interpretation of available information concerning foreign countries or areas."[28] Definitions from various government sources involved in the IC generally agree with this premise: the FBI defines intelligence as "information that has been analyzed and refined

[27] Office of the Director for National Intelligence, "Members of the Intelligence Community," http://www.dni.gov/index.php/intelligence-community/members-of-the-ic.

[28] U.S. Joint Chiefs of Staff, "Joint Publication 2–02. National Intelligence Support to Joint Operations," (September 1998), 12.

so that it is useful to policymakers in making decisions;"[29] and the Central Intelligence Agency defines it as "knowledge and foreknowledge of the world around us,"[30] and includes the connection to policymakers. Simplified, it can be depicted in the equation "Intelligence= Information + Analysis,"[31] is scrutinized to determine or formulate meaning and relevance,[32] and includes a deliverable of actionable choices and likelihood of outcomes.[33] It is also often used interchangeably to describe, "product, organization, mission, or process."[34]

From a national strategic and operational perspective, there is an effort to define the parameters of what can be classified as intelligence, as information gathered on any topic and analyzed would not necessarily qualify. The Intelligence Reform and Terrorism Prevention Act of 2004 defines national intelligence as "information gathered in the U.S. or abroad that pertains to more than one agency and involves threats to the U.S., its people, property or interests…or any other matter bearing on national or homeland security."[35] As the HSE moves towards the all-hazards concept, however, the scope of intelligence becomes larger and includes: "political, military, scientific and technical, economic, sociological, and environmental"[36] information. The mission now dictates a broader intake of information.

---

[29] Federal Bureau of Investigation, Intelligence Defined, http://www.fbi.gov/about-us/intelligence/defined.

[30] Dr. Michael Warner, "Wanted: A Definition of Intelligence," (Central Intelligence Agency), https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol46no3/article02.html (accessed October 23, 2012) as cited from Central Intelligence Agency (Office of Public Affairs), A Consumer's Guide to Intelligence (Washington, DC: Central Intelligence Agency, 1999), vii.

[31] Canadian Defence Intelligence Agency, Intelligence Analyst Course Textbook (Joint Military Intelligence Training Center, 2000), II-4–2.

[32] U.S. Department of Homeland Security and U.S. Department of Justice, Comprehensive Preparedness Guide 502: Considerations for Fusion Center and Emergency Operations Center Coordination (May 2010), 10.

[33] Valerie Lucus-McEwen, "Recalibrating Emergency Management: Information is not the same as intelligence," Emergency Management, December 2010, http://www.emergencymgmt.com/emergency-blogs/campus/Recalibrate-Emergency-Management-Information-Intelligence-122910.html.

[34] Lt. Col. Patrick Kelly III, "Intelligence Support to Homeland Security: Supporting the Supporting Effort," U.S. Army War College-Strategy Research Project (April 2002), 11.

[35] United State Government, "Intelligence Reform and Terrorism Prevention Act of 2004," Public Law 108–458 of December 17, 2004; 118 STAT.3638, 148.

[36] Lt. Col. Patrick Kelly, "Intelligence Support to Homeland Security," 11.

From the government documents reviewed for this literature review, there is general consensus and acceptance of the general definition of intelligence, with nuances attributable to the mission goals of the organization defining it (i.e., the U.S. Central Intelligence Agency includes foreign and secret considerations, as these align with their mission). Sources from the academic community vary minimally, and offer that intelligence is collected with national welfare in mind,[37] and includes secret information that is not available in the public domain.[38] Dr. Michael Warner, historian with the Central Intelligence Agency, asserts that, "without secrets, it is not intelligence" and offers the definition of intelligence to be, "secret, state activity to understand or influence foreign entities."[39] However, the counter-argument is that intelligence, at its most basic level, is simply information that helps you solve a problem and gives you a decision-making advantage; it is not "secrets." Because the model proposed in Chapter IV is not reliant on confidential or secret information, the broader, more global context of intelligence will be utilized, as the definition of intelligence at this higher level thus appears to be fairly standard.

2. The Intelligence Process

The process of Intelligence also has generally accepted tenets with minor debate limited mainly to semantics amongst government agencies that utilize such a process. The Canadian intelligence process includes five key steps: direction, planning, collection, analysis, and dissemination.[40] The FBI adds a requirements section to the front end of this process, and includes a processing and exploitation step between the collection and analysis.[41] These fundamental elements are utilized by members of the

---

[37] Warner, Wanted, as cited from Herman Kent, Strategic Intelligence for American Foreign Policy (Princeton, NJ: Princeton University Press, 1949), vii.

[38] Ibid, as cited from Council on Foreign Relations [Richard N. Haass, project director], Making Intelligence Smarter: Report of an Independent Task Force (New York, NY: Council on Foreign Relations, 1996), 8.

[39] Ibid.

[40] Canadian Security Intelligence Service, Backgrounder No. 3 – CSIS and the Security Intelligence Cycle, February 2004, http://www.csis-scrs.gc.ca/nwsrm/bckgrndrs/bckgrndr03-eng.asp.

[41] Federal Bureau of Investigation, Intelligence Cycle, http://www.fbi.gov/about-us/intelligence/intelligence-cycle.

U.S. Military (the Air Force's Intelligence Surveillance Reconnaissance process, for example),[42] as well as internationally.[43] The entire process is continuous and only completed when the needs of the decision maker are met for a given subject or event.[44] At the State level, SLFCs in particular use this process regardless of the mission, the disciplines they support, or the types of information they receive.[45] Information from the academic community supports this process; however, there is an argument for the need for action on the intelligence to be included, as evidenced by Mark Lowenthal's addition of an operational component to the end of the intelligence process.[46]

3. Information Sharing and Fusion

In addition to the traditional and somewhat standard use of the term "intelligence," a vernacular for the all-hazards and intelligence communities has developed to include terms that are now directly associated with the intelligence process. Of most relevance to this course of study are the terms "information sharing," and "fusion." In the IC, "information sharing is the act of exchanging intelligence information between collectors, analysts, and end users in order to improve national and homeland security."[47] Both the Intelligence Reform and Terrorism Prevention Act of 2004 and the 9/11 Commission Recommendations Implementation Act of 2007 mandated the IC to revise their methods of dissemination and collaboration to achieve information sharing,[48] and the proliferation of the term throughout federal all-hazards guidance is readily evident. Nearly synonymous with information sharing, the term "fusion" implies "dissemination of both raw information and finished intelligence."[49] This term is where

---

[42] U. S. AIR FORCE, Air Force Doctrine Document 2–5. In:Command, A. F. D. edited 2002, 5.

[43] Canadian Chief of Defence, Joint Intelligence Doctrine, CF Publication B-GJ-005–200FP-000, May 2003, 2–4.

[44] Lt. Col. Patrick Kelly, "Intelligence Support to Homeland Security," 19.

[45] DHS-DOJ, CPG 502, 9.

[46] Warner, Wanted, as cited from Mark M. Lowenthal, Intelligence: From Secrets to Policy (Washington, DC: Congressional Quarterly Press, 2002 [second edition]), 8.

[47] ODNI, USIC Information Sharing Strategy, 3.

[48] The Markle Foundation, "Nation At Risk: Policy Makers Need Better Information to Protect the Country," (March 2009), 4.

[49] Lt. Col. Patrick Kelly, "Intelligence Support to Homeland Security," 37.

SLFCs derive their moniker, as they are hubs of both finished and unfinished information products. Both terms are important to the all-hazards community; thus their inclusion in this literature review.

C. LITERATURE ON CURRENT STATUS OF EM-IC OPERATIONS

What role, if any, is there then for an established process for intelligence gathering in the discipline of EM? If there is general agreement and understanding of the definition of intelligence and the process for intelligence gathering and analysis, why hasn't there been a more well-defined and established process for employing it in routine operations? With definitions ruled out, a survey of literature on the current relationship between the IC and EM is important to further flesh out a potential connection. A review of areas of discrepancy and opportunity then follows in the remaining sections of this literature review to provide a framework for future considerations.

1. Intelligence in the HSE

The literature on the broader IC is exhaustive; in an effort to provide a basis for the study and subsequent findings of this project, I will therefore limit the survey of the use of intelligence to the HSE, narrowing to the use of intelligence in EM. The U.S. DHS, as a member of the U.S. IC, takes its broader objectives and priorities from the Director of National Intelligence.[50] However, DHS has established its own Intelligence Enterprise (DHSI) within the agency composed of three offices/programs (the Office of Intelligence & Analysis (I&A), Homeland Infrastructure Threat and Risk Analysis Center (HITRAC), and the Intelligence Division of the Office of Operations Coordination and Planning), and the "intelligence elements of six operational components: U.S. Customs and Border Protection (CBP), U.S. Immigration and Customs Enforcement (ICE), U.S. Citizenship and Immigration Services (USCIS), Transportation Security Administration

[50] U.S. Government, IRPTA, 2.

(TSA), U.S. Coast Guard (USCG), and U.S. Secret Service (USSS)."[51] Noticeably absent from this list is the Federal Emergency Management Agency (FEMA), the lead EM agency in the nation.

Within the DHSI, I&A and the HITRAC provide the greatest connection to the EM community. I&A's mission is to provide intelligence and staff to support DHS-wide "operational planning and coordination to support crisis and contingency planning and operations to support the Secretary of Homeland Security in his/her HSPD-5 role as the principal Federal official for domestic incident management."[52] I&A includes the Interagency Threat Assessment and Coordination Group (ITACG), which provides support and leadership to risk analysis and threat assessments in collaboration with state and local governments.[53] Although these threat assessments are conducted for HS-identified threats, their potential use by and application to the EM community will be discussed in detail below. Also within the DHSI, the HITRAC dually supports the Infrastructure Protection and I&A functions of DHS. Specifically, the HITRAC "provides timely and integrated risk, threat, and consequence analyses to give the Department and its security partners an understanding of threats, infrastructure vulnerabilities, and potential consequences of attacks or natural disasters."[54] With the inclusion of natural disasters, HITRAC is one of the few DHSI members that expressly mentions the value of intelligence to the EM community.

Moving away from the research on the organizational aspects and towards literature supporting the utility of such a function, several potential connections are identified. The use of intelligence by EM can be divided into six functions[55]:

---

[51] Mark A. Randol, "The Department of Homeland Security Intelligence Enterprise: Operational Overview and Oversight Challenges for Congress," Congressional Research Service 7–5700 (May 27, 2009), 2–3.

[52] Ibid., 18.

[53] U.S. Department of Homeland Security, "Interaction with State and Local Fusion Centers: Concept of Operations," (December 2008), p. 12. (Note: the ITACG has recently been renamed the Joint Counterterrorism Assessment Team- JCAT.)

[54] U.S. Department of Homeland Security, About the Infrastructure Analysis and Strategy Division, http://www.dhs.gov/infrastructure-analysis-and-strategy.

[55] Lt. Col. Patrick Kelly, "Intelligence Support to Homeland Security,"19.

- Indications and Warning–Intelligence has been identified to bolster both preparedness efforts pre-incident, and well as during the response phase.[56] Because of this, intelligence operations (such as indications and warnings) tend to be proactive in nature,[57] which directly addresses the EM posture problem identified in Chapter I. The indications portion also has significant applications to the mitigation phase of disaster preparedness.[58]

- Intelligence Preparation (including threat/vulnerability assessments)–one of the biggest obstacles to the use of information in EM is volume: "an abundance of threat information from various sources often reaches emergency managers in an uncoordinated fashion."[59] The information needs to be "selected, interpreted, and acted on;"[60] this interpretation is what takes place through the intelligence process. Part of this preparation phase is accomplished through threat/vulnerability assessments, which help jurisdictions identify their high probability, high consequence assets and direct resources accordingly. This function would also utilize risk analysis capabilities, as the collaboration between HS risk analysts and the IC have been identified to be "critical for producing effective threat assessments…(for) managing homeland security risk."[61] Currently, this function is handled primarily by the Information Analysis Directorate of DHS, and includes intelligence provided by other agencies (i.e., FBI, CIA).[62] At the State and local level, this manifested itself in the Strategic Hazard Identification and Risk Analysis, which has now evolved into the Threat Hazard Identification and Risk Analysis.[63]

- Situation Development–intelligence is a critical portion of ongoing situational awareness, as the cyclical and iterative process of intelligence gathering, processing, and producing ensures that incident commanders have "the intelligence he actually needs, when he needs it, in order to

---

56 FEMA, Intelligence/Investigations, 12.

57 Lt. Col. Patrick Kelly, "Intelligence Support to Homeland Security," 20.

58 Keeley Townsend, John P. Sullivan, Thomas Monahan, & and John Donnelly (2010), Intelligence-led Mitigation, Journal of Homeland Security and Emergency Management, 7 (1, Article 63), 5.

59 Howard Bean and Lisa Keranen (2007), The Role of Homeland Security Information Bulletins within Emergency Management Organizations: A Case Study of Enactment, Journal of Homeland Security and Emergency Management, 4 (2, Article 6), 4.

60 Ibid., 5.

61 David P. Jackson, "Intelligence-Led Risk Management for Homeland Security: A Collaborative Approach for a Common Goal," (Master's Thesis, Naval Postgraduate School, 2011), 2.

62 The Honorable Jane Harman, Testimony before the U.S. Senate Homeland Security and Governmental Affairs Committee, July 12, 2012, 2.

63 John Baker, "Risk Analysis and Intelligence Communities Collaborative Framework," Homeland Security Institute (April 2009), 63.

make rapid decisions."[64] Situational analysis is conducted in a ongoing manner, and is used to gain a common operating picture for all EM/response personnel.[65] This intelligence can help make resource decisions[66] at the EOCs, as well as in the field. Its utility in this function is becoming more standardized, as seen by the inclusion of intelligence in National Incident Management System Components[67], and the use of Intel & Analyst Functions at national-level operations centers.[68]

- Target Development–once a threat, vulnerability, or risk is identified in Function 3 (above), "targets can be appropriately hardened and suspects identified while an event is still in its inchoate stage."[69]
- Damage Assessment–the literature is sparse in the use of intelligence in damage assessments. DHS' I&A retains information about CI/KR, including private sector information.[70] Knowing what exists before an incident is key to assessing damage.
- Force Protection–the literature here, too, is silent, as this function seems to apply more to offensive military-type operations. Its application to first responders, however, will be discussed more in Chapter IV.

2. EOC-SLFC Relationship

Outside of the aforementioned functions, the best source of potential collaboration as found in current literature is the EOC/SLFC relationship. Each state and metropolitan area has an EOC; the primary function of which is to provide a "physical location where information and resources are coordinated to support incident management (on-scene operations) activities.[71] As of 2011, DHS reported that there are seventy-seven (77) SLFCs nationwide,[72] primarily found in the same metropolitan areas and within close

64 Keeley Townsend, John P. Sullivan, Thomas Monahan, & and John Donnelly, "Intelligence-led Mitigation," 7.

65 FEMA, Intelligence/Investigations ,1

66 Keeley Townsend, John P. Sullivan, Thomas Monahan, & and John Donnelly, "Intelligence-led Mitigation," 6.

67 FEMA, Intelligence/Investigations, 2–3.

68 U.S. Department of Homeland Security, About the Office of Operations Coordination and Planning, http://www.dhs.gov/about-office-operations-coordination-and-planning.

69 Howard Bean and Lisa Keranen, "The Role of Homeland Security Information Bulletins," 9.

70 Mark A. Randol, "The Department of Homeland Security Intelligence Enterprise," 5.

71 DHS-OIG, Relationships, 5.

72 U.S. Department of Homeland Security, "Fusion Center Locations and Contact Information," http://www.dhs.gov/fusion-center-locations-and-contact-information.

range of the metropolitan/State EOC. The SLFCs exist to "promote greater collaboration and information sharing among federal, state, and local intelligence and law enforcement entities."[73] They are typically staffed by intelligence, law enforcement, and functional professionals who "facilitate the multi-directional flow of timely, accurate, actionable 'all-hazard' information."[74] DHS has established an Office of Operations Coordination and Planning that supports SLFC's by providing "domestic situational awareness of all threats and all-hazards, whether man-made or natural."[75] A 2013 report on SLFCs indicated that 26% of the SLFCs are collocated with EOCs;[76] however, some sources surmise that 100% is inevitable as the SLFCs become more firmly established and mature[77].

A review of key literature on the EOC-SLFC relationship further shows that the potential benefits of a connection between the two has been explored to some degree, primarily in government-published documents. Viewed from both an organizational and operational standpoint, many sources identified value in a connection due to various commonalities in responsibilities and resources. For example, Our National Intelligence Strategy doesn't directly address the EM community, but includes climate change and pandemic disease as "transnational forces and trends" that present strategic challenges for the IC to address.[78] The U.S. Congress has also stressed the importance of EM as being a part of the fusion process, as evidenced by EM's inclusion in the 9/11 Commission Report and the 2010 Quadrennial Homeland Security Report.[79] Congress has even gone so far as to formalize this mandate through the 9/11 Commission Act of 2007, requiring DHS to establish standards for intelligence products produced within its agency's

73 DHS-OIG, Relationships, 2.

74 DHS, Interaction with Fusion Centers, 33.

75 DHS, Interaction with Fusion Centers, 15.

76 National Network of Fusion Centers, "2012 Final Report," June 2013, 33.

77 Dr. James Steiner, "Needed: State-level, Integrated Intelligence Enterprises," Studies in Intelligence (Volume 63, No. 3), September 2009, 4.

78 Office of the Director of National Intelligence, *The National Intelligence Strategy*, August 2009, 4.

79 DHS-OIG, Relationships, 7.

purview.[80] The ODNI also contains a National Intelligence Emergency Management function whose goal is to "lead an integrated and resilient IC enterprise capable of sustaining the 'intelligence cycle' under any crisis or consequence management event."[81] Additionally, several federal agencies that contain intelligence components collocate those functions with their EM and response operations; the U.S. Department of Transportation is an example.[82]

The strongest case for a connection between the EM and Intelligence communities came from a joint U.S. Department of Justice (DOJ) and DHS publication that established standards for SLFCs, including their links to EOCs: "The Fusion Center provides intelligence to the EOC regarding the disaster or related events (regardless of whether the Fusion Center is all-crimes or all-hazards). (P)lans and procedures should include how each Fusion Center will support the jurisdiction's emergency management structure during a crisis."[83]

The literature in support of the EOC-SLFC interface also agrees on some common competencies that the collaboration should strive for. DHS includes the production of threats and risk assessments as a competency both should assist each other in conducting, and includes EM in their list of providers of intelligence.[84] DHS plays a key role in this through both the production of HS Threat Assessment and Intelligence reports on a regular basis[85] and the deployment of Intelligence Officers and Protective Security Advisors to support its partners in the HS regions.[86] This federal literature also

---

80 U.S. Congress, 9/11 Commission Act of 2007 - P.L. 110–53, August 3, 2007.

81 Office of the Director for National Intelligence, "National Intelligence Emergency Management," http://www.dni.gov/index.php/about/organization/niema.

82 U.S. Department of Transportation, "Office of Intelligence, Security and Emergency Response," http://www.dot.gov/ost/oiser/intelligence.htm.

83 U.S. Department of Homeland Security and U.S. Department of Justice, Fusion Center Guidelines, 2006, 12.

84 U.S. Department of Homeland Security and U.S. Department of Justice, Common Competencies for State, Local, and Tribal Intelligence Analysts, June 2010, 7.

85 Mark A. Randol, "The Department of Homeland Security Intelligence Enterprise," 9–10.

86 U.S. Department of Homeland Security, "Deployed Intelligence Officers and Protective Security Advisors," http://www.dhs.gov/deployed-intelligence-officers-and-protective-security-advisors.

emphasizes the all-hazards approach, charging SLFC with "identify(ing) and prioritize(ing) types of major disasters and emergencies–beyond terrorism and crime-that could occur within their jurisdiction."

D. AREAS OF DISCREPANCY

Although the rhetoric is strong in the literature, especially in governmental circles, the action in formalizing the EM-IC relationship has been far less thorough indicating some disagreement on fundamental issues. The disagreements manifest themselves primarily as obstacles to implementation, but also in the lack of significant practical progress in overcoming them. DHS' acknowledges this deficiency, as their strategic plan for FY2012–2016, recognizes intelligence as an area needing "enhancement."[87] Outside agencies also recognize the lack of information sharing within the EM and IC communities; most notably, the 2009 Markle Report identified that the task of "ensur(ing) that all government information relevant to national security is discoverable and accessible to authorized users," remained largely "unfinished."[88]

The obstacles identified in the literature primarily fall into two categories: securitization of information, and lack of cross-disciplinary training. Of primary concern to the IC is that a greater sharing of information (intelligence) may "compromise source confidentiality—a legitimate concern for intelligence gatherers."[89] With a broadened IC comes an increase in the number of intelligence requests; this increase could tax existing sources of intelligence with an overwhelming number of inquiries, potentially hindering their utility. In addition to the confidentiality concerns, the classification of information also presents a challenge. "As long as multiple levels of security continue, isolation and duplication will complicate intelligence support to homeland security."[90] The cost in both time and effort to maintain such a classification system is somewhat prohibitive to

---

87 The Honorable Jane Harman, Testimony before the U.S. Senate Homeland Security and Governmental Affairs Committee, 2.

88 Markle Foundation, "Nation at Risk," 1–2.

89 Kiki Caruson, Mission Impossible? The Challenge of Implementing an Integrated Homeland Security Strategy. Journal of Homeland Security and Emergency Management, 1 (4, Article 407), 6.

90 Lt. Col. Patrick Kelly, "Intelligence Support to Homeland Security," 37.

the inclusion of more members. This obstacle is often exacerbated by the training and background requirements necessary to handle intelligence properly. Beyond training, collaboration between the two communities is further hindered by an absence of cross-discipline familiarity.[91] This obstacle is cyclical, as training creates cross-discipline awareness, but without even the basic context for the use of intelligence, it is incredibly difficult to work in a peer-to-peer setting without first bringing one discipline up to proficiency.

Turning to the EOC-SFLC relationship, because the literature detailing the relationship is somewhat sparse outside of the government realm, some inference could be drawn about the strained relationship by what is *not* addressed directly. No clearer is this exemplified than in an Office of the Inspector General (OIG) Report on relationships between EOCs and SLFCs which found that many SLFCs have designated themselves as either "all-crimes" or counterterrorism specific. "Where Fusion Centers adopt such designations (i.e., "all-crimes," "counterterrorism," etc.), information sharing with EOCs is significantly limited or non-existent."[92] This information directly contradicts a 2012 report on SLFCs that reported that "92.2% disseminate information to the EOC or respective lead EM agency in their area of responsibility."[93] This second number is suspect in that it is self-assessed, whereas the OIGs report was an independent review, and shows that there is a big disconnect in perception vs. action. In fact, the OIG's investigation found that more than 83% of the locations visited during their fieldwork did not receive or were not using Comprehensive Preparedness Guide 502,[94] nor did DHS formally track whether SLFCs have taken an all-crimes or all-hazards approach in their operations.[95] By inference, the overwhelming majority of SLFCs has chosen willfully to ignore these suggestions, or is unaware that a relationship might be beneficial. Even the

---

91 John Baker, "Risk Analysis and Intelligence Communities Collaborative Framework," 45.

92 DHS-OIG, Relationships, 7.

93 National Network of Fusion Centers, "2012 Final Report," 19.

94 Ibid., 22.

95 DHS-OIG, Relationships, 10.

National Intelligence Strategy, mentioned above, discusses traditional EM responsibilities, but never makes mention of the role of EM in our national IC.

On a more operational level, there is disagreement over the level of cooperation needed, with the two opposing views drawn along the EM-IC divide. On the EM side, the U.S. DHS and DOJ see a role for intelligence analysts from SLFCs to be available to serve as liaisons during an incident with a reciprocal role played by EOCs depending on the nature of the event.[96] However, proponents in the IC as identified by the OIG report hold that the diverse nature of response to and sources of information utilized in these varying events would limit the usefulness of such a connection.[97] The same is true of the suggestion of integrating SLFC personnel to analyze information gather by EOC sources,[98] as the skill sets required for each are not necessarily compatible according to the IC. The OIG report also identified a concern over duplication of resources with EOCs if SLFCs were required to be all-hazards.[99]

E. AREAS OF OPPORTUNITY

Because the discussion surrounding the need for and level of coordination between EM and the IC is a fairly new debate and dominated by government documents heavy in rhetoric ("intelligence coordination is a cornerstone of the HS mission"),[100] many issues remain unconsidered and unresolved as evidenced by substantial gaps in literary discourse. For starters, there is a lack of adequate research or clarity on the role of the federal government in dictating the parameters of any relationship that could, or should, exist. While the nation's foremost EM agency, FEMA, was moved after September 2001 under DHS to "improve coordination and delivery of services after a natural disaster or terrorist attack,"[101] DHS's own Intelligence Enterprise does not

96 DHS-DOJ, CPG 502, 20.

97 DHS-OIG, Relationships, 8.

98 DHS-DOJ, CPG 502, 21.

99 DHS-OIG, Relationships, 9.

100 Kiki Caruson, Mission Impossible? 18.

101 W. David Stephenson, and Eric Bonabeau, "Expecting the Unexpected: The Need for a Networked Terrorism and Disaster Response Strategy" Homeland Security Affairs III, no. 1 (February 2007), 1.

include FEMA amongst their operational components, an omission that is not clearly explained in written form.[102] DHS has made strides recently in acknowledging this deficiency, primarily in their EOC-SLFC guidance. DHS has even gone so far as to pledge support to "continue to develop mechanisms to more effectively identify opportunities to collaborate to include the Fire Service, Public Health, and Emergency Management."[103]

The literature reviewed for this thesis was also surprisingly thin on real-world examples of collaborative efforts, including best practices. Despite the generally accepted notion that a relationship *could* exist and *could* be mutually beneficial, most examples that were given were one-sided and of such a small scale that they could be written off to coincidence. If the relationship *should* exist and *is* beneficial, surely a more robust set of examples and best practices should be available. Although there is a chance that this relationship is still in its infancy and thus examples are forthcoming, a lack of concrete examples betrays the suggested importance of a link. A discussion of the strengths and weaknesses of each community and direct lessons each could learn from the other would be helpful in advancing the concept.

A final glaring omission from the literature was a discussion on tried and true methods for information collection, analysis, and dissemination that could be applicable to and functional for EM. With some minimal effort, the application of the intelligence cycle to the EM process can be developed and followed. Part of the challenge that exists in establishing common ground between EM and the IC, and more specifically EOCs and SLFCs, exists in semantics; however, the remainder of the translation will require some effort. For instance, the process of analysis is clearly defined and implemented in the IC community; the same cannot be said of the EM community. Beyond semantics, a shift in

---

[102] Mark A. Randol, "The Department of Homeland Security Intelligence Enterprise," 3.

[103] DHS, Interaction with Fusion Centers, 9.

culture will be required to support the all-hazards community and concept from "need-to-know" to "need-to-share."[104] It will require the IC to move to a "'responsibility to provide' (model) to ensure all members of the Community can retrieve the information they need and effectively support intelligence customers."[105]

F. LITERATURE REVIEW CONCLUSION

A review of the literature on the relationship between EM and the IC has revealed a substantial amount of discourse on the topic. However, a consensus has yet to be reached, and accordingly minimal progress has been made. With a concerted effort to further explore the strengths and benefits of a partnership, including standardization of roles and responsibilities, a more robust HS & EM enterprise could emerge. Chapters III-V will explore this concept more fully, and provide recommendations for just such a IC-EM collaborative model.

[104] Markle Foundation, "Nation at Risk," 2.

[105] ODNI, USIC Information Sharing Strategy, 5.

THIS PAGE INTENTIONALLY LEFT BLANK

III. NEED FOR AND ROLE OF AN EMERGENCY MANAGEMENT INTELLIGENCE PROCESS

> *Listen, S-2, the colonel said, I don't care about how many inches of rainfall to expect. I don't care about the percentage of lunar illumination. I don't want lots of facts and figures. Number one, I don't have time, and number two they don't do me any good. What I need is to know what it all means.*[106]

This chapter directly addresses the first two portions of the Research Question: is there a role for intelligence in EM, and if so what role could it play? The first part of this will be answered through a framework directly related to the all-hazards goals of collaboration, greater efficiency, and an improved HSE posture. The second portion will be addressed through FEMA's five mission areas, and provide examples of how a formalized intelligence process would function in EM.

A. EM INTELLIGENCE ROLE THROUGH ALL-HAZARDS FRAMEWORK

1. Collaboration

Collaboration without shared goals is frivolous and pointless; however, when there is a natural fit and something to be gained, collaboration is a worthwhile endeavor. Such a natural fit exists between the IC and EM communities, yet hasn't been explored to its fullest. Although an intelligence process within EM has far-reaching benefits solely within the EM field, the benefits of connecting resources, processes, and personnel from the multiple disciplines and agencies are greater in depth and quantity.

Collaboration, in order to be mutually beneficial, requires each partner to bring a capability to the table that creates the win-win situation. Additionally, it requires structure: "Assuming that agencies have an incentive to cooperate, they can only do so successfully with the proper infrastructure."[107] Because EM doesn't have an intelligence process, this collaboration infrastructure is crippled by a lack of common capability

---

106 United States Marine Corps, Marine Corp Doctrinal Publication 6: Command & Control, October 1996, 2.

107 Kiki Caruson, "Mission Impossible?" 5.

within the EM community. An EM intelligence process would allow for a common language and understanding that would enable both parties to communicate in an expeditious fashion and generate comprehensive products that all sides can understand, interpret and utilize. This includes information, such as assessments on CI/KR and Hazardous Materials reporting, that would be beneficial for the two to share and collaborate on.

Moving from theoretical to practical, as one of the primary end goals of an EM intelligence process is to foster greater collaboration between the EM and Intelligence communities, multi-discipline partnerships are key. Beginning with the SLFC-EOC relationship, the traditional EM-Fire-Police network is expanded to connect to resources such as the Terrorism Liaison Officer program and relevant information held within the SLFC walls. From there, this formalized process would allow the EM community to connect into broader communities, such as the National Guard, locally-based Federal resources, and Federal IC agencies when necessary. It would even expand into private industry, as an established intelligence process would only amplify the quantity and quality of information that is gathered through existing partnerships between EM and the private sector, processed by EM intelligence analysts, and shared amongst the broader IC. In a State such as Arizona, for example, where the security of our southern border is a multi-discipline, multi-jurisdiction, multi-sector concern, this strategy could help integrate the EM community and its resources into the fold to assist in developing solutions.

This collaboration amongst the HSE and expansion of the use of intelligence would also align with the National Intelligence Strategy of 2009. Three of the enterprise objectives presented in the Strategy are to 1) build familiarity of the IC and its capabilities; 2) expand partnerships; and 3) establish new partnerships.[108] EM, as an all-hazard partner, would be a logical partnership for the IC, and by establishing a formalized intelligence process better support the missions of the overall HSE.

[108] ODNI, National Intelligence Strategy, 11–12.

2. Resource Efficiency

A formalized intelligence process would also help the all-hazards approach in creating a more efficient HSE. Currently, duplications exist in equipment and personnel who are tasked with identical roles and responsibilities in all phases of an incident, but are siloed within their respective communities. By incrementally increasing the purview of an EM intelligence community, the HSE as a whole would be able to eliminate redundancy and increase efficiency. As an example, threat assessments are currently conducted on Critical Infrastructure by the IC for terrorist events; assessing them for vulnerability to floods, earthquakes, or tornadoes might have substantial overlap, and could therefore be conducted by one similar sized team with representatives from EM and the IC, rather than two separate and distinct teams. Similar overlaps occur in the collection and analysis of data for tactical purposes (i.e., routes of ingress/egress, damages post-event, etc.). There are obviously areas of specialty, as well, that do not necessitate a complete integration of the EM community and IC. However, in those areas where resources overlap, it makes sense to collaborate and share the tasking and resulting intelligence to maximize resource efficiency.

Greater efficiency could also result from an EM intelligence process that aided the resource allocation process. This is particularly evident at the State level, where EOCs and SLFCs provide support to the same agencies and departments, and have the ability to coordinate or request many of the same resources. In these instances, "decisions on operational priorities and resource allocations (often) depend on receiving tailored threat judgments from intelligence analysts."[109] Without an equivalent capability within EM, there is no voice to advocate on behalf of EM needs in a manner that adheres to objective criteria and an "apples-to-apples" measurement. Instead, the allocation is left to the IC, who may or may not have a solid understanding of the EM need to make an informed, comprehensive. An intelligence process within EM levels the playing field and enables greater efficiency in resource allocation. This ability to conduct a standardized risk assessment capable of examining and comparing dissimilar events (such as Hazardous

[109] John Baker, "Risk Analysis and Intelligence Communities Collaborative Framework," 11.

Materials transportation, earthquakes and terrorism hazards) illustrates a "common framework that a decision-maker can use to compare risks threatening a region."[110] From there, decision-makers can make well informed decisions and establish priorities for both personnel and resources. This capability currently does not exist.

Finally, efficiency could also be realized in the dramatic reduction of information decision-makers are presented with during both steady state and EOC activations. With the inclusion of Intelligence and Information Sharing as a core capability within the NPG,[111] DHS has recognized the importance of information sharing amongst the all-hazards community, and also that there is a need to compartmentalize and pare down the information and intelligence that a practitioner is seeing. With information flowing into the EOC from all angles, an intelligence process is needed to whittle that information down to a product that allows for efficient review and decision-making. This is especially problematic for the IC and EM communities when it comes to comprehensive threat assessments for high-ranking officials. "Some threats, such as terrorism, are new to governors but familiar to intelligence officers, but most of the threats facing a governor—blackouts, floods, hurricanes—are familiar to (governors) but new to intelligence officers."[112] In order to develop a single, integrated assessment, EM must have an ability to generate an intelligence product that can be submitted alongside the IC's in order to support efficient decision-making.

3. Posture of EM

A well-defined, formalized intelligence process within EM would also allow for a greater proactive posture in preparing and mitigating for incidents. Rather than focusing on response capabilities, an intelligence process would give decision-makers the necessary analysis required to make resource allocations and establish priorities that would swing the focus to more preventative measures. Although planning is a standard

---

[110] Mark D. Abkowitz, and Samrat Chatterjee (2012), "Regional Disaster Risk: Assessment and Mitigation Concepts in an All-Hazards Context," Journal of Homeland Security and Emergency Management, 9 (1, Article 15), 10.

[111] Federal Emergency Management Agency, *Mission Areas*, http://www.fema.gov/mission-areas.

[112] Dr. James Steiner, "Needed: State-level, Integrated Intelligence Enterprises," 3.

across the EM community, the planning process alone does not translate into preparedness. For example, in a survey conducted of counties nationwide, 90% of counties have an emergency operations plan, yet only 42% felt that their agency was adequately prepared for a disaster.[113] Plans alone are insufficient for developing and maintaining a proactive approach to preparedness for disasters.

Nowhere is our current reactive posture greater exemplified than in federal spending for preparedness vs. recovery activities. In Federal fiscal year 2013, State and local and first responder grants received about $2.5 billion;[114] these grants are spread amongst FEMA's five mission areas, but would ideally constitute the majority of funds used for proactive posturing. However, a 2009 study of the allocation of these funds by state and local agencies showed the distribution to be 14.1% on Prevention, 13.2% on Protection, 32.8% on Response, .6% on Recovery, and 39.3% on developing a capability that spanned all four areas.[115] Thus, the majority of these funds are indeed spent on reactive measures, not a proactive posturing.

In contrast, $7 billion was allocated to the Disaster Relief Fund (DRF) in FY2013[116], the overwhelming majority of which goes towards Recovery efforts, a portion to Response activities, and a minimal amount to mitigation. For example, the to-date totals for DRF allocations to Hurricane Sandy show that the total funding designated to the overall relief efforts is $8.4 billion. Of that, the total currently designated for mitigation is $111 million,[117] or 1.3% of the total allocation. Again, the reactive posture of our current EM community is reflected in these expenditures.

---

113 Wes Clarke, "Emergency Management in County Government: A National Survey," National Center for the Study of Counties, University of Georgia (August 2006), 16–17.

114 Mickey McCarter, "Interoperable Communications Under FY2013 Consolidated Spending, Appropriations Consistent with 2012," Homeland Security Today, March 29, 2013.

115 Federal Emergency Management Agency, FEMA GPD Grant Program Accomplishments Report, May 2009, 7.

116 Ibid., 1.

117 Federal Emergency Management Agency, Disaster Relief Fund: Monthly Report Through June 30, 2013, published July 5, 2013, 11.

The foundation for a proactive posture exists in high-quality data sets and models for assessing threat and vulnerability, as well as partnerships[118] with subject matter experts from FEMA, the U.S. Army Corps of Engineers (USACE), the National Weather Service, U.S. Geological Survey, the Department of Interior, the U.S. Forest Service, and many others. However, without a formalized iterative intelligence process for EM, these partnerships are not utilized to their fullest capacity, and proactive measures aren't at the forefront of EM priorities. The data and resources exist; the intelligence process necessary to convert these into products and support decision-makers does not. Integrated with intelligence from outside partners, conclusions drawn from the EM intelligence community would be a substantial asset in determining preparedness priorities.[119]

B. EM INTELLIGNECE ROLE THROUGH FEMA MISSION AREAS FRAMEWORK

If the EM community were to implement a process for intelligence gathering, analysis, and dissemination, what role would it play within EM and the all-hazards community at large? The NPG established five mission areas (prevention, protection, mitigation, response, and recovery)[120] that set the national standard for federal, state, local, and tribal EM programs. As such, any intelligence process that would be considered for the EM community would be most readily integrated if it fit within this mission area framework and augmented the 31 core capabilities within each.[121] Of these 31, the core capabilities of Planning, Public Information and Warning, and Operational Coordination span all five mission areas, and are directly relevant to EM responsibilities. The following analysis shows how such an EM intelligence process fits well within each mission area, including the core capabilities, and provides a real-world example where intelligence was, or could have been, utilized to bolster EM's current capabilities.

---

118 David P. Jackson, "Intelligence-Led Risk Management for Homeland Security," 21.

119 U.S. Congress' Local, State, Tribal and Federal Preparedness Task Force, "Perspectives on Preparedness: Taking Stock Since 9/11, September 2010, 49.

120 Federal Emergency Management Agency, *National Preparedness Goal*, http://www.fema.gov/national-preparedness-goal.

121 FEMA, *Mission Areas*.

1. Prevention

The Prevention mission area "comprises the capabilities necessary to avoid, prevent, or stop"[122] an act that threatens the safety of UC citizens or critical infrastructure. Although the prevention mission is mainly focused on the prevention of terrorist acts, the proliferation of all-hazards has softened this to include prevention of losses due to natural disasters. The prevention mission includes an Intelligence and Information Sharing core capability intended to bolster and support the all-hazards community's ability to collect and share key information and analysis across impacted partners.

An intelligence process for EM would primarily be used within the prevention mission for assessing the risk of an event that could potentially occur. These risk assessments could span specific impacts to key facilities/areas for a specific event, or include broader topics such as climate change, changing demographics within a target location, or the interdependency of systems within a geographic location (i.e., water/electrical systems).[123] With this intelligence in hand, planning could either consider preventative measures when possible, or assess their own capability to respond to such an event and prepare measures to address anything that is beyond their ability to handle.[124] Intelligence also provides situational awareness, or "the process of recognizing a threat at an early stage and taking measures to avoid it."[125] Situational awareness according to such a definition closely mirrors the goal of the prevention mission, and can provide adequate warning to implement preventative measures.

a. Prevention Exampl—Hurricane Sandy

A prime example of the effective use of intelligence to support the prevention mission recently came to light in the wake of 2012's Hurricane Sandy that devastated the eastern coast of the United States. As the storm hit shore, the community

---

122 Ibid.

123 U.S. Congress Preparedness Task Force, 34–35.

124 FEMA, Intelligence/Investigations, 2.

125 Fred Burton & Scott Stewart, "Threats, Situational Awareness, and Perspective," STRATFOR Global Intelligence Security Weekly, August 22, 2007.

of Stamford, Connecticut, sat comfortably behind a seventeen-foot storm wall that had been activated and raised from the sea floor[126] two days prior in response to reports that a storm surge was imminent. The wall had been constructed by the USACE in 1969, and helped prevent about $25 million in damage to businesses and homes during the Sandy event.[127] The original cost of construction was $15 million, but has been utilized in hundreds of storms and tidal surges in the past forty-four years, preventing much more in response and recovery costs. In light of the Hurricane Irene and Sandy events, calls have been made for a feasibility study to be completed by the USACE[128] (in conjunction with scientists and engineers familiar with the concept) to see if additional walls could be completed in other vulnerable areas of the eastern seaboard. This type of prevention effort would not have been possible without a thorough process of inquiry and informed decision-making that was based on collaboration of multiple disciplines and agencies. This decision-making depended on information and analysis—intelligence—and similar successes could be achieved through replicating this process.

2. Protection

The Protection mission area addresses the "the capabilities necessary to secure the homeland against acts of terrorism and manmade, or natural disasters."[129] The Protection area is primarily concerned with physical and technological security measures that reduce vulnerability and accessibility to CI/KR. Although this mission has the least overlap with the EM community, the core capabilities of Physical Protective Measures and Risk Management are areas prime for collaborative opportunities with the IC. The Protection mission area includes an Intelligence and Information Sharing core capability, where an EM intelligence process could integrate into and support the overall mission.

---

126 Mireya Navarro, "Weighing Sea Barriers as Protection for New York," *New York Times*, November 7, 2012.

127 Ibid.

128 Ibid.

129 Ibid.

a. Protection Example–Hurricane Katrina Flood Maps

Although the lack of a formalized intelligence process often impacts critical infrastructure and key resources, it can also lead to an uniformed policy decision that greatly impacts the EM community and the tax-paying citizen. One such example from the Protection mission area occurred in Louisiana parishes impacted by Hurricane Katrina in 2005. As part of the multi-year recovery efforts, FEMA published preliminary flood maps used in determining risk in areas with non-federal systems.[130] However, when they were published maps contained errors and failed to incorporate local flood protection measures such as "non-accredited levees and pump stations that were promised to be part of the formula creating preliminary maps."[131] In the community, the issuance of these maps caused "heightened anxiety"[132] for residents concerned that the findings in these maps could affect their eligibility or premiums for the National Flood Insurance Program. On a broader scale, though, the proliferation throughout the federal EM system of maps that failed to indicate or consider localized protection measures could have devastating consequences. The lack of foresight to include these in official maps, as well as the message it would communicate to the general public in the impacted area, could had been resolved with a more careful analysis.

3. Mitigation

The prevention and protection missions are intended to eliminate the threat or effects of a terrorist attack or natural disaster; Mitigation efforts comprise "the capabilities necessary to reduce the loss of life and property by lessening the impact"[133] of an inevitable disaster. DHS and FEMA recognize that some disasters are unavoidable (i.e., natural disasters), and therefore include as part of their overall mission the goal of reducing the impact of incidences that do occur.[134] The Mitigation mission area is where

---

130 Andrew Shaw, "FEMA Announces Program Analyzing Non-federal Levees After Criticism from Vitter, Parish Presidents," The Times-Picayune, July 12, 2013.

131 Ibid.

132 Ibid.

133 FEMA, *Mission Areas*.

134 William Waugh, "Terrorism and the All-Hazards Model," paper presented on the IDS Emergency Management On-Line Conference, June 28–July 16, 2004, 3.

the majority of EM's proactive measures take place, as vulnerabilities are identified and addressed through various means of reducing said vulnerabilities. The savings recognized by these measures are not only monetary, but also in both an increased public safety and corresponding first responder safety. An EM intelligence process would directly support the core capabilities of Community Resilience, Long-Term Vulnerability Reduction, Risk and Disaster Resilience, and Threat and Hazard Identification. Through the formalized process of collection, analysis, and generation of intelligence, areas of concern can be identified and decision makers charged with implementing mitigation strategies can determine priorities accordingly.

a. Mitigation Example–Post-Schultz Fire Flooding

Numerous studies have been conducted over the years showing the beneficial impacts of mitigation efforts. One such study was conducted on the costs associated with Arizona's Schultz Fire and subsequent Post-Fire Flooding that caused significant damage to private and public property in 2010. The Schultz Fire burned over 15,000 acres in a heavily sloped area, and was followed shortly thereafter by heavy seasonal monsoon rains. Although efforts were made to put mitigation measures in place, the community was largely overwhelmed and underprepared for the flooding off the burned slopes. Through a comprehensive survey of both public and private sources, the report concluded that "by treating a significant portion of the Schultz Fire imprint with an investment of $15 million could have greatly reduced the cost of the Schultz Fire and avoided the damage and loss of life associated with post-fire flooding that is now conservatively estimated to be between $133 and $147 million."[135] The damage to infrastructure could have been substantially mitigated if the problem was addressed immediately through a formalized process. Additionally, if the problem was identified and disseminated as a stronger warning to the public through channels established as part of an intelligence process, the loss of life may also have been mitigated.

[135] Thomas Combrink, Cheryl Cothran, Wayne Fox, Jeff Peterson, and Gary Snider, "A Full Cost Accounting of the 2010 Schultz Fire," Northern Arizona University Ecological Restoration Institute, May 2013, 22.

4. Response

The Response mission area encompasses "the capabilities necessary to save lives, protect property and the environment, and meet basic human needs after an incident has occurred."[136] Response operations go beyond lights and sirens, and include transportation, environmental, health, and mass care considerations. These non-tactical decisions fall under the purview of EM, and an intelligence process within EM could greatly expedite the decision making process for these key issues that affect life and safety both during and immediately following an incident. During the ongoing event, the EOC is a key focal point for information sharing and gathering, as it provides a "structure for needed support for executive decision making."[137] Information alone is not adequate, however, as the volumes of information that flow into an EOC need to be collected, analyzed, and shared to the right people in a timely fashion[138] to support these decision-making processes.

Decisions during the response phase typically fall into the tactical or operational levels, although they could simultaneously be formed for long-term strategic goals. From a tactical perspective, receiving intelligence updates during an incident helps, "ascertain changes in the operational environment and make appropriate tactical and safety decisions."[139] This intelligence would provide responders with key information that isn't readily available in the field, such as near-term weather conditions, location of key infrastructure, and prioritized impact areas. The Response mission includes the core capabilities of Critical Transportation, Environmental Response/Health and Safety, Fatality Management Services, Mass Care Services, Public and Private Services and Resources, Public Health and Medical Services, Situational Assessment, all of which the EM community plays a primary or support role in addressing.

---

136 FEMA, *Mission Areas*.

137 Gregory T. Brunelle, "Achieving Shared Situational Awareness During Steady-State Operations in New York State: A Model for Success," (Master's Thesis, Naval Postgraduate School, 2010), 2.

138 Fahem Kebair and Frederic Serin, "Towards an Intelligent System for Risk Prevention and Emergency Management," proceedings from the 5th International ISCRAM Conference – Washington, DC, USA, May 2008, 527.

139 Keeley Townsend, John P. Sullivan, Thomas Monahan, & and John Donnelly, "Intelligence-led Mitigation," 6–7.

a. Response Examples–North Carolina Division of Emergency Management and Novato Fire

Two examples of Response actions that were aided through the use of intelligence are warranted showcasing two of the IC's newer capabilities: Geospatial Intelligence (GEOINT) from Geographic Information Systems (GIS), and Open Source Intelligence (OSINT) from Social Media. GIS is widely used in EOCs and provides visual displays of information that can range from weather conditions to the location of deployed resources.[140] The North Carolina Division of EM utilized GIS capabilities as a part of their response to flooding caused by Tropical Storm Nicole in September of 2010. Once the EOC was activated, North Carolina Division of EM utilized their "intelligence map viewer to display real-time National Oceanic and Atmospheric Association weather alerts feeds pertaining to the weather conditions including rain fall totals and flooding numbers."[141] From a utilization of intelligence in the response phase, the interactive nature of the maps provided North Carolina Division of EM leadership with accurate and updated information[142] at any point in the response effort without having to comb through piles of data. The data was already collected, validated, and processed into a working intelligence product that was able to incorporate new information as it was gathered.

A second example of the use of intelligence during Response operations includes the use of Social Media during an active incident. The following timeline from the Fourmile Canyon Fire in Boulder, Colorado shows the speed and role of social media for EM operations[143]:

- 10:07AM–Fire begins in wildland-urban interface near Boulder
- 11:34AM–An unaffiliated citizen begins a Twitter feed related to the fire

---

140 North Carolina Division of Emergency Management, "Situational Intelligence Maps Add Value During Emergencies," MEMO Publication 4 (Issue 11) November 2010, 1.

141 Ibid., 1.

142 Ibid.

143 Adapted from Eric D. Nickel, "Collective Intelligence in Emergency Management: Social Media's Emerging Role in the Emergency Operations Center, " Novato Fire District, www.usfa.fema.gov/pdf/efop/efo45101.pdf, 24–26.

- 11:35AM–A second unaffiliated citizen begins Tweeting fire dispatch info
- 1:17PM–A third unaffiliated citizen begins uploading fire movement and public safety information onto Google Maps
- 2:32PM–The City of Boulder begins posting information on their Department Facebook site
- 3:23–5:41PM–The Boulder County Sheriff's Office initiates the use of their Reverse 911 calling system; the software fails and none of the calls go through. Messages are pushed out to the public through various methods pointing people to the evacuation information being posted on the Office's website and social media sites.

The use of social media was a valuable means as both a collection point and a source to disseminate incident information out to the community. Its real-time nature and low cost to operate and monitor make it a feasible tool to capitalize on for OSINT. A formalized EM intelligence process would help expedite the processing of such information into a useable product, and greatly enhance response operations.

5. Recovery

The Recovery mission area spans "the core capabilities necessary to assist communities affected by an incident to recover effectively."[144] Recovery efforts from a disaster can vary based on scope and severity of the damage caused by the event. However, the challenge in all recovery efforts is to determine the best course of action given the limited resources, and whether or not damaged infrastructure (including homes) should be repaired to its pre-disaster condition or potentially relocated out of harms way. These decisions, spanning from tactical to strategic, would be supported by intelligence gathered pre-, during, and post-event. Examples of intelligence-fed recovery decisions would be: ideal locations for shelters & service centers, routes for ingress/egress for humanitarian aid,[145] and broader social and economic concerns (key cultural/historical sites). It would also include the security concerns that disasters present (i.e., registered

144 FEMA, *Mission Areas*.

145 Peter R. J. Trim, "An Integrative Approach to Disaster Management and Planning," Disaster Prevention and Management 13 (Number 3), 2004, 222.

sexual offenders in shelters and short-term housing), which could be vastly improved through the sharing of intelligence between the IC and EM community. The Recovery mission spans the Economic Recovery, Health and Social Services, Housing, Infrastructure Systems, and Natural and Cultural Resources core capabilities, all of which EM plays a role in supporting or coordinating.

a. Recovery Example–Whole Community

The recovery mission could be supported by a formalized intelligence through which the pace and scope of efforts are determined. The communities of Northwood, North Dakota, and Greensburg, Kansas, had several key decisions to make in the aftermath of devastating tornadoes.[146] Determining priorities amongst the damage (i.e., homes, businesses, municipal buildings, schools, recreation facilities), deciding how best to incorporate mitigation efforts, and then bringing the necessary resources to the table is a daunting task. However, through the use of a process of inquiry akin to the intelligence cycle, information was collected, vetted, analyzed, and a course ahead was determined.[147] The process was successful due not only to thorough and deliberate intelligence-fed planning, but also because of the substantial community involvement.

[146] Christine Becker, "Disaster Recovery: A Local Government Responsibility," ICMA Public Management Magazine 91 (Number 2) March 2009, http://webapps.icma.org/pm/9102/.

[147] Ibid.

IV. INTELLIGENCE MODELS

In order for the EM community to be able to integrate with the IC in a manner that most effectively supports the all-hazards concept, it is imperative that EM learns the premises of intelligence to establish a common understanding and language. Although intelligence is fundamentally a "information + analysis" equation, the methods by which it is gathered and utilized varies between military, federal, and local members of the IC. Because these methods are well refined and have proven their worth over years of use, it behooves EM to consider aspects of each to develop a model that best suits the mission and responsibility of EM. This chapter will thus review three intelligence processes utilized by different members of the IC, representing two levels of government and three distinct mission areas. Each section will begin with an overview of the intelligence process as practiced by the agency/agencies in question, and conclude with a brief summary of the transferrable concepts to EM. The transferrable concepts will form the basis for the EM Model presented in Chapter V and include an expanded analysis of their utility and application.

A. FEDERAL BUREAU OF INVESTIGATION–INTELLIGENCE CYCLE

The United States FBI is an "intelligence-driven and a threat-focused national security organization with both intelligence and law enforcement responsibilities."[148] Although it functions on a global basis, the FBI is highly active domestically and is a key point of interaction between the local law enforcement community and the national IC. In addition to their well-documented intelligence process, this connection to both the national and local intelligence community (including a lead role in SLFCs) makes them a good subject for this research study. A review of the FBI's intelligence process is a good step towards establishing common understanding and language with a primary player in domestic intelligence.

[148] Federal Bureau of Investigation, *Quick Facts*, http://www.fbi.gov/about-us/quick-facts.

The FBI's intelligence process follows a broad process of inquiry, production, and dissemination termed the "Intelligence Cycle." (Figure 1) The cycle includes six steps, is not necessarily linear in fashion, and is indicative that the process continues on an ongoing basis. This cycle is the process by which the FBI actively collaborates with both internal external partners to develop raw data and information into finished products for use in both tactical and strategic operations.[149]

Figure 1. FBI's Intelligence Cycle[150]

1. The Six Steps of the FBI's Intelligence Cycle

a. Step One–Requirements

The first step of the FBI's intelligence cycle is the establishment of identified information needs (requirements) that can be either generic or specific in nature. These requirements are established by the ODNI according to guidance from the president, national homeland security advisors, the attorney general, and internally from FBI leadership.[151] This step essentially defines the "what" of the inquiry; what the

[149] FBI, *Intelligence Cycle*.

[150] Ibid.

[151] Ibid.

subject of the inquiry is and what types of information are required for the policy maker who will be responsible for the ultimate decision on course of action. It is high level, and outlines overarching parameters including longevity of study.

A key part of this step is deciding what type of analysis is being requested. The FBI (and IC in general) generates intelligence that falls into three categories:

- Current Analysis–time-sensitive intelligence reporting, usually concerning a recent event or action on newly discovered information.[152] It addresses an issue of immediate concern, and typically requires quick movement through the intelligence cycle for action on a short timeline.
- Trend Analysis–this is the mid-range intelligence requirement. It requires information on an event or series of events, and includes background information, an assessment of the reliability of the intelligence, and information on similar events to give the decision maker context.[153]
- Long-Term Assessments–this requirement allows for cultivation of information and comprehensive research on on-going issues, future trends or developments, or topics in a much broader context.[154] Although these assessments can be done on a short timeline, they are typically given a longer time line to allow for more comprehensive intelligence gathering.

b. Step Two–Planning and Direction

Once the requirement for the intelligence analysis is established and the parameters are clear, this step develops the methods of inquiry and the management of the entire effort.[155] Step one establishes the framework; Step two fills in the details with specific collection techniques, time windows for individual deliverables, and resources that will be essential to develop the final product.

---

[152] Office of the Director of National Intelligence, "National Intelligence: A Consumers' Guide," (2009), 14.

[153] Ibid., 15.

[154] Ibid.

[155] FBI, *Intelligence Cycle*.

A key aspect of Step two is determining what type of intelligence product is most appropriate given the requirement, as well as who is best suited to conduct the intelligence collection and analysis (Steps three and four). The National Counterterrorism Center's ITACG, which includes the FBI, categorizes finished intelligence products into five categories[156]:

- Current–day-to-day events and new developments; short-term
- Estimative–similar to the long-term assessment described above, these includes multiple scenarios and probabilities of occurrence
- Warning–identifying or forecasting events that are likely to occur based on current information and trends; includes low probability/high impact events[157]
- Research–supports both 1) and 2), but includes a much broader range of source material
- Scientific and Technical–requires the inclusion of technical experts who can assess the information from a scientific or technological perspective (i.e., Chemical, Biological, Radiological, Nuclear, and Explosion events or capabilities).

Once the majority of the planning and direction phase is fleshed out, resources are then put in place to begin the actual intelligence gathering process.

Of Note: Some researchers on the topic of intelligence combine Steps One and Two into a single step and show the sixth step as "continuous evaluation."[158] For purposes of this study, the process as articulated by the FBI is more appropriate and thus utilized. The sole reason for mention of this alternative process is to illustrate that although the naming convention utilized by other members of the USIC may be different, their conceptual scope is identical.

c. Step Three–Collection

The Collection step is where the gathering of raw information based on the parameters established in Steps One and Two begins. The collection can draw upon

156 Office of the Director for National Intelligence (Coordinating Agency), "Intelligence Guide for First Responders," (2nd Edition, March 2011), 24–25.

157 Ibid., 25.

158 David M. Keithly, "Intelligence Fundamentals," in *Homeland Security and Intelligence*, ed. Keith Gregory Logan (Santa Barbara, CA: Praeger Security International, 2010), 44.

multiple sources as dictated both by the direction of management and needs of the study. The ODNI categorizes these sources into the following disciplines (INTs):

- Signals Intelligence (SIGINT)–intelligence collected in this discipline comes from the interception of communications from or to the subject of inquiry, regardless of the method of communication. This discipline includes communications intelligence (COMINT), electronic intelligence (ELINT), and foreign instrumentation signals intelligence (FSINT).[159] The U.S. National Security Agency is the primary federal agency responsible for SIGINT collection and cultivation.
- Imagery Intelligence (IMINT)–IMINT comes from photographs, radar, or any other method utilized to gain a visual representation of the subject of study. It is gathered primarily from surveillance and satellite imagery, but can also be gathered from more advanced technological means, such as electro-optics.[160] The U.S. National Geospatial-Intelligence Agency is the primary federal agency responsible for IMINT collection and cultivation.
- Measurement and Signature Intelligence (MASINT)–MASINT is "technically derived intelligence"[161] that comes from sources other than IMINT or SIGINT. This discipline is highly scientific, and includes such fields of expertise as seismology, materials engineering, and nuclear/chemical/environmental studies. The collection of air, water, and soil samples would be examples of intelligence that is collected in MASINT. The U.S. Defense Intelligence Agency houses the primary federal directorate responsible for MASINT collection and cultivation.
- Human Intelligence (HUMINT)–this discipline includes intelligence that is gathered from human sources, whether overtly or clandestinely. HUMINT is collected through interviews, documents, surveillance, photographs of human subjects, or diplomatic methods.[162] The Central Intelligence Agency is the federal agency most often associated with HUMINT collection.
- Open-Source Intelligence (OSINT)–OSINT is "publicly available information appearing in print or electronic form including radio, television, newspapers, and the Internet."[163] With the advent and

[159] Office of the Director for National Intelligence, *ODNI FAQ: About the Intelligence Community*, http://www.dni.gov/index.php/about/faq?start=2.

[160] Ibid.

[161] Ibid.

[162] Ibid.

[163] Ibid.

rapid proliferation of social media in the past decade, OSINT has become a wealth of information that is freely and readily acquired, although it does require a greater degree of validation. As such, OSINT is used by most agencies within the IC, although the lead agencies for U.S. OSINT are the DNI's Open Source Center and the National Air and Space Intelligence Center.[164]

- Geospatial Intelligence (GEOINT)–GEOINT is the "analysis and visual representation of security related activities on the earth."[165] It is closely related to IMINT, and is even represented as a part of IMINT in some discussions of the disciplines.[166] Recent innovations in GEOINT allows for greater capabilities than simple 2-D images; terrain maps and 3-D depictions are now commonplace.
- Although the FBI does not utilize all of these disciplines for each product it develops, it has these capabilities either in house or at their disposal from a partner agency.

d. Step Four–Processing and Exploitation

Step four in the FBI's intelligence process organizes the raw data and identifies additional needs for information. The intent is to convert the information into a form that will enable analysts to use it, whether through databases or non-automated means. This step includes the use of methods like decryption, language translations, and data reduction.[167] If gaps in the information are detected through preliminary evaluation, a loop back to Step Three may be warranted either prior to or concurrently with a move to Step Five. This step is critical in situations where the information is voluminous, as data can be grouped or culled down to the essentials for the analysts, and subsequently the decision makers.

e. Step Five–Analysis and Production

Step five is the hinge point of the entire process, where information is converted into intelligence. Data that is processed as part of Step Four is given to an

---

164 Ibid.

165 Ibid.

166 David M. Keithly, "Intelligence Fundamentals," 51.

167 FBI, *Intelligence Cycle*.

analyst where a four–step sub-step process[168] takes place to synthesize the information into a final product:

- Evaluation–information is appraised for credibility, relevance, and usefulness
- Analysis–identifying key facts and relationships within the information
- Integration–assembling the analysis into a single, cohesive picture
- Interpretation–determining the significance of the picture generated in the integration step and postulating implications

The final product provides both context and implications for review by the ultimate decision makers.

As part of this step, it is important to clarify the limitations of intelligence products in order to manage the expectations of consumer. Intelligence can provide warnings of potential threats, insight into key current events, situational awareness, and support to long-term strategic decision-making efforts.[169] It cannot predict the future, although it can provide solid assessments of likely scenarios[170] given the intelligence. This is crucial for policy makers to understand, as the intelligence in some cases can be unclear or inconclusive.

f. Step 6–Dissemination

The final step in the FBI's intelligence cycle is the distribution of the product to the policy makers who initiated the request, as well as others within the HSE whose mission includes the subject matter if warranted. The FBI publishes their products in three standard formats: Intelligence Information Reports, Intelligence Bulletins, and Intelligence Assessments.[171] Outside of the FBI, other IC agencies' intelligence products include Threat Assessments,[172] memorandums, technical analyses, research studies, and

---

168 David M. Keithly, "Intelligence Fundamentals,"46–47.

169 ODNI, *Consumer's Guide*, 10.

170 Ibid., 11.

171 FBI, *Intelligence Cycle*.

172 ODNI, *Intelligence Guide*, 29.

situational reports.[173] These products vary in their scope of study, frequency of dissemination, and level of analysis, based on the needs identified in Step one.

2. Transferrable Concepts to EM

At its most basic level, the intelligence cycle utilized by the FBI is directly relevant to the EM community as a method of inquiry and analysis. Without any formalized or standardized method currently in use, gaps in information, validation, and analysis are inevitable. Although the requirements can be clear from a broad perspective, the expectations of the end-user may be unrealistic in both level of analysis and type of outcome. Establishing a formalized process, such as the one utilized by the FBI, allows for consistency in expectations and quality of products, as the parameters are determined at the outset. It also increases professionalism of the analyst who has a clearer picture of the resources at his/her disposal, and the process by which to go through to achieve the desired end product.

Additionally, although the categorization of methods of collection is of little benefit in and of itself, the cultivation of resources and partners within these categories could prove widely useful. The understanding of available sources of information greatly expedites the acquisition of key data that can help the decision-making process within the EM community. By adopting a system similar to the INTs, EM can develop relationships in these areas to rely on when an event requires information in these areas of expertise. These sources may also have intelligence products already developed, and with a common understanding and language, would be beneficial to EM in all phases of an event. A more comprehensive discussion of the use of INTs in EM is included in Chapter IV.

B. UNITED STATES ARMY–INTELLIGENCE PREPARATION OF THE BATTLESPACE

The Intelligence Preparation of the Battlespace (IPB) doctrine utilized by the United States Army is a "systematic, continuous process of analyzing the threat and the

[173] David M. Keithly, "Intelligence Fundamentals," 48.

environment."[174] Through a simple, repeatable four-step cycle, IPB helps prepare a set of operational objectives that support overarching missions.[175] IPB reduces uncertainty about threats,[176] provides situational awareness of the area of operations (AO), and provides essential information to the commander for purposes of planning courses of action (COA). It also aids in developing intelligence collection plans,[177] determining the allocation[178] and placement[179] of resources, and in synchronizing staff members to a common mission, and understanding of objectives.[180] As a point of reference, IPB relates to the second phase of the FBI's intelligence cycle, as it identifies "facts and assumptions about the environment and priority intelligence requirements."[181]

IPB is useful in both scalable and flexible, and is useful in multiple planning levels and scenarios. The U.S. Army's military intelligence (including IPB) has three levels:

- Tactical–focused on short-term actions (strikes); can be highly specific in scope[182]
- Operational–focused on larger scale endeavors (battles); considers environmental concerns to the AO such as enemy assets, terrain, weather, etc.[183]

---

174 Center for Army Lessons Learned, "Intelligence Preparation of the Battlefield," U.S. Army Training and Doctrine Command, Fort Leavenworth, KS, no. 96–12 (December 1996), I-1.

175 Carl Rhodes, Jeff Hagen, and Mark Westergren, "A Strategies-to-Tasks Framework for Planning and Executing Intelligence, Surveillance and Reconnaissance (ISR) Operations" Rand Corporation-Technical Report 434 (2007), 11.

176 Jin Kim and William Allard, "Intelligence Preparation of the Battlespace: A Methodology for Homeland Security Analysis" SAIS Review 28 (No. 1, Winter-Spring 2008), 76.

177 Jamison Jo Medby and Russell W. Glenn, "Street Smart: Intelligence Preparation of the Battlefield for Urban Operations," RAND Corporation, MR-1287 (2002), xiv.

178 Jin Kim and William Allard, "Intelligence Preparation of the Battlespace," 81.

179 Center for Army Lessons Learned, "Intelligence Preparation of the Battlefield," V-1.

180 Ibid., I-1.

181 Major Troy S. Thomas, "Beneath the Surface: Intelligence Preparation of the Battlespace for Counterterrorism," Center for Strategic Intelligence Research, Washington, DC (November 2004), 38.

182 Ibid., 38.

183 Ibid., 37–38.

- Strategic–long-term, comprehensive assessments of an enemy's overall "capabilities, capacities, and intentions,"[184] but not necessary at the time of war or conflict.

The IPB model is composed of four steps (Figure 2) each intended to be a part of a cyclical process. The first two phases look outside the organization to the environmental conditions of the intended AO; the second two phases focus on the anticipated enemy to "uncover sources of strengths and vulnerabilities."[185] The IPB process can be conducted by a team of analysts or a single trained individual; this entity dictates the collection of information and simultaneous analysis[186] to ensure it is delivered to the commander in an appropriate time frame. It also includes a feedback loop whereby all participants in the operation are trained in "casual observation skills and brief/debrief prior to and after each mission."[187] This ensures that prior assumptions are validated or negated and new information is constantly and readily available.

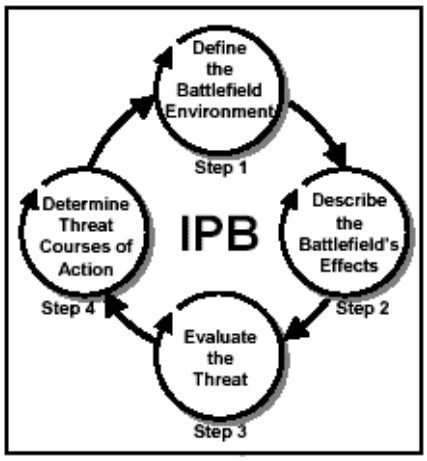

Figure 2. Intelligence Preparation of the Battlespace (IPB) Steps[188]

[184] Louis Liotti, "Military Intelligence," in Homeland Security and Intelligence, ed. Keith Gregory Logan (Santa Barbara, CA: Praeger Security International, 2010), 100.

[185] Ibid., 35.

[186] Center for Army Lessons Learned, "Intelligence Preparation of the Battlefield," IV-3.

[187] Office of the Chief of Naval Operations, "Domestic Disaster Relief Operations Planning," Department of the Navy Command TACMEMO 3–07.7–06 (May 2006), 68.

[188] Global Security.ORG, Urban Intelligence Preparation of the Battlefield, http://www.globalsecurity.org/military/library/policy/army/fm/3–06/appb.htm.

1. Four Steps of the IPB Process

a. Step One–Define the Battlefield Environment

The first step of IPB includes identifying characteristics of the anticipated battlespace environment,[189] including evaluating gaps in information and anticipated resource needs. This stage allows the analyst to determine what intelligence has already been gathered and what intelligence will need to be gathered in order to support decision-making. This is akin to situational awareness in that the goal is to develop a good operating picture complete with all the relevant information.

b. Step Two–Describe Battlefield Effects

The second step of IPB is where the majority of the true analysis occurs. With the information gathered from Step One, an analyst will then assess them for pertinence to the operation, as well as potential impacts for the anticipated time frame. This analysis traditionally concentrated on weather and terrain[190], as well as the capabilities of the enemy. It has since expanded to include logistical, economic, political, and social demographics.[191] This expansion was necessary as operations moved into a more urban environment,[192] as infrastructure and the movement of people during an evolving situation creates an added challenge to decision-makers.

A tool commonly utilized during this step of IPB is the assessment of the "OCOKA" factors of the AO. "OCOKA" includes Observation and fields of fire, Concealment and cover, Obstacles, Key terrain, and Avenues of approach.[193] Utilizing OCOKA provides the analyst with some common areas of concern and consideration for every mission, and acts as an intelligence checklist of sorts. It is most helpful in tactical

---

189 Center for Army Lessons Learned, "Intelligence Preparation of the Battlefield," I-2.

190 Ibid., I-2.

191 Lt. Col. Patrick Kelly, "Intelligence Support to Homeland Security,," 20.

192 Jamison Jo Medby and Russell W. Glenn, "Street Smart," 4.

193 Center for Army Lessons Learned, "Intelligence Preparation of the Battlefield," I-2.

operations,[194] but as with the rest of the IPB doctrine, is scalable to meet the needs of operational and strategic missions, as well.

c. Step Three–Evaluate the Threat

The focus in step three shifts to the enemy force (threat). Intelligence is gathered from as many sources as necessary to develop a robust picture of various aspects of the enemy. These include how the enemy conducts operations, high value targets in the enemy's possession,[195] as well as information pertaining to the size and capabilities of the enemy's force. This step, in the absence of the structure of IPB, would be more commonly referred to as the threat analysis.[196]

d. Step Four–Determine Threat Courses of Action

The final step in the IPB doctrine is developing a prioritized list of potential enemy (threat) movements that are both most likely and most dangerous to friendly forces.[197] The list should be as comprehensive as time permits; the detail of each potential enemy COA should follow this same criteria. Once the most likely enemy COA is identified, the ensuing collection strategy for the next iteration of the IPB within the event should reflect this decision.[198] The IPB cycle continues and builds another layer on top of the previous one, reflecting both previous decisions and new intelligence gathered from sensors.

2. Transferrable Concepts

Similar to the FBI model presented earlier, the IPB doctrine presents a high-level model that aids in identifying needed information, provides a framework for collecting targeted data, and ultimately a process to convert that into intelligence. The framework is cyclical, and is able to accommodate the ongoing input of new information into the cycle.

---

194 Jamison Jo Medby and Russell W. Glenn, "Street Smart," 67.

195 Center for Army Lessons Learned, "Intelligence Preparation of the Battlefield," I-3.

196 Major Troy S. Thomas, "Beneath the Surface," 36.

197 Center for Army Lessons Learned, "Intelligence Preparation of the Battlefield," I-4.

198 Ibid., I-4.

IPB also considers the threat's COA, helping the analyst to recommend the deployment of resources to the most probable area of engagement. All three of these aspects are helpful to EM, especially during an evolving event such a flood or hurricane. Their utility would be limited during a sudden event like an earthquake, but could be helpful in the mitigation efforts in establishing priorities for limited mitigation funds.

The OCOKA concept is also of interest, as again this offers the analyst a checklist of common considerations to review as part of their intelligence production. This includes training all field personnel in basic observation techniques to gather information pertinent to intelligence development. The OCOKA process would be helpful to response and recovery efforts, primarily in planning the entry of resources into an impacted area to address the immediate needs of the victims.

In addition to having transferrable intelligence concepts for the EM community, the military also has a role in domestic disaster response. The Defense Support to Civil Authorities mission includes "measures to foster mutual assistance and support between Department of Defense and civil government agencies in planning, preparation for, or in response to consequences of civil emergencies such as natural and man-made disasters."[199] During these operations, the development of situational awareness by Department of Defense operations adheres to the IPB process.[200] Because of this role in support of the all-hazards mission, it is wise to also establish a common understanding, language or awareness of the IPB process for greater military-EM collaboration.

C. INTELLIGENCE-LED POLICING

Intelligence-Led Policing (ILP) is a policing approach that utilizes data analysis and crime intelligence within a "objective, decision-making framework that facilitates crime and problem reduction, disruption and prevention through both strategic management and effective enforcement strategies.[201]" Through the use of this intelligence and analysis, law enforcement organizations can target areas of high criminal

199 Office of the Chief of Naval Operations, 1–4.

200 Ibid., 2–1.

201 Jerry Ratcliffe, *Intelligence-Led Policing* (Portland, OR: Willan Publishing, 2008), 6.

activity and allocate resources accordingly. This allows law enforcement to police "smarter"[202] with their current resources, rather than through increasing personnel and equipment.

ILP represents a progression from previous law enforcement strategies, as intelligence is now an integral part of the mission of the organization,[203] as opposed to the "undefined tangential activity as was too often the case in the past."[204] ILP is linked directly to the intelligence cycle, and provides a method for information to be converted to intelligence and subsequently disseminated to partners.[205] Because of this, ILP is useful in complex, multi-jurisdictional operations[206], particularly in the collaborative environment of SLFCs[207] where agencies can pool resources and information.

ILP is similar to the previous two models presented earlier, as it provides an intelligence function that aids decision-makers in the development of policies and strategies. It is also useful in providing "guidance on operational activities based on empirical evidence,"[208] which then drives operations[209] rather than the converse. ILP results in an "actionable intelligence product intended to aid law enforcement in developing tactical responses to threats and/or strategic planning to emerging or changing threats."[210] Ratcliffe describes it through a 3i Model: intelligence interpreting the

---

202 Jennifer Wood and Clifford Shearing, *Imagining Security*. (Cullompten, UK: Willan Publishing, 2007), 55.

203 David L. Carter, "Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies," U.S. Department of Justice Project #2003-CK-WX-0455 (November 2004), 41.

204 David L. Carter, "The Law Enforcement Intelligence Function: State, Local, and tribal Agencies," The FBI Law Enforcement Bulletin (June 1, 2005), 1.

205 Jerry Ratcliffe, *Intelligence-Led Policing*, 81.

206 David L. Carter, "The Law Enforcement Intelligence Function," 1.

207 Marilyn Peterson, "Intelligence-Led Policing: The New Intelligence Architecture," U.S. DOJ Bureau of Justice Assistance, NCJ 210681 (September 2005), 9.

208 David L. Carter, "The Law Enforcement Intelligence Function," 1.

209 Jerry Ratcliffe, *Intelligence-Led Policing*, 8.

210 David L. Carter and Jeremy Carter, "Intelligence Led Policing: Conceptual Considerations for Public Policy" Criminal Justice Policy Review, 20(3) (2009) 312.

environment and influencing decision-makers, who in turn impact the environment through actions (Figure 3).[211]

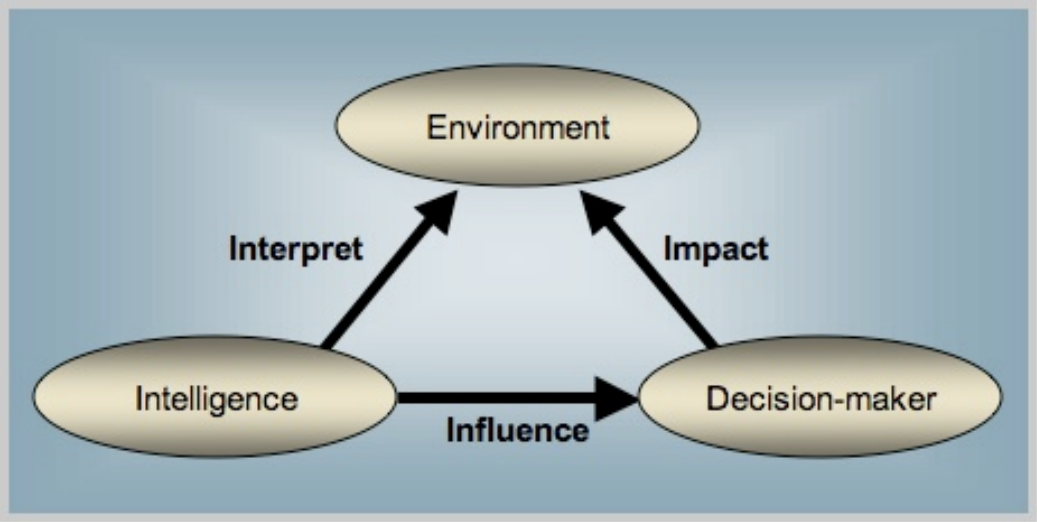

Figure 3. Ratcliffe's 3i Model of Intelligence-Led Policing.

ILP relies on three main tenets as part of the overarching strategy: two-way communications with the public and information management, scientific data analysis, and problem solving.[212] To effectively implement ILP on any scale, all three tenets must be utilized to produce the most comprehensive intelligence and support effective decision-making.

1. Intelligence-Led Policing Tenets

a. Tenet One–Two-way Communications and Information Management

Tenet One of ILP provides both the key raw data that will be utilized in the intelligence analysis, but also the means of dissemination once the data is refined and analyzed. ILP is dependent on information flow and feedback, regardless of whether it is crime analysis or intelligence analysis.[213] The two-way communication could be better

211 Jerry Ratcliffe, *Intelligence-Led Policing*, 110.

212 David L. Carter, "Law Enforcement Intelligence: A Guide," 41–42.

213 Ibid, 44.

stated as two sets of two-way communications as ILP engages both field officers and the public in dialogue.

ILP is driven by an information flow that comes from the "boots on the ground," line level employees[214] who are in the field and in the best position to make observations of the true state of affairs. Officers must be trained not only how to identify hallmarks of criminal enterprises or potential hotspots, but also to "regularly channel that information to the intelligence unit for input into the intelligence cycle for analysis."[215] Once the information has been submitted and analyzed through Tenets Two and Three, the ensuing intelligence is disseminated back to the field officers, completing the communications loop and creating a more informed police force.

The public also plays a big role in the success of ILP in their community. The process begins with community education on the threats that exist within their community, and the methods for identifying suspicious behavior.[216] Members of the community must also be made familiar with the "means of and processes for relaying observed (crime) data to the police officers and police organizations."[217] The data is then fed to the analysts, and the outcomes can be communicated back to the public through community meetings or community leaders in an effort to emphasize vigilance and create public awareness.[218]

b. Tenet Two–Scientific Data Analysis

With the information collected and corroborated through Tenet One, ILP relies heavily on scientific data and the utilization of technical processes for quality analysis.[219] An example of this is the CompStat program, which collects and processes "crime and disorder data…to produce crime maps, trends, and other analysis

---

214 Ibid., 44.

215 Ibid.

216 Ibid., 46.

217 Ibid., 44.

218 Ibid., 40.

219 Marilyn Peterson, "Intelligence-Led Policing," vii.

products."[220] The inputs are largely quantitative in nature (i.e., crime statistics within a geographic area, nature of arrests/interdictions, etc.), but the outputs given decision-makers basis for qualitative decisions. The focus of the outputs is identifying prolific and persistent offenders,[221] who are responsible for a majority of the crime, thereby warranting immediate attention. This scientific data then forms the hinge point[222] (similar to the FBI's Step Five) for the other two tenets, as information collected and products disseminated will be validated and refined through this analytical step.

c. Tenet Three– Problem-Solving

With the intelligence generated by Tenets One and Two, the impetus is then put on the decision-maker for how best to address the problems identified by the analysis. In addition to broad strategies for implementing tactics, operations and strategies, the ILP process is highly effective at providing an "objective basis for deciding priorities and resource allocation."[223] This gives ILP a more proactive posture,[224] as action is being taken to reduce or prevent crime from taking hold in a particular area, rather than simply responding to emergency calls as they occur.

At a multi-jurisdictional level, the intelligence received in this step also aids in the development of linkages[225] and connections with intelligence from multiple agencies. Criminal enterprises do not adhere to jurisdictional boundaries, so the effort to collaborate to gain information and perform joint operations in a cross-jurisdictional area is ideal. With the inclusion of federal level assets in the SLFCs (such as the FBI), this benefit is greatly expanded as intelligence is shared externally,[226] rather than cultivated with only in-house sources.

---

220 University of Maryland, "What is CompStat?" http://www.compstat.umd.edu/what_is_cs.php.

221 Jerry Ratcliffe, *Intelligence-Led Policing*, 8.

222 David L. Carter, "Law Enforcement Intelligence: A Guide," 40.

223 Jerry Ratcliffe, *Intelligence-Led Policing*, 4.

224 David L. Carter, "Law Enforcement Intelligence: A Guide," 1.

225 National Criminal Intelligence Service (UK), "National Intelligence Model," (2000), 14.

226 DOJ Bureau of Justice Assistance, "Reducing Crime Through Intelligence-Led Policing," U.S. Department of Justice Project #2008-DD-BX-K675 (2008), 2.

2. Transferrable Concepts

The use of data and metrics in ILP to establish and inform decision-making processes is directly relevant to the EM community. Using these scientifically validated intelligence products generated by ILP would "enhance understanding of the operational environment and enable (EM) to make informed decisions on appropriate preparedness, prevention, protection, response, and recovery actions to mitigate incidents."[227] By gathering information on previous disasters, including metrics on cost of recovery, resources can be allocated on a much more informed basis. EM could focus the limited resources and policy efforts on these "prolific and persistent offenders," and provide guidance to stakeholders on potential remedies.

The other intriguing transferrable concept from ILP is the role of the community in reducing their vulnerability to threats and engaging them in an active way. Rather than broadly targeting preparedness in a generic form ("Be Ready"), the community is educated on specific threats that exist in their neighborhoods. The citizenry is also engaged in the problem-solving efforts through the identification of potential hazards, and ideally would engage in mitigation efforts as a result. Rather than relying on government sources for disaster recovery assistance, the community is encouraged to take ownership through their ongoing involvement and dialogue with EM officials.

[227] Keeley Townsend, John P. Sullivan, Thomas Monahan, & and John Donnelly, "Intelligence-led Mitigation," 1.

V. THE EMERGENCY MANAGEMENT INTELLIGENCE CYCLE

Research Question: Is there a role for an intelligence process within the emergency management field? If so, what role could it play, what would the process look like, and how best could it be implemented to improve the all-hazards homeland security enterprise?

In light of the information presented in Chapters I through IV, this chapter will return to the research question and present evidence that addresses each aspect individually. To accomplish this, the questions will be addressed in a reverse fashion (with the exception of the implementation portion), building on each other and providing both evidence and examples for an EM intelligence process. The implementation portion will follow as part of Chapter V.

A. INTELLIGENCE IN EM–WHAT WOULD THE PROCESS LOOK LIKE?

Given the three models presented in Chapter III, it is suggested that intelligence in EM should adhere to the most fundamental of the three models: the FBI's Intelligence Cycle. The steps are generic enough to apply directly to EM with minimal effort (as described below), and would allow the EM community to adopt a formalized process for intelligence that it currently lacks. However, the other models contain good principles the EM should not neglect. Therefore, the model presented below incorporates principles of both models that were not selected into the EM intelligence cycle. The six steps are as follows:

1. Step One–Requirements

The requirements step for the EM Intelligence Cycle (EMIC) would be identical to that of the FBI model. Once the EM intelligence community receives a request for an intelligence product, a similar process for establishing the parameters of the desired end product would be followed. The subject of the study could be from a wide variety of topics that are of importance to the EM field, including critical infrastructure vulnerability and potential for impacts from a given natural disaster. It could also require collaboration with the SLFC or IC to develop a dual, comprehensive intelligence product

on a target where both communities would play a role in prevention, response, or recovery. The type of analysis being requested would also be solidified, and the EM intelligence community would be able to provide current analysis, trend analysis, or long-term assessments on the subject.

2. Step Two–Planning and Direction

The planning and direction step would also follow the FBI's model for the basic functions and activities that would need to take place. A timeline would be established for the individual deliverables, giving sufficient time to conduct a thorough collection and analysis based on the requirements established during Step one. This step would also address the need for any subject matter expertise that might be required, whether it be a member of the EM community or an external partner (i.e., health, science, or technical). The appropriate finished product format would be determined, as the EM intelligence community would also be capable of providing all five categories identified by the ITACG.

Step two would deviate slightly from the FBI model in that the EMIC's model would include the implementation of IPB's steps one and two. A certain amount of information on the current capabilities within the impacted jurisdiction would already be available due to an already established baseline capabilities assessment and general familiarity. With this information in mind, the EM intelligence community would know what intelligence has already been gathered and what intelligence will need to be gathered in order to support decision-making. This includes information that is readily available such as weather and terrain.

Additionally, in order to support this step, the use of the OCOKA Process would be a powerful tool in establishing baseline capabilities as part of pre-event assessments. Conducted by local, county, Tribal, or State officials, the OCOKA model would provide information on:

- General observations of the community (including demographics).
- Concealment and cover (shelter from the event, areas of high ground).

- Obstacles—potential hotspots or areas that are prone to the effects of inclement weather and should be avoided.
- Key terrain—areas that are crucial to protect due to second-order effects, including those that are of symbolic or cultural importance to the citizens.
- Avenues of approach—routes of ingress and egress that are safe for first responders to utilize, as well as for evacuations of residents, if necessary.

Based on this information, collection requirements could be established, priorities could be determined, and assessments of key facilities within these parameters could be requested.

3. Step Three–Collection

With the requirements, planning, and assessment of baseline capabilities completed, the collection of information necessary to complete the product would then ensue. Although similar in the basic function of collection, the EMIC would employ different methods of collection to complete the assessment. This is understandable given the nature of the areas of interest, but the EM intelligence community could utilize an INT categorization to determine what types of intelligence would be most pertinent and useful to the inquiry. The EM INTs that could be tapped into would be:

- Signals Intelligence (SIGINT)–the least applicable to the EM intelligence community, SIGINT could be utilized to monitor radio communications openly (not clandestinely) between first responders or potential victims for the sake of collecting pertinent information. Such SIGINT could employ the assistance of Ham Radio Operators, either employed by the agency or part of a volunteer EM organization (such as the FEMA-endorsed Radio Amateur Civil Emergency Services group[228])
- Imagery and Geospatial Intelligence (IMINT/GEOINT)–GIS capabilities are now commonplace in EOC's with data available both on-hand (pre-event) and capabilities from regional assets (FEMA Regions[229] and the National Oceanic and Atmospheric Administration's satellite feeds[230]). These could be supported by real-time feeds from first responders, surveillance cameras in the impacted area, and strategically placed EM

[228] U.S. Radio Amateur Civil Emergency Service, *Radio Amateur Civil Emergency Service*, http://www.usraces.org/.

[229] Federal Emergency Management Agency, *FEMA GIS Data Feeds*, http://gis.fema.gov/DataFeeds.html.

[230] National Oceanic and Atmospheric Administration, *Satellites*, http://www.noaa.gov/satellites.html.

resources deployed to provide such imagery. The United States Air Force Auxiliary's Civil Air Patrol[231] or other air assets that provide aerial views of the ongoing event or impacted area could also support this capability.

- Measurements and Signature Intelligence (MASINT)–the EM intelligence community could greatly benefit from the utilization of technical experts who could provide scientifically developed intelligence on the potential patterns or impacts of various events. Seismologists, hydrologists, and nuclear/chemical/environmental/ structural engineers could provide valuable insight that is beyond the traditional scope of EM expertise and help determine potential courses of action. Such experts could also be used prior to events to conduct research on potential areas of failure or impact, leading to the development of mitigation and protection priorities.

- Open Source Intelligence (OSINT)–the use of open sources to collect information is a goldmine of raw data, although it must be put through the intelligence cycle in order to validate the information that is being shared. The news media is a good source of OSINT, as they are often on the scene with cameras rolling shortly after an incident begins. Additionally, social media has seen a surge in the last decade, and sites like Twitter, Facebook, Instagram, and Flickr provide real-time information in an easily searchable format. For example, a study conducted on the use of Twitter during the Joplin tornado of 2011 found that 206,764 unique tweets were posted with the hashtag **#joplin** a few hours after the tornado hit.[232] A similar tactic was used during the El Reno tornado in May of 2013, when Oklahoma Emergency Management use "social media to gain situational awareness about the level of damage in the early hours following the storms,"[233] when information from the field was sparse. Capitalizing on this source of information, EM organizations ranging the gambit from international[234] to local[235] have taken to Twitter to gather information during events. Specific information is also available on the various phases of disaster

231 United States Air Force Auxiliary Civil Air Patrol, *Emergency Services*, http://www.gocivilairpatrol.com/about/civil_air_patrols_three_primary_missions/emergency-services/.

232 Muhammad Imran, Shady Elbassuoni, Carlos Castillo, Fernando Diaz, and Patrick Meier. "Extracting Information Nuggets from Disaster-Related Messages in Social Media," proceedings from the 10th International ISCRAM Conference – Baden-Baden, Germany, May 2013, 2.

233 Albert Ashwood, "Emergency MGMT 2.0: How #SocialMedia & New Tech are Transforming Preparedness, Response, & Recovery #Disasters #Part2 #Govt/NGOs," Statement for the Record before the U.S. House of Representatives Committee on Homeland Security, July 9, 2013, 3.

234 Australian and New Zealand Joint Association Initiative, *Disaster Management Forum*, https://twitter.com/DisasterForums.

235 Cal Fire, *Cal Fire Information Forum*, https://twitter.com/CALFIRESANDIEGO.

management (i.e., Recovery[236]). Properly mined and analyzed, these sources of information could prove invaluable to the EM intelligence community.

- Human Intelligence (HUMINT)–the HUMINT role within EM becomes another powerful source of information with the introduction of the ILP principle of using field sensors to gain information. These field sensors would come from the EM and first responder communities, but could also come from the general citizenry of the area of concern, as well. Residents of an area who have seen direct impacts in the past could be a good source of historical data on vulnerable areas. Coupled with the public education loops within ILP, citizens could be trained as field sensors and work with local EM staff to provide information on specific subjects. This development of HUMINT also has the second-order effect of engaging citizens in both resilience and recovery efforts. This engagement of citizens is the crux of FEMA's "Whole Community" campaign,[237] a part of the all-hazards concept.

This collection of information should also include reports that are already proliferated throughout the EM community. For example, on a daily basis the Arizona Division of Emergency Management receives situation reports from the North American Aerospace Defense Command, NOAA, the U.S. Department of Health and Human Services, FEMA, and the U.S. Department of the Interior. These reports offer both national and local level information that should be considered as part of Steps Four and Five.

4. Step Four-–Processing and Exploitation

The processing and exploitation step of the EM intelligence cycle would encompass the process of sorting through the data, determining what is relevant, and ensuring it is in a form that is usable to analysts. This includes data reduction, as in cases where the data is voluminous (such as the Twitter example above), the information must be culled significantly. ILP's emphasis on metrics would be pertinent here, especially if it aids the data reduction effort. Being able to provide analysts, and subsequently decision-makers, empirical data that helps in establishing historical trends and forecasting future likely scenarios is a powerful capability. This step would also include a loop back to Step

[236] Disaster Recovery Today, *Disaster Management Forum*, https://twitter.com/DRToday.

[237] Federal Emergency Management Agency, *Whole Community*, http://www.fema.gov/whole-community.

Three if gaps in the information are detected through preliminary evaluation. As in the FBI model, this could occur either prior to or concurrently with a move to Step Five.

5. Step Five–Analysis and Production

The area of analysis and production is where EM could most benefit from a formalized process. Without this key step, information is not transformed into a product that is validated and consolidated to provide only the essential data required for decision-makers. Among these decisions is the allocation of resources, as accentuated by the ILP model. With a finite amount of equipment on hand, a leader needs to have intelligence on the potential scope of the event and subsequently determine where to place these resources, as well as if outreach to other agencies for support personnel and equipment is warranted. This support system is already in place through mutual aid agreements, the Emergency Management Assistance Compact,[238] and multiple federal resources; however, without a formalized intelligence process this decision is left to individual EM entities to determine. This approach defaults to a reactive posture, as resources are a consideration as the event unfolds and raw information flows into EOCs, rather than prior to the event or immediately after the onset through the formalized intelligence process.

The analysis step should also employ Step Four of the IPB process and take into consideration the potential courses of action of the threat. Although this is exceptionally more difficult for immediate natural events (such as earthquakes or tornados), evolving events (such as floods and hurricanes) are far more predictable. Studies of watersheds and flow capacities of critical runoff areas are feasible both before and during an event, and key decisions on moving resources, the protection of critical infrastructure, and the release of water from potentially impacted dams and levees would all serve to reduce impacts of the event. As an example, New York's Metropolitan Transportation Authority suspended subway service prior to the landfall of Hurricane Irene, marking the "first time

238 Emergency Management Assistance Compact, *Resources That Deploy Under EMAC*, http://www.emacweb.org/index.php?option=com_content&view=article&id=200&Itemid=287.

public officials closed the system in preparation for a storm."[239] Additionally, the MTA crews "moved trains and other valuable equipment to higher ground, blocked station entrances, covered vents, and positioned pump trains and emergency generators in locations where they could be immediately used after the surge."[240] By evaluating the courses of action of these events, preparations can be made to reduce the loss of life and property.

The other consideration during this step is to determine what type of product will be most appropriate to convey the intelligence. This is dictated primarily by the requirements step, but the EM community could consider a more finite range of products similar to the FBI or national IC community. A categorical system of situation reports, bulletins, and assessments would give the EM intelligence community a template for reporting that could then be sent to multiple jurisdictions or partners in a standardized format that would be easily read and understood.

6. Step Six–Dissemination

As depicted in all three models reviewed in Chapter III, the dissemination of the intelligence is the ultimate goal. Intelligence for intelligence's sake is of no benefit; it is only when given to decision-makers that intelligence becomes action (or a concerted decision for inaction) that intelligence reaches its intended end state. In addition to decision-makers, the intelligence could also be disseminated to multi-jurisdictional and multi-discipline partners who may benefit from greater situational awareness that informs their own decision-making processes. The intelligence could also be disseminated to the community according to the ILP model for their review, awareness, and possible action. This dissemination to the community can occur through either direct interaction with community leaders or through public education efforts to the citizenry as a whole.

---

239 Sarah Kaufman, Carson Qing, Nolan Levenson, and Melinda Hanson, "Transportation During and After Hurricane Sandy," New York University Wagner Graduate School of Public Service (November 2012), 5.

240 Ibid., 5.

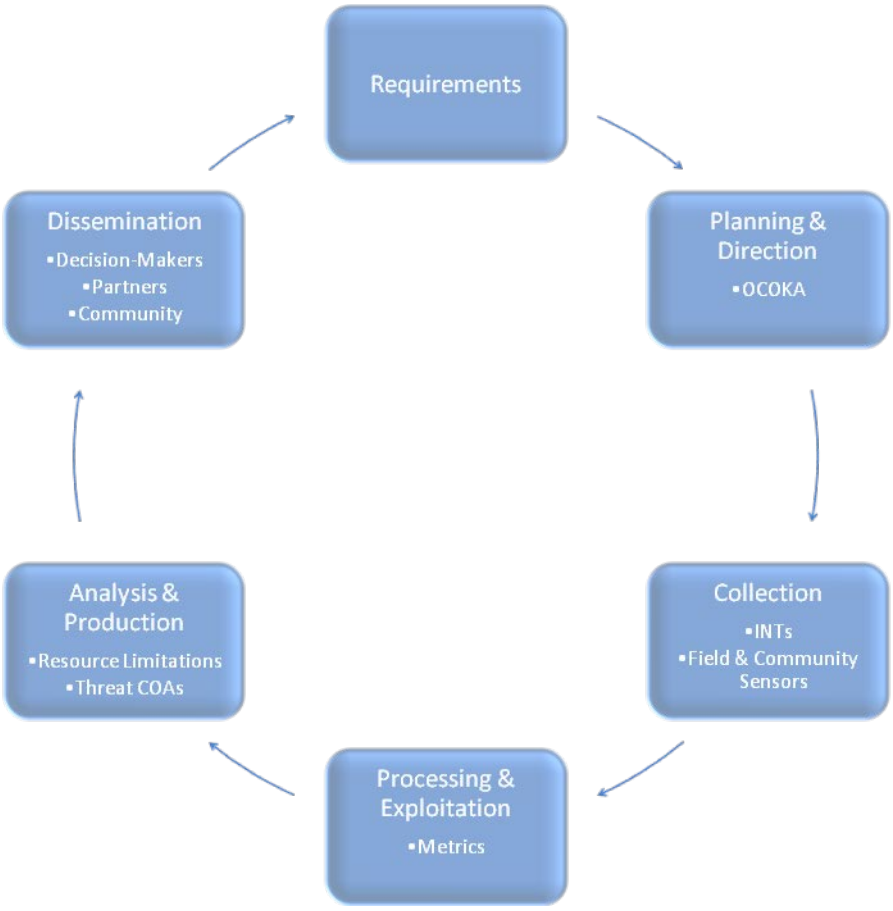

Figure 4. The Emergency Management Intelligence Cycle (EMIC)

VI. CONCLUSION AND RECOMMENDATIONS

Know the enemy, know yourself; your victory will never be endangered.
Know the ground, know the weather; your victory will then be total.

Sun Tzu, The Art of War

The threat environment facing today's HSE is both complex and evolving; in order to meet the challenge this dynamic situation presents, our all-hazards community must also consider changes to current practices that limit our collaboration, efficiency, and posture. As suggested by the findings of this thesis, a key area of opportunity is the use of a well-defined intelligence model that would at minimum improve the capabilities of EM to better prevent and mitigate impacts from natural disasters when possible, protect citizens and critical infrastructure from adverse impacts, respond intelligently to incidents, and ultimately recover quickly from events that are unavoidable. As highlighted in Chapter V, the process currently exists to some degree yet lacks definition and wholesale implementation; therefore, the adoption of the EMIC would be fairly basic and require a minimal investment of time and funding. In line with current emphasis from FEMA and DHS, this effort should begin at the local and state level with Federal support and guidance, and should consider the following recommendations for implementation:

A. RECOMMENDATIONS

Develop a nationwide EM Intelligence Officer program to be implemented at the state and local level that initially consists of key current EM personnel who have related duties. Once identified, introduce the EMIC process to the EM Intelligence Officers, and further develop a role in routine EM operations for its use.

The first step towards implementing the EMIC and bolstering the all-hazards community with this capability would be developing a nationwide EM Intelligence Officer program establishing some common standards for implementation and use of the EMIC. This step would rely heavily on identifying key current local and state EM personnel whose positions or skill sets most closely match those required of the Intelligence Function. Personnel within the Response or Mitigation mission areas may provide a base for the initial push, as both are integrally involved in activities that

correlate to the Collection and Analysis & Production steps of the EMIC. Mitigation, in particular, commonly has ties to key resources outside the EM community (such as scientists or engineers), and those connections would provide valuable data for the EMIC; the EM Intelligence Officers would be dependent on such sources, and it logically follows that the EM Intelligence program start where those relationships exist. Mitigation is also best poised, through both their daily activities and resources (i.e., federal mitigation grants) to implement the intelligence products and work to improve the posture of EM. By starting with current EM staff, the initial cost outlay for implementing the EMIC is minimized, resources are more efficiently used through an EMIC-driven process, and we ensure that the initial cadre of EM Intelligence Officers is familiar with EM concepts and missions. Their initial focus would be exploring, refining, and integrating the concepts discussed in Chapter III, improving EM's role and capabilities in all five national mission areas.

The introduction of the EMIC to the EM community and larger IC as a whole would also be streamlined by the identification of a static role within routine operations where EM Intelligence Officers could function, ideally in a consistent manner nationwide. Using the Intelligence/Investigation Function guidelines as developed by FEMA in 2008 that defined the roles and responsibilities within an Incident Command System structure,[241] this role should then be expanded to include both field and routine operations to ensure constant input of information into the EMIC. Each jurisdiction interested in the utilization of such a function should then consider which personnel from their EM operations could best fill this role based on the identified need of their specific threat environment and the guidelines provided above.

Once the role is defined, a training regimen for EM Intelligence Officers should be developed and implemented based on training for the current IC.

Once the role is defined and some loose initial parameters are established for preliminary deployment, the EM Intelligence Officers will require training that blends the development and use of intelligence with EM concepts to ensure immediate application. Although a new concept to the EM community, the EMIC will benefit from established

241 FEMA, Intelligence/Investigations Function, 1.

training and practices in the current IC. This would include training alongside Intelligence Analysts in the current state-level IC, such as the Specialized Analytic Seminar Series identified as a primary curriculum for SLFC personnel.[242] The EM Intelligence Officers would be trained in the Nationwide Suspicious Activity Reporting Initiative,[243] which has pre-identified EM as key members, and will also foster cross-discipline collaboration on information gathering outside of the traditional EM responsibilities. With an intelligence process foundation, the training would then graduate to a more specific EM-oriented program that would include the EMIC, best practices from current use, and the incorporation of subject-matter experts on relevant topics. With a trained cadre of EM Intelligence Officers developed, the EMIC concept could then push forward into the third recommendation.

Development of local level multi-disciplinary teams who will be primarily responsible for implementation of the EMIC at the ground level, collaborating on assessing the local threat environment, and developing intelligence products.

The third recommendation would be accomplished at the State, county, or local level, depending on need and personnel, and be primarily responsible for implementing EMIC principles and processes at the local level. Based on the Local Emergency Planning Committee concept currently employed by the Hazardous Materials response community, this group would streamline the IC and be able to provide a more comprehensive picture of the all-hazards threat environment that policy makers (i.e., Mayors, Governors) require.[244] The coordination group would include representation from the IC, EM, and first responder communities, as well as other agencies that are key sources of intelligence given the local threat environment.

As an intermediary between the IC and local/State EOC, the group would be responsible for acting on requests for intelligence from policy makers, as well as disseminating information back to the community responsible for preparing and responding to the threat. This solution would also give both communities an opportunity

242 National Network of Fusion Centers, "2012 Final Report," 81.

243 USDOJ Bureau of Justice Assistance, "Suspicious Activity Reporting Training for Hometown Security Partners," Nationwide SAR Initiative Flyer (revised March 2012), 1.

244 Dr. James Steiner, "Needed: State-level, Integrated Intelligence Enterprises," 3.

to meet on a regular basis and "foster an ongoing understanding and appreciation of the roles, responsibilities and current endeavors undertaken by each center."[245] Members of this group could be used during an incident to expedite resources and also provide liaisons or personnel when requested[246] ensuring expertise is available where needed. The EM Intelligence Officers could work closely with Terrorism Liaison Officer programs, where established, and collaborate on intelligence requests that had a requirement for an all-hazards analysis. Based on prior events and successes, key roles could include:

- Intelligence support to incident command[247]
- Situation reports that include current information on locations of shelters, road closures, status of transportation, and overall state of the disaster[248]
- Damage assessments following an event to help prioritize response and recovery efforts[249]
- Threat and risk assessments prior to an event to ensure comprehensive, intelligent planning

The EMIC plays a key role in the above groups from both a philosophical and practical level. Without an EMIC, collaboration would relegate the EM participants to their current information provider role. However, with a well-defined EMIC in place, EM has an equivalent role in both groups and plays a key role in the collection, analysis, and dissemination of intelligence that strengthens the all-hazards community. The foundation that the EMIC provides allows for common language and understanding amongst the partners. As the groups continue to collaborate, trust is built, victories are won, and the process is refined for maximum benefit.

Development of a State-Level Coordination Group to oversee the statewide implementation of the EMIC and define policies and parameters for a SLFC-EM collaboration.

Concurrently with the implementation of the first three recommendations, a critical final piece towards achieving this goal would be to establish a State level

---

245 DHS/DOJ- CPG 502, 27.

246 Ibid., 20.

247 National Network of Fusion Centers, "2012 Final Report," 89.

248 Col. Rick Fuentes, "Fusion Center Coordinates New Jersey Hurricane Sandy Disaster Response," Information Sharing Environment- http://ise.gov, February 5, 2013.

249 Ibid.

coordination group that would act as an intermediary between the SLFC and EOC. Without the support and leadership of Directors and high-level officials from both sides who can champion the effort, the EMIC will not have direct impact on the all-hazards preparedness of the State and local governments. As the primary connection to the IC, this group would not only be able to provide the best avenue to get the EMIC implemented, but also outline the connections to the larger all-hazards community and readily identify points of application. Amongst the State-Level Coordination Groups that already exist in the SLFC, just over 50 percent include EM partners in their governing boards;[250] the template for such a high-level Coordination Group is already roughly modeled. This group could lean on Federal policy yet simultaneously develop guidelines that would help best address the demographic and geographic nuances of their area of responsibility.

This group could also determine whether a joint SLFC-EOC operation was warranted given their current and anticipated future threat environment. Although this combination may not be warranted in every situation, this group could consider established joint operations and determine suitability for their situation. The State-Level Coordination Group could consider the successes of states such as New Jersey, where the Regional Operations and intelligence Center has combined both an SLFC and EOC. The ROIC supports the all-hazards community by analyzing and sharing information that includes both natural and man-made disasters, and played a key role in the overall response operations from events like 2012's Superstorm Sandy.[251] This type of collaboration should be considered by the SLFCs and EOCs of every state in light of potential benefits and capability strengthening.

B. CONCLUSION

The introduction and proliferation of the all-hazards approach to homeland security has presented the HSE with great opportunities to improve our current range of operations and strengthen our capabilities. As identified in Chapter I, the all-hazards

[250] National Network of Fusion Centers, "2012 Final Report," 59.

[251] Col. Rick Fuentes, "Fusion Center Coordinates New Jersey Hurricane Sandy Disaster Response."

concept seeks to increase collaboration, reduce inefficiencies, and improve national posture for both man-made and natural events. The development and use of intelligence will play a key role in all three of these areas, but requires implementation of intelligence capabilities across the HSE partners. The EM community falls woefully behind in this area; the EMIC is a solid foundation from which to develop this capability within EM, as well as foster greater collaboration amongst the all-hazards partners. Such a process will "encourage a broader perspective on risks and how to deal with them and a broader foundation on which to build effective programs to manage hazards and disasters."[252] The EMIC strengthens the all-hazards community and provides a significant step forward in achieving the all-hazard goals:

1. Collaboration

The National Intelligence Strategy states that three of its enterprise objectives are to, "build familiarity of the IC and its capabilities, expand partnerships, and establish new partnerships."[253] The EM community, through the EMIC, can capitalize on this objective and bring a capability to the HSE table that adds dimension and depth to the all-hazards community. Collaboration on assessing risks that will require responses from all partners will foster a partnership that positively benefits all stages of an incident. The EMIC also improves the flow of intelligence information, established channels for dissemination, and proper handling of intelligence. In light of ever-increasing information sharing requirements established by Federal policy makers (i.e., HR 1542, Weapons of Mass Destruction Information Sharing Bill[254]), the EMIC establishes a means by which this information is received and handled.

2. Reducing Inefficiencies

The EMIC fosters greater all-hazards planning, and is inherently more cost and time effective. Rather than conducting risk assessments, gathering key situational

---

252 William Waugh, "Terrorism and the All-Hazards Model," 3.

253 ODNI National Intelligence Strategy, 11–12.

254 U.S. Congress, "WMD Intelligence and Information Sharing Act of 2013," H.R. 1542- 113th Congress, 1st Session (July 23, 2013).

information, and developing strategies for future events in a silo, these activities are conducted in concert with other partners charged with roles in planning, response, and recovery. It facilitates a centralized approach whereby policy-makers are provided comprehensive intelligence assessments, resources are coordinated and managed, and leadership can make well-informed, timely decisions. The EMIC helps expedite the information gathering process within the EM community itself, as the process pre-identifies considerations and frames the intended outcomes, establishing structure where there is currently little.

3. Posture

Most importantly, the EMIC will dramatically improve the posture of the EM community, and as a natural consequence, the HSE as a whole. The EMIC encourages a more proactive approach to all-hazards planning, and also promotes a broader perspective that includes consideration of political, psychological, social and economic impact of events.[255] By defining and formalizing a process of intelligence within EM, practitioners would require information in advance of an event to provide adequate context, and thereby pushing a big portion of information gathering to the front-end of an event. Rather than waiting for information to flow into the EOC in disorganized pieces, EM Intelligence Officers are proactively seeking information to feed into the EMIC, and evaluating the information against a pre-established framework. Because the EMIC also supports collaboration and efficiency of resources, it provides a more comprehensive approach to EM that allows for a better posture.

As Sun Tzu observed in the quote that began this chapter, knowing our capabilities and limitations is only a small portion of the battle. To achieve the most comprehensive victory as possible in our HSE goals and objectives, we must also know the hazards we face and the peripheral factors that also play a role in our all-hazards preparedness, response, and recovery. Across the national EM and all-hazards landscape, this mindset exists to varying degrees. However, without a formalized process for intelligence within EM, the victory will struggle to be comprehensive enough to consider

255 William Waugh, "Terrorism and the All-Hazards Model," 3.

the range of factors that each event presents. The EMIC provides this process, and enables our all-hazards community to intelligently address the threat environment we face as a unified army. Total victory is within our grasp.

LIST OF REFERENCES

Abkowitz, Mark D., and Samrat Chatterjee. (2012). Regional Disaster Risk: Assessment and Mitigation Concepts in an All-Hazards Context. Journal of Homeland Security and Emergency Management, 9 (1, Article 15).

Ashwood, Albert. "Emergency MGMT 2.0: How #SocialMedia & New Tech are Transforming Preparedness, Response, & Recovery #Disasters #Part2 #Govt/NGOs," Statement for the Record before the U.S. House of Representatives Committee on Homeland Security, July 9, 2013.

Australian and New Zealand Joint Association Initiative, *Disaster Management Forum*, Accessed July 27, 2013, https://twitter.com/DisasterForums.

Baker, John. "Risk Analysis and Intelligence Communities Collaborative Framework," Homeland Security Institute (April 2009), 63.

Bean, Howard, and Beth Keranen. (2007). The Role of Homeland Security Information Bulletins within Emergency Management Organizations: A Case Study of Enactment. Journal of Homeland Security and Emergency Management, 4 (2, Article 6).

Becker, Christine. "Disaster Recovery: A Local Government Responsibility," ICMA Public Management Magazine 91 (Number 2) March 2009, Accessed June 3, 2013, http://webapps.icma.org/pm/9102/.

Brunelle, Gregory T. "Achieving Shared Situational Awareness During Steady-State Operations in New York State: A Model for Success," (Master's Thesis, Naval Postgraduate School, 2010).

Burton, Fred and Scott Stewart, "Threats, Situational Awareness, and Perspective," STRATFOR Global Intelligence Security Weekly, August 22, 2007.

Bush, George W. Homeland Security Presidential Directive 8, December 2003.

———. "Using 21st Century Technology to Defend the Homeland," Accessed April 6, 2013, http://www.whitehouse.qov/homeland/21st-technology.html.

Cal Fire, *Cal Fire Information Forum,* Accessed July 27, 2013, https://twitter.com/CALFIRESANDIEGO.

Canadian Chief of Defence, *Joint Intelligence Doctrine,* CF Publication B-GJ-005–200FP-000, May 2003.

Canadian Defence Intelligence Agency, Intelligence Analyst Course Textbook (Joint Military Intelligence Training Center, 2000), II-4–2.

Canadian Security Intelligence Service, *Backgrounder No. 3 – CSIS and the Security Intelligence Cycle,* February 2004, http://www.csis-scrs.gc.ca/nwsrm/bckgrndrs/bckgrndr03-eng.asp.

Carter, David L., and Jeremy G. Carter. Intelligence Led Policing: Conceptual Considerations for Public Policy. Criminal Justice Policy Review, 20(3), 310–325. (2009).

Carter, David L. "Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies," U.S. Department of Justice Project #2003-CK-WX-0455 (November 2004).

———. "The Law Enforcement Intelligence Function: State, Local, and Tribal Agencies," The FBI Law Enforcement Bulletin (June 1, 2005).

Caruson, Kiki. Mission Impossible? The Challenge of Implementing an Integrated Homeland Security Strategy. Journal of Homeland Security and Emergency Management, 1 (4, Article 407).

Center for Army Lessons Learned, "Intelligence Preparation of the Battlefield," U.S. Army Training and Doctrine Command, Fort Leavenworth, KS, no. 96–12 (December 1996).

Clarke, Wes. "Emergency Management in County Government: A National Survey," National Center for the Study of Counties, University of Georgia (August 2006).

Combrink, Thomas, Cheryl Cothran, Wayne Fox, Jeff Peterson, and Gary Snider. "A Full Cost Accounting of the 2010 Schultz Fire," Northern Arizona University Ecological Restoration Institute, May 2013.

Disaster Recovery Today, *Disaster Management Forum,* Accessed July 27, 2013, https://twitter.com/DRToday.

Emergency Management Assistance Compact, *Resources That Deploy Under EMAC*, Accessed July 28, 2013, http://www.emacweb.org/index.php?option=com_content&view=article&id=200&Itemid=287.

Federal Bureau of Investigation. *Intelligence Cycle.* Accessed September 16, 2012, http://www.fbi.gov/about-us/intelligence/intelligence-cycle.

———. *Intelligence Defined.* Accessed September 16, 2012, http://www.fbi.gov/about-us/intelligence/defined.

———. *Quick Facts*. Accessed July 14, 2013, http://www.fbi.gov/about-us/quick-facts.

Federal Emergency Management Agency. Disaster Relief Fund: Monthly Report Through June 30, 2013, published July 5, 2013.

———. *FEMA GIS Data Feeds*, Accessed July 2, 2013, http://gis.fema.gov/DataFeeds.html.

———. FEMA GPD Grant Program Accomplishments Report, May 2009.

———. "Intelligence/Investigations Function Guidance Document" Version 3 (Draft), February 2008.

———. *Mission Areas*, Accessed June 7, 2013, http://www.fema.gov/mission-areas.

———. *National Planning Frameworks*, Accessed May 13, 2013, www.fema.gov/national-planning-frameworks.

———. *National Preparedness Goal*, Accessed May 19, 2013, http://www.fema.gov/national-preparedness-goal.

———. The State of FEMA, 2012.

———. *Whole Community*. Accessed July 27, 2013, http://www.fema.gov/whole-community.

Fuentes, Col. Rick. "Fusion Center Coordinates New Jersey Hurricane Sandy Disaster Response." Information Sharing Environment–http://ise.gov, February 5, 2013.

Global Security.ORG, Urban Intelligence Preparation of the Battlefield. Accessed June 18, 2013, http://www.globalsecurity.org/military/library/policy/army/fm/3–06/appb.htm.

Harman, The Honorable Jane. Testimony before the U.S. Senate Homeland Security and Governmental Affairs Committee, July 12, 2012.

Imran, Muhammad, Shady Elbassuoni, Carlos Castillo, Fernando Diaz, and Patrick Meier. "Extracting Information Nuggets from Disaster-Related Messages in Social Media." proceedings from the 10th International ISCRAM Conference – Baden-Baden, Germany, May 2013.

Jackson, David P. "Intelligence-Led Risk Management for Homeland Security: A Collaborative Approach for a Common Goal." (Master's Thesis, Naval Postgraduate School, 2011).

Jenkins, William O. (2007). Homeland security: Applying risk management principles to guide Federal investments: Testimony before the Subcommittee on Homeland Security, House Committee on Appropriations. (GAO Report No. GAO-07–386T). Washington, D.C.: United States. Government Accountability Office.

Kaufman, Sarah, Carson Qing, Nolan Levenson, and Melinda Hanson. "Transportation During and After Hurricane Sandy." New York University Wagner Graduate School of Public Service (November 2012).

Kebair, Fahem, and Frederic Serin. "Towards an Intelligent System for Risk Prevention and Emergency Management." proceedings from the 5th International ISCRAM Conference – Washington, DC, USA, May 2008.

Keithly, David M. "Intelligence Fundamentals." In *Homeland Security and Intelligence*, edited by Keith Gregory Logan. Santa Barbara, CA: Praeger Security International, 2010.

Kelly III, Lt. Col. Patrick. "Intelligence Support to Homeland Security: Supporting the Supporting Effort." U.S. Army War College-Strategy Research Project (April 2002).

Kim, Jin, and William Allard. "Intelligence Preparation of the Battlespace: A Methodology for Homeland Security Analysis." SAIS Review 28 (No. 1, Winter-Spring 2008), 76.

Liotti, Louis. "Military Intelligence." in *Homeland Security and Intelligence*. ed. Keith Gregory Logan (Santa Barbara, CA: Praeger Security International, 2010).

Lucus-McEwen, Valerie. "Recalibrating Emergency Management: Information is not the same as intelligence." *Emergency Management,* December 2010, http://www.emergencymgmt.com/emergency-blogs/campus/Recalibrate-Emergency-Management-Information-Intelligence-122910.html.

The Markle Foundation. "Nation At Risk: Policy Makers Need Better Information to Protect the Country." (March 2009).

McCarter, Mickey. "Interoperable Communications Under FY2013 Consolidated Spending, Appropriations Consistent with 2012." *Homeland Security Today*, March 29, 2013.

Medby, Jamison Jo, and Russell W. Glenn. "Street Smart: Intelligence Preparation of the Battlefield for Urban Operations." RAND Corporation, MR-1287 (2002), xiv.

National Criminal Intelligence Service (UK). "National Intelligence Model." (2000).

National Network of Fusion Centers. "2012 Final Report." June 2013.

National Oceanic and Atmospheric Administration. *Satellites*. Accessed July 2, 2013, http://www.noaa.gov/satellites.html.

Navarro, Mireya. "Weighing Sea Barriers as Protection for New York." *New York Times*, November 7, 2012.

Nickel, Eric D. "Collective Intelligence in Emergency Management: Social Media's Emerging Role in the Emergency Operations Center. "Novato Fire District, Accessed January 15, 2013, www.usfa.fema.gov/pdf/efop/efo45101.pdf.

North Carolina Division of Emergency Management. "Situational Intelligence Maps Add Value During Emergencies." MEMO Publication 4 (Issue 11) November 2010.

Obama, Barack. Presidential Policy Directive 8, March 2011.

Office of the Chief of Naval Operations, "Domestic Disaster Relief Operations Planning," Department of the Navy Command TACMEMO 3–07.7–06 (May 2006).

Office of the Director for National Intelligence (Coordinating Agency). "Intelligence Guide for First Responders." (2nd Edition, March 2011).

Office of the Director for National Intelligence. *Members of the Intelligence Community*." Accessed September 19, 2012, http://www.dni.gov/index.php/intelligence-community/members-of-the-ic.

———. "National Intelligence: A Consumers' Guide." (2009).

———. *The National Intelligence Strategy*. August 2009.

———. *National Intelligence Emergency Management*. Accessed September 19, 2012, http://www.dni.gov/index.php/about/organization/niema.

———. *ODNI FAQ: About the Intelligence Community*. Accessed June 30, 2013, http://www.dni.gov/index.php/about/faq?start=2.

Office of the Director of National Intelligence. "United States Intelligence Community Information Sharing Strategy" (February 2008).

Pelfrey, William V. The Cycle of Preparedness: Establishing a Framework to Prepare for Terrorist Threats. Journal of Homeland Security and Emergency Management, 2 (1, Article 5), 2005.

Peterson, Marilyn. "Intelligence-Led Policing: The New Intelligence Architecture," U.S. DOJ Bureau of Justice Assistance, NCJ 210681 (September 2005).

Randol, Mark A. "The Department of Homeland Security Intelligence Enterprise: Operational Overview and Oversight Challenges for Congress." Congressional Research Service 7–5700 (May 27, 2009).

Ratcliffe, Jerry. *Intelligence-Led Policing*. (Portland, OR: Willan Publishing, 2008).

Rhodes, Carl, Jeff Hagen, and Mark Westergren. "A Strategies-to-Tasks Framework for Planning and Executing Intelligence, Surveillance and Reconnaissance (ISR) Operations." Rand Corporation–Technical Report 434 (2007).

Shaw, Andrew. "FEMA Announces Program Analyzing Non-federal Levees After Criticism from Vitter, Parish Presidents." The Times-Picayune, July 12, 2013.

Steiner, Dr. James. "Needed: State-level, Integrated Intelligence Enterprises." Studies in Intelligence. (Volume 63, No. 3), September 2009.

Stephenson, W. David, and Eric Bonabeau. "Expecting the Unexpected: The Need for a Networked Terrorism and Disaster Response Strategy." Homeland Security Affairs III, no. 1 (February 2007): 1.

Thomas, Major Troy S. "Beneath the Surface: Intelligence Preparation of the Battlespace for Counterterrorism." Center for Strategic Intelligence Research, Washington, DC (November 2004).

Townsend, Kenneth, J. P. Sullivan, J. P., T. Monahan, and J. Donnelly. (2010). Intelligence-led mitigation. Journal of Homeland Security and Emergency Management, 7 (1, Article 63).

Trim, Peter R. J. "An Integrative Approach to Disaster Management and Planning." Disaster Prevention and Management 13 (Number 3), 2004.

U. S. Air Force. *Air Force Doctrine Document 2–5. In:Command, A. F. D.* edited 2002.

United States Air Force Auxiliary Civil Air Patrol. *Emergency Services*. Accessed July 2, 2013, http://www.gocivilairpatrol.com/about/civil_air_patrols_three_primary_missions/emergency-services/.

United States Congress. *9/11 Commission Act of 2007 –P.L. 110–53*. August 3, 2007.

———. Local, State, Tribal, and Federal Preparedness Task Force. "Perspectives on Preparedness: Taking Stock Since 9/11." September 2010.

———. "WMD Intelligence and Information Sharing Act of 2013." H.R. 1542–113th Congress, 1st Session (July 23, 2013).

U.S. Department of Homeland Security. *About the Infrastructure Analysis and Strategy Division*. Accessed March 18, 2013, http://www.dhs.gov/infrastructure-analysis-and-strategy.

———. *About the Office of Operations Coordination and Planning*. Accessed March 17, 2013, http://www.dhs.gov/about-office-operations-coordination-and-planning.

———. *Automated Critical Asset Management System (ACAMS)*. Accessed April 4, 2013, http://www.dhs.gov/automated-critical-asset-management-system-acams.

———. "Deployed Intelligence Officers and Protective Security Advisors." Accessed September 21, 2012, http://www.dhs.gov/deployed-intelligence-officers-and-protective-security-advisors.

———. "Fusion Center Locations and Contact Information." Accessed August 28, 2013, http://www.dhs.gov/fusion-center-locations-and-contact-information.

———. "Interaction with State and Local Fusion Centers: Concept of Operations." December 2008.

———. National Preparedness Goal (First Edition), September 2011.

———. National Preparedness Report, March 2012.

U.S. Department of Homeland Security Office of Inspector General. *Relationships Between Fusion Centers and Emergency Operations Centers*. December 2011.

U.S. Department of Homeland Security and U.S. Department of Justice. *Comprehensive Preparedness Guide 502: Considerations for Fusion Center and Emergency Operations Center Coordination* (May 2010).

———. *Common Competencies for State, Local, and Tribal Intelligence Analysts*. June 2010.

———. *Fusion Center Guidelines*, 2006.

U.S. DOJ Bureau of Justice Assistance. "Reducing Crime Through Intelligence-Led Policing." U.S. Department of Justice Project #2008-DD-BX-K675 (2008).

——— "Suspicious Activity Reporting Training for Hometown Security Partners." Nationwide SAR Initiative Flyer (March 2012).

U.S. Department of Transportation. "Office of Intelligence, Security and Emergency Response." Accessed September 19, 2012, http://www.dot.gov/ost/oiser/intelligence.htm.

United States Government. "Intelligence Reform and Terrorism Prevention Act of 2004." Public Law 108–458 of December 17, 2004; 118 STAT.3638.

U.S. Homeland Security Council, National Strategy for Homeland Security, October 2007.

U.S. Joint Chiefs of Staff. "Joint Publication 2–02. National Intelligence Support to Joint Operations" (September 1998).

United States Marine Corps. Marine Corp Doctrinal Publication 6: Command & Control. October 1996.

University of Maryland. "What is CompStat?" Accessed June 29, 2013, http://www.compstat.umd.edu/what_is_cs.php.

U.S. Radio Amateur Civil Emergency Service. *Radio Amateur Civil Emergency Service*. Accessed July 2, 2013, http://www.usraces.org/.

Warner, Dr. Michael. "*Wanted: A Definition of Intelligence.*" (Central Intelligence Agency). Accessed October 23, 2012, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol46no3/article02.html.

Waugh, William. "Terrorism and the All-Hazards Model." paper presented on the IDS Emergency Management On-Line Conference. June 28–July 16, 2004.

The White House. National Security Strategy. May 2010.

Wood, Jennifer, and Clifford Shearing. *Imagining Security*. Cullompten, UK: Willan Publishing, 2007.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California