GENERATING THE ALL-HAZARDS INTELLIGENCE SYNTHESIS MODEL IN THE HOMELAND SECURITY INTELLIGENCE ENTERPRISE

____

A Thesis

Presented to

The Faculty of the Department of Homeland Security Studies

Sam Houston State University

____

In Partial Fulfillment

of the Requirements for the Degree of

Master of Science in Homeland Security Studies

____

by

Walter G. Reeves

December, 2018

GENERATING THE ALL-HAZARDS INTELLIGENCE SYNTHESIS MODEL IN THE HOMELAND SECURITY INTELLIGENCE ENTERPRISE

by

Walter G. Reeves

____

APPROVED:

Dr. Magdalena Denham
Committee Chair

Dr. Nadav Morag
Committee Co-Chair

Dr. David Webb
Committee Member

Dr. Phillip Lyons
Dean, College of Criminal Justice

DEDICATION

I dedicate this thesis in loving memory of my daughter Hailey Marie Reeves who passed away too soon. I love you sweet-pea.

1990 - 2017

ABSTRACT

Reeves, Walter G., *Generating the all-hazards intelligence synthesis model for the homeland security intelligence enterprise*. Master of Science (Homeland Security Studies), December 2018, Sam Houston State University, Huntsville, Texas.

The United States all-hazards homeland security operational and intelligence domains are multijurisdictional, multiagency, and multidisciplinary intelligence challenges for all-hazards intelligence analysts. A common analytical conceptual framework is needed to help unify homeland security intelligence enterprise analysts who work in an all-hazards, all-source, all-crimes, and all-disciplinary intelligence environment. A unifying all-hazards intelligence synthesis model that unites intelligence analysts with the law-enforcement, cybersecurity, technology, and natural science disciplines, would benefit the homeland security and intelligence domain enterprises. The purpose of the applied research was to discover and generate an all-hazards analysis model that enables the production of risk-informed applied intelligence products in a pluralistic intelligence environment that is privacy, civil rights, and civil liberties compliant. A comprehensive literature review was conducted following the four-step collect, analyze, synthesize, and apply process. This process is derived from proven knowledge, information, and risk management programs, as well as proven intelligence analysis methodologies, for gathering information about adversarial, cyber, technological, and natural hazards and threats to social, technological, and environmental resources. The research resulted in the generation of a universal all-hazards intelligence synthesis model that may be applicable to systems safety engineering, criminal, political, military, economic, social, and medical intelligence activities.

KEY WORDS: Homeland security, All-hazards, Intelligence, Synthesis, Analysis, All-crimes, All-source, Hazards, Threats, Crisis, Disaster, Catastrophe, Adversarial, Cyber, Technological, Natural, Interdisciplinary, Multijurisdictional, Interagency, Knowledge management, Information management, Risk management, Systems, Knowledge organization, Knowledge generation, Knowledge transfer, Knowledge application, Privacy, Civil rights, Civil liberties, Critical reasoning, Critical thinking, Clinical reasoning, Communication, Law enforcement.

ACKNOWLEDGEMENTS

I would like to acknowledge my thesis committee members, especially Dr. Magdalena Denham and Dr. Nadav Morag, who encouraged and advised me throughout my research and *knowledge generation* process. I also would like to acknowledge my loving wife Zsuzsanna who supported me with a tremendous amount of patience, and my parents who, twenty-nine years later, get to see me earn a second degree from Sam Houston State University.

Thank you for sharing this rewarding experience with me.

PREFACE

I chose an all-hazards analysis research topic because I wanted to have a deeper understanding of national security and intelligence from a different perspective than that of my U.S. Army Military Intelligence career. Although I had experience with assessing security risk from weather phenomenon, restrictive terrain, and, of course, military forces, I wanted to challenge myself to understand the broader context of adversarial, cyber, technological, and natural hazards in the homeland security context. This new look angle developed into a wider systemic analysis of crisis events. Looking back—way back—I now know my thesis began with something I had heard many times before: we are part of something larger than ourselves.

My systems view of life, although I didn't realize it was called that at the time, was stoked after reading *The systems view of life* by Fritjof Capra and Pier Luisi. I am very glad this book was required reading in my homeland security studies curriculum because it made me think a lot about life's connectivity and the relationships among all things social, technological, and natural. This perspective is an imperitive for security studies students in their understanding of safety, security, and resilience and it became my analytic approach to all-hazards.

Lastly, a chapter in *Security and Risk Management* by Bruce Newsome established what I call my point-of-entry-test into all-hazards research because of his explanation about the transformational nature of hazards into crises. Life is change—the world always is in flux so, with that understanding, the homeland security domains are better poised to ensure national safety, security, and resilience. I hope other students find similar activators to ignite their research interest and passion. I also hope this thesis does for them what my professors and thesis committee challenged me to do: contribute to the body of knowledge in the emerging homeland security studies field.

TABLE OF CONTENTS

Page

LIST OF FIGURES

CHAPTER I

Introduction

The Department of Homeland Security (DHS) is the United States federal government's lead homeland security enterprise institution for ensuring the nation's domestic security, resilience, and safety (Our Mission, 2018). The homeland security enterprise of public and private organizational partnerships generates and operationalizes national resource capacity in support of the national preparedness missions. These federal, state, local, and tribal governmental institutions, corporations, and homeland security organizations are guided by a collection of security directives, policies, doctrines, plans, and procedural publications. Similarly, the operational agencies of the homeland security enterprise are supported by a host of resource procurement and intelligence generation agencies (Bullock, Haddow, & Coppola, 2016, pp. 1-28).

My research is focused on the Homeland Security Intelligence Enterprise's (HSIE) (Homeland Security Committee, 2016, p. 11; Lahneman, Homeland Security Intelligence, 2018) all-hazards intelligence analysis and synthesis system. The HSIE is a networked and nested information and analysis system, as well as a community-of-practice, consisting of institutions, practitioners, and processes within the HSIE's security enterprise (Office of Intelligence and Analysis Mission, 2018). The HSIE's all-hazards analysis community-of-practice also is a community-of-people. Behind every intelligence analysis product and intelligence synthesis assessment, are all-hazards analysts working in a regional fusion center, critical infrastructure risk management office, or Intelligence Community (IC) cubicle. They work in a networked intelligence and information-sharing system of dispersed physical structures, virtual collaborative chat-rooms, and intelligence collection, analysis, production, and dissemination cycles. This collective intelligence synthesis system informs the homeland security enterprise's operational missions.

The population of the United States depends on the collaborative efforts of all-hazards analysts, who work within this intelligence and information-sharing community, to expertly advise, inform, and participate in the nation's homeland security decision-making process of policy, preparedness, and practice. The all-hazards analyst must be knowledgeable in a diverse range of social, scientific, and environmental disciplines because the broad array of homeland security threats is both human-caused and natural (Threat and Hazard Identification and Risk Assessment Guide, 2013). The nation's population justifiably expects all-hazards analysts to make sense of these threats to its well-being, way of life, and environment.

The all-hazards homeland security operational environment (HSOE) is a multijurisdictional, multiagency, and multidisciplinary intelligence challenge for an all-hazards analyst. However, the intelligence enterprise's training standards, jointly set by the DHS and the Department of Justice (DOJ), are law enforcement centric (Global Justice Information Sharing Initiative, 2007, 2010). To alleviate this challenge, all-hazards analysts need common core training, community-of-practice analysis methodologies, and a unifying conceptual framework. A common analytic mindset would help unify analysts who work in an all-hazards, all-source, all-crimes, and all-disciplinary intelligence field. Thus, a unifying all-hazards analysis conceptual framework, that ties together the intelligence, law-enforcement, natural science, and technological disciplines, would benefit the entire homeland security enterprise community.

Research Problem

Throughout my literature review process, I have not found a DHS publication that is all-hazards analysis centric or one that is specifically written about common all-hazards analysis concepts, methods, or techniques. Although DHS has published preparedness frameworks and guides on field operations; risk, incident, and crisis management; intelligence and information sharing; and analyst competency tasks; it has not publicly published a reference document that compiles common all-hazard analysis and intelligence synthesis frameworks, methodologies, and techniques. To be sure, the DHS does not have a publicly accessible doctrinal reference solely dedicated to all-hazards analysis.

The purpose of my applied research was to discover common all-hazards analysis frameworks, methods, and techniques within the DHS's HSIE at the federal government level, and to develop one that can be universally applied within a pluralistic all-hazards intelligence environment. I generated an intelligence synthesis model and an all-hazards analysis model from my research as the first step. I will apply and test them in post and premortem analysis scenarios to determine the extent of its usefulness as a common analytic framework in the HSIE as future research. Thus, this thesis is limited to building an all-hazards intelligence synthesis model (AH-ISM).

My research goals are grouped as personal, intellectual, and practical (Maxwell, 2013, p. 24). My personal research goal is to earn a master's degree with a full-thesis option for self-fulfillment and a sense of accomplishment. My military career, personal obligations, and a few setbacks interfered with my earning a graduate degree until now. However, I have earnestly pursued this personal goal since my retirement from the Army. My intellectual research goal is to advance my military intelligence experience and criminal justice background into the homeland security domain to expand my understanding of national and domestic security. Specifically, I want to better understand how intelligence analysis is applied in an all-hazards environment. Lastly, my practical research goal is to apply the knowledge gained from my academic research as a practitioner or consultant in the homeland security enterprise. Nevertheless, I am strongly considering doctoral programs as another personal and academic option before beginning a new career.

Justification and Relevance to the Homeland Security Intelligence Enterprise

The Department of Defense (DoD) is an established national institution since 1949 with constitutional origins as the War Department since 1789. As a national security institution, its doctrinal foundations are organized into functional categories such as operations, intelligence, or training (Bullock et al., 2016, pp. 156-158). These organizational domains have their own catalogue of doctrinal publications that are solely dedicated to their unique frameworks, guiding principles, terms, methods, procedures, tactics, and techniques. In comparison, the DHS was established in 2002 and is a relatively young national institution. Its domestic security doctrinal foundations also are organized into functional categories, but not all of them have dedicated doctrinal publications. Specifically, the intelligence and information sharing functions of the DHS lack a domain directory of all-hazards intelligence publications.

The enterprise's all-hazards analysis methods, terms, and concepts are distributed throughout operationally focused frameworks and field operational guides. I read at least 20 different DHS and Federal Emergency Management Agency (FEMA) documents, in addition to many more public and private non-departmental publications and academic textbooks, to garner a full appreciation of the all-hazards analyst's role and responsibilities. An HSIE analyst would have to read these publications and more to be knowledgeable of all-hazards, threats, and crises. I believe the DHS should compile a catalogue of intelligence domain publications, with unifying conceptual frameworks, all-hazards analytic methods, and intelligence process guidelines, into a single set of doctrinal reference materials specifically written for HSIE analysts.

Social Context and the Homeland Security Domain's Audience

The socioenvironmental system consists of the nation's population, social institutions, infrastructure, and environmental resources (Pine, 2015, p. 15). These systems, including technological systems, underpin the nation's capacity for survival and prosperity because without them modern life would cease. Clearly, national and domestic safety, security, and resilience preparedness goals are dependent upon the nation's social, technological, and environmental systems and a robust domestic security apparatus. In other words, the protection of lives, property, and the environment depends upon the homeland security enterprise's ability to carry out its missions.

In turn, the homeland security enterprise depends on timely, relevant, and risk-informed all-hazards intelligence assessments produced by the HSIE. Security professionals across the nation teaching at universities, planning emergency response operations, conducting critical infrastructure risk assessments, and patrolling the nation's borders should have access to current and actionable intelligence products. Therefore, the audience for my research findings will be the all-hazards academics, analysts, and practitioners of the HSIE.

Implications for the Emerging Homeland Security Studies Discipline

The applied knowledge of my research will help all-hazards analysts to identify, analyze, and assess adversarial, cyber, technological, and natural hazards, threats, and crisis events. The intelligence synthesis and all-hazards analysis models, which are discussed in detail in chapter V, are intended to provide conceptual clarity to the structures, processes, functions, and purpose of the HSIE's all-hazards intelligence synthesis system. Additionally, the all-hazards analyst's competency traits, which will be explained more in my findings, coupled with these analytic models are intended to establish a common foundation for multidisciplinary analyst-to-analyst communication, collaboration, and coordination.

These models, the baseline intelligence synthesis model (ISM) and the all-hazards intelligence synthesis model (AH-ISM), are intended to give multidomain all-hazards analyst with a set of interdisciplinary terms and analytic methods. For example, subject matter experts in safety engineering, or natural hazards risk analysis, would share the same analytic conceptual framework as a law enforcement all-crimes analyst. In other words, an all-hazards common core training standard, that goes beyond the current law enforcement-based training, could help unify interdisciplinary subject matter experts in the intelligence and security domains.

Research Questions

My applied research questions are aligned with my pragmatic realist world view and are designed to generate a practical solution to the all-hazards conceptual framework problem. They are intended to be specific, realistic, and process oriented (Maxwell, 2013, pp. 78-83). Like the purpose of intelligence analysis, my questions are meant to provide actionable findings and recommendations at the end of my research.

Central research question. What is a unifying interdisciplinary all-hazards analysis and intelligence synthesis model for providing risk-informed applied intelligence in support of the United States National Preparedness Goal by the homeland security intelligence enterprise?

Research questions.

1. What are the current and common all-hazards analysis and intelligence synthesis methods used by analysts in the homeland security intelligence enterprise at fusion centers and in other intelligence production and information sharing organizations?

2. To what extent does current homeland security intelligence enterprise approved training and certification courses teach common all-hazards analytic methodologies to intelligence analysis students?

3. What, if any, are the knowledge-centric and intelligence operations principles, programs, or policies that are relevant to the all-hazards analysis and intelligence synthesis model?

4. What, if any, are the homeland security operational environment's socio-technological-environmental system components that are relevant to the all-hazards analysis and intelligence synthesis model?

5. What, if any, are the consequential relationships among socio-technological-environmental systems and adversarial, cyber, technological, and natural hazards, threats, and crisis event systems?

6. To what extent is the all-hazards analysis and intelligence synthesis model replicable and applicable as an analytic model in the interdisciplinary homeland security intelligence enterprise?

Conceptual Framework for Researching All-hazards and Intelligence Synthesis

My conceptual framework for researching the all-hazards analysis and intelligence synthesis system is influenced by a selection of practical and theoretical approaches beginning with a systems worldview that is reinforced by two principles drawn from physics and chemistry. Together, they form my views on entities, interdependent relationships, transformation, emergence, and cause-effect associations (Ackoff & Emery, 2017, pp. 13-32; Capra & Luisi, 2014, pp. 63-83; Meadows, 2008, pp. 1-34). My analytic and research framework is based on the complementary views of holism and reduction that form my approach to the analysis phase of the intelligence synthesis process (Verschuuren, 2017, pp. 69-74). My conceptual framework for comprehending historical and environmental context, meaning-making, and decision-making is influence by three sense-making models: (a) Panarchy theory's adaptive cycle (Gunderson & Holling, 2002, pp. 5-8), (b) the Cynefin complexity framework (Brougham, 2015, pp. 6-10), and (c) the critical-thinking process (Elder & Paul, 2012, pp.

5-7). Lastly, my understanding of the HSOE is based on the all-hazards and the risk management approaches to national safety, security, and resilience; the human and environmental security approaches to domestic and global security; my professional military intelligence experience; and my personal experience with personal loss, hurricanes, tornadoes, and flooding disasters.

Worldview. Having a worldview or an established paradigm of beliefs about the *real* world does not automatically simplify how we live. The only way a worldview simplifies our life is when we surround ourselves with likeminded people. In this way, life is less complicated and less confrontational—making sense of it all and making choices are easier. However, I think the best way to challenge our personal worldview is to apply it in life. We should be willing to apply our worldview, and sincerely attempt to understand the worldviews of others, because this kind of application guides how we set goals, find purpose, create, perceive others, and react to danger.

In our search to understanding life and gaining knowledge, context is everything. Its within historical and environmental context that we broaden our mindset about the human and natural worlds (Kincheloe & Berry, 2004, pp. 6-8). Our personal individualistic context is our educational background multiplied by our life experiences and our willingness, or unwillingness, to adapt and change. Thus, a worldview's greater value is that it guides our quest to answer the *why* questions as well as the *how* questions in pursuit of a greater purpose.

Our worldview should challenge us and make us feel a little uneasy at times. It should make us pause and think when we encounter complications, confrontations, and crises rather than make us withdraw and become headstrong. It should cause us to consider other points-of-view and reconsider our own. It should help us understand, empathize, and at times compromise. I believe a worldview is not only for meaning-making, it also is for decision-making. This is the multiperspective view of *bricolage* (i.e., multiperspectival knowledge generation) [Kincheloe & Berry, 2004, p. 9]. There are times when our worldview should make us feel conflicted in our views, force us to confront our personal resilience, and make us choose either to challenge, concede, compromise, or change—that is the value of our worldview.

My worldview is considered as both pragmatic realist (Miles, Huberman, & Saldaña, 2014, p. 7) and critical realism (Maxwell, 2013, p. 43). As a pragmatic realist, I believe in the *real* world as it exists without human cognitive interpretation and people's imaginative explanations. I also believe that people construct their own perceptions and versions of the world through their personal experiences and by adopting other people's perceptions. Accordingly, conflicting views of the natural and human world are inevitable and must be reconciled through critical reasoning.

The world—life—is a mixture of human systems, technological systems, and natural systems. Each type of system exists within the physical boundaries of the earth's atmosphere and outer space as well as in the boundless creativity of people's minds. Indeed, spy satellite orbits and ballistic missile trajectories expand our systems boundaries beyond the earth's atmosphere. Our perception of the world is a "simplified and incomplete attempt to grasp something about a complex reality" (Maxwell, 2013, p. 43). The reality is, from my perspective, that we are part of something larger than ourselves.

The pragmatic side of this worldview is that our human constructs of institutions, infrastructure, culture, safety, or security are subject to the natural laws of our environment. Likewise, the natural environment is affected by our human constructs, which are based on our perceptions and belief systems (Capra & Luisi, 2014; Kincheloe & Berry, 2004). There is little to no separation among human populations, technology, and the natural world's intertwined systems of structures, processes, and functions, and purposes. These social, technological, and environmental systems and their components interact daily and will influence our future as much as they have our past.

History shows that people inherently look for meaning in nearly everything they experience and do. Humans tend to assign meaning to things, patterns, relationships, and our own intentions (Miles et al., 2014, p. 7) thus enhancing their perceptions of the real world. In addition to searching for meaning, we—people—also create it. We choose to create things, patterns, relationships, and ideas with good and bad intentions. Benevolent and malevolent intentions are evident in our actions and speech acts and reveal our true creative purposes. We are meaning-making and decision-making beings—purposeful systems—because we desire having a purpose in our lives that transcends just surviving (Ackoff & Emery, 2017, pp. 30-31). Hence, we want to be part of that big *something* and we want it to be meaningful.

Systems view. My approach to homeland safety, security, and resilience is grounded in the systems view of the world. This viewpoint begins with the interactive relationship between human systems and natural systems because both types overlap as an all-encompassing socio-technological-environmental (STE) system. Likewise, my viewpoint about the progressive relationships between meaning-making, decision-making, and problem-solving is grounded in the systems view of purposeful human systems (Ackoff & Emery, 2017; Capra & Luisi, 2014; Meadows, 2008). According to the University of Pennsylvania's Ackoff Collaboratory for Advancement of the Systems Approach (ACASA), there are four types of systems that exist in the world: (a) mechanistic, (b) animate, (c) social, and (d) ecological (ACASA, 2018). Accordingly, my understanding of the similarities and differences among humans, human-created mechanistic systems, human social constructs, and the natural ecological world underpins my systems view of homeland security. It shapes my approach to analyzing hazards, threats, crisis events, STE systems, and multidisciplinary all-hazards intelligence synthesis.

The four types of systems in the world are hierarchical in their structure meaning the larger natural ecological system subsumes the human systems of societies, individual people, and technology. Each type of system is conceptually and literally nested within the other and they are intricately intertwined. These tiers of systems lead to a better understanding of their interdependent roles in sustaining life and, consequently, the origins of disastrous crisis events. In addition to knowing the types of systems in the world, understanding how systems work is important to my research.

Systems have three basic components: (a) structure, (b) process, and (c) function or a purpose (Ackoff & Emery, 2017, p. 13). The interactions of these three components are essential to its function. System structures can be either tangible (e.g., a tree's roots, or a home's plumbing) or intangible (e.g., ideological beliefs or claims). The tangible structures of a system are more easily identifiable, measurable, and visually depicted in pictures, or descriptive text. The intangible structures of a system are better represented in the form of structured communication (e.g., formatted text document; verbal presentation; graphics) that is based on relevant data, claims, and supporting evidence.

System processes are the steps, phases, or methods taken by the system, within its structure, to achieve its function or purpose. A distinguishing system aspect is that technological systems typically have a functional objective whereas humans have a goal-oriented purpose and intent (Ackoff & Emery, 2017, p. 26). However, machine produced function and human created purpose can work together to accomplish a system's objective. For instance, typing this sentence is an intentional and purposeful activity that is aided by the functional word processing objective of my laptop; it's an interactive machine-human process with a shared objective.

Both function and purpose give meaning to a system's cooperative structures and processes. "A system is a set of things—people, cells, molecules, or whatever—interconnected in such a way that they produce their own pattern of behavior over time" (Meadows, 2008, p. 2). All three system components (e.g., structure, process, and function / purpose) coexist and form the basic components of human, societal, technological, and environmental systems (Ackoff & Emery, 2017; Capra & Luisi, 2014; Meadows, 2008). Another important characteristic of systems to be understood for my research is the types of relationships among systems and their components.

The types of relationships between system components and other systems determines how they will interact with each other. How these systems relate to and react with one another in either positive, negative, or neutral ways produce outcomes with sometimes devastating consequences (e.g., an industrial accident near a neighborhood). A holistic analytic view considers each of the three system components, the whole system, and all the connections among them to better assess what may emerge from their interactions. This is commonly stated as the sum of the parts is more than the whole meaning what comes from adding together the individual parts of a system is often more meaningful and complex than it appears to be.

A simple model of an intelligence synthesis system illustrates an open system that consists of inflows, stock, and outflows (Meadows, 2008, p. 18). Inflows of collected data are added to the stock of information while the knowledge generation process produces an outflow of actionable intelligence. Adding self-correcting critical examination as feedback loops within the process ensures higher quality, or quantity, of outflow intelligence products. This systems model explanation appears to be simple; however, systems and systems comprised of subsystems can be quite complex. For example, the intelligence synthesis system comprised of networked people, machines, and institutions within the national security intelligence community (IC) is a complex globally distributed system-of-systems.

“Components, whether cells or transistors, acquire new ‘causal power’ when they are organized into a mechanism that performs a higher-level function” (Verschuuren, 2017, p. 72). In other words, a system’s purpose and function can be complex and challenging to understand because what one sees in its structural and process elements is not always what one gets in return. Sometimes, there are unintended and unforeseen consequences when human, technological, and natural systems interact. I will briefly introduce these central types of systems before continuing with my worldview discussion.

Human systems. Human and social systems are purposeful systems because they exhibit intentional behavior demonstrated by setting goals and objectives. Purposeful systems also display an intent to change their behavior to achieve their goals especially when internal or external conditions change (Ackoff & Emery, 2017, p. 14). To better understand this concept, think of a criminal organization that is adaptive and changes its modus operandi according to its victim's vulnerabilities and law enforcement presence. Meanwhile, human created technological systems are not purposeful systems, but they do have a functional objectives. After all, they are created by humans as mechanical or digital machines for a reason.

Technological systems. A technological system, more specifically, has what is called a system objective that is its primary purpose. It also has a system function that is its underlying operational performance design meant to achieve the objective (Ericson, 2016, p. 11). In my research, I will equate the term *function* to the term *purpose,* so it will not be confused with a system's underlying processes. Finally, it is notable that natural systems are like human and technological systems because they too have structures, processes, and their own natural purpose or function.

Natural systems. An example of a natural system with easily identifiable elements is a hurricane. It has a visually recognizable eye, spiral and rotational form, and measurable wind speeds. A hurricane forms under certain climatic conditions, locations, and time of year in a pattern that is identifiable, discoverable, and measurable. As a natural weather phenomenon and cyclic climatic system, a hurricane takes in energy from the atmosphere and ocean, cycles it through its structure, and then discharges it in the form of powerful and potentially destructive winds and rain. A hurricane's hydrologic cycle and process reveals its natural purpose to transfer water between the ocean and the atmosphere and to transform kinetic energy from one state to another. In addition to the systems elements triad of structure, process, and function / purpose, this example highlights three more characteristics of systems, they are: (a) identifiable, (b) discoverable, and (c) measurable (Capra & Luisi, 2014, pp. 7-8).

Scientific disciplines. Systems-thinking is a holistic view of the world derived from the combination of experience and science (i.e. experiential epistemology) that are the sources of knowledge. Systems-thinking is influential in nearly all scientific disciplines from architecture to zoology and it frames the systematic study of matter and form. A holistic approach studies quantities and constituents as well as their patterns and relationships (Capra & Luisi, 2014, p. 4) and reveals the links among people, technology, and the earth. Systematic scientific research requires identifying and measuring the quantities and constituents of system elements, how they are related to each other, how they relate with other entities, and it recognizes their patterns and relationships. Matter and form, which are akin to structure and process, are essential to the system's elemental triad along with function and purpose. Two scientific disciplines, physics and chemistry, contribute to my systems view of homeland security. The constructal law of physics and the reaction process of chemistry both relate to the transformational processes that are inherent to crisis events and intelligence synthesis.

The constructal law of physics. The constructal law, a physics principle, asserts that all natural and human systems facilitate the efficient flow of energy, information, or even culture, from one system to another (Bejan & Zane, 2012). For instance, energy in a chemical reaction flows—transforms—from one state condition into another. Or, in the example of an exothermic reaction, releases energy into the environment. The flow of energy throughout the ecosystem, from the sun to our sources of food, is a natural law of physics.

Human systems also are subject to the flow principle. The authors state the constructal law “governs any system, anytime, anywhere, encompassing inanimate (rivers and lightning bolts), animate (trees, animals), and engineered (technology) phenomena, as well as the evolving flows of social constructs such as knowledge, language, and culture” (Bejan & Zane, 2012). Therefore, homeland security information sharing structures and intelligence synthesis systems also are flow systems that “evolve over time, acquiring better and better configurations to provide more access for the currents that flow through them” (Bejan & Zane, 2012).

I believe that the movement of energy, information, culture, and ideas in human and natural systems follow the principle of efficient flow even in the presence of obstacles. Although there are potential physical and virtual disruptions to flow, and multiple paths of least resistance that can be taken, the natural tendency is for energy and ideas to flow efficiently among systems. The advent of the telegraph, telephone, television, and the internet demonstrate a human tendency to technologically facilitate the flow of information in the fastest and most efficient manner possible between individuals and larger communities. Certainly, there will be disruptions, alterations, and even the destruction of flow systems by a wide range of threats. Furthermore, facts, falsehoods, and flood waters can flow from point-to-point, point-to-area, area-to-point, or area-to-area in both natural and human systems (Bejan & Zane, 2012, p. 4). The flow principle is relevant to the all-hazards analysis of STE systems as well as adversarial, cyber, technological, and natural (ACTN) threat systems because each have the capacity to either originate or facilitate the flow of destructive energy and ideology.

Three of the five preparedness missions of the National Preparedness Goal (NPG), which are named by their intended functional effects, are meant to prevent, protect, and mitigate the flow of potentially destructive energy in threat systems. In agreement with flow theory, the tendency for energy to transform hazards and threats into disastrous crises is a natural phenomenon regardless of the hazard source. Put in the context of the homeland security intelligence synthesis system, it is the all-hazards analyst's responsibility to understand the safety and security consequences about the flow of energy and information to better generate knowledge about social, technological, and natural threats.

Chemical reactions and state changes in chemistry. In a chemical reaction, substances are changed into other substances or compounds when they collide and transfer energy. This process is a change of state typically from a solid form of matter to a liquid or into a gaseous state (Moore, 2010, pp. 6-7, 87-88). Simply put, the chemical reaction process entails reactants interacting and then reacting with each to produce products of different types and states. This is a common occurrence in nature and laboratories and is in-line with the flow principle of the constructal theory. Like systems, the reaction process is recurring, identifiable, discoverable, measurable, and thereby predictable. Furthermore, it serves as another example of transformative processes in both natural and human systems regarding cause-effect and state changes and is applicable to the hazard, threat, and crisis event transformation model.

What is probable also is predictable and likely is preventable too; this is a common refrain in the security domain. The flow principle and chemical reactions both give to the rationality of this security mantra because they offer guiding principles for all-hazards analysts in understanding how hazards can transform into crisis events. The concept of entity state change from one condition to another, like the dormant to active to realized transformation continuum, applies to a natural hazard source, a technological mishap, and evidentiary data during the analysis process. The parallel flows of energy and information contribute to my systems view of all-hazards intelligence synthesis in two fundamental ways: (a) a dormant hazard condition becomes an active threat and then a realized disaster; and (b) analyzed data points become useful information and then synthesized applied intelligence. Energy and information (i.e., ideas) can experience state changes under the right circumstances.

Holism and reduction cognitive approaches. In addition to the systems construct of component structure, process, function, and purpose that is combined with the science principles about energy and idea flows, and transformational state changes, my worldview also includes two complementary concepts of holism and reduction. I should point out that by using the term *reduction* I am not advocating *reductionism*. Simply put, reduction is an analysis technique that reduces an object of study, an entity, to its elemental components or subentities. It is an analytic step in the systemic process of understanding the whole. Reductionism is a philosophy that emphasizes understanding is found primarily in the most elemental components with less regard for their relationships and emergent qualities (Verschuuren, 2017). A pure reductionism philosophy is contrary to holism, so I am focused on the analytic process of reduction.

Holism. A holistic view, which is strongly correlated with systems-thinking, considers the whole condition of an entity, event, or an act in its appropriate context. This holistic view emphasizes connections, relationship qualities, networks, nodes, and context as necessary properties for emergent conditions and outcomes. A holistic view of social, technological, and environmental systems helps with understanding how their entities relate and interact to create emergent patterns and themes thereby supporting the systems view that the sum of the parts is greater than the whole.

Holism also helps all-hazards analyst to anticipate outcomes and consequences thereby leaning towards a more predictable and preventable approach to homeland security. Anticipatory and risk-based (i.e., probability calculations and likelihood estimates) intelligence assessments are a more reasonable goal for an intelligence analyst and researchers because predictive analysis is a fallacy—we cannot accurately predict the future. By taking a holistic view, an all-hazards analyst is more likely to understand cause and effect relationships that have cross-domain, direct, secondary, and tertiary probabilistic consequences thereby better able to anticipate future scenarios.

Reduction. Complementing the holistic approach is reduction. It is not possible for an all-hazards analyst to understand the whole STE mix of people, machines, computers, and nature without first identifying their subsystems and parts. Reduction is the disassembly of a system into its components of structure, process, function and purpose and then into its subsystems and their constituent entities. Identifying the system's basic elements and their relationships are the first steps towards a holistic understanding of the entire system.

The system's hierarchy, or levels, is composed of layered building blocks called part-whole relationships with emergent properties at each level (Verschuuren, 2017, p. 21). All-hazards analysts may begin with dissection and identification of the system's parts, but they also should go a step further and recognize the system's emergent properties from a holistic perspective. Both approaches to intelligence synthesis, reduction and holism, are necessary systems-thinking and critical-thinking qualities.

Meaning-Making Conceptual Frameworks. Moving from systems theory, scientific principles, and cognitive concepts, the next influential conceptual framework in understanding all-hazards intelligence synthesis is the symbiotic meaning-making and decision-making relationship. Although each one can occur without the other, they are incomplete as stand-alone frameworks. Understanding can be attained without follow-on action and decisive action can be taken with little thought. Well informed and effective homeland security decisions on policy, standards, training, and operations must come after a comprehensive intelligence analysis and synthesis process. Good decisions that solve problems follow good analysis that attempts to make sense of the situation. In the preparedness and risk management processes of the DHS and the United States Army for example, the process steps are easily separated into meaning-making initial steps followed by decision-making final steps. It is a logical and necessary method of generating knowledge and action by following the meaning-making to decision-making to problem-solving continuum.

Two conceptual frameworks that are useful in making sense of an operational situation, environmental context, and change are the Panarchy theory and the Cynefin complexity framework (Brougham, 2015; Gunderson & Holling, 2002). The adaptive cycle, which comes from Panarchy, and the five Cynefin realms, ranging from obvious to disorder, provide invaluable context to the all-hazards analyst's understanding of the socio-technological-environmental domain. Existing within the adaptive cycle and the Cynefin realms are the populations, institutions, infrastructure, and environmental systems of the world. Accordingly, the hazard, threat, and crisis event interactive processes are found in these realms and the cycle. It is important to understanding how the adaptive cycle and the Cynefin realms apply to the homeland security operational environment and enterprise.

Panarchy. "Panarchy is an integrative theory to help understand the source and role of change in systems, and to identify development paths that are truly sustainable" (Gunderson & Holling, 2002, p. 2). It is an interdisciplinary systems approach to understanding that the human, technological, and natural worlds are linked together with far reaching cause-effect relationships. "Fundamental to panarchy is an understanding of the adaptive cycle—a pattern of rapid, opportunistic growth, conservation, destruction, and renewal—and the concept of scale" (Gunderson & Holling, 2002, p. 3). The adaptive cycle reveals the dynamic systems of the human and natural world through its four phases and its cyclical nature; therefore, it also is predictable under certain conditions. Thus, knowing the current phase, as well as the historical context, of the cycle allows an all-hazards analyst to anticipate likely future events.

Cynefin. The Cynefin framework realms of (a) obvious, (b) complicated, (c) complex, (d) chaotic, and (e) disorder also help the all-hazards analyst to assess the current situation and anticipate future conditions. The separation line between Panarchy and Cynefin is best explained temporally (i.e., by time). Panarchy is a broad view of natural cycles that also are human-influenced or human-caused that cycles over periods of time from months, years, or even extended periods of geologic time eras. Although it is applicable to other domains such as economics and business, it is better served as meaning-making model for long-term socioenvironmental cycles.

Cynefin realms offer a clearer perspective of the current operating environment as a model of identifying simple solutions to an obvious situation, for example, or for understanding how complexity contributes to uncertainty. It is better explained as a short-term situational awareness model that recognizes that systems are not always stable and that the state of a system will change over time (Brougham, 2015, p. 8). In this context, the adaptive cycle and the Cynefin realms help analysts with current situation and contextual meaning-making and helps the decision-maker with managerial decisions.

Security theories. Social and security theories attempt to explain why and how humanity manages hazards, threats, and crises of all types. These theoretical perspectives range from a pessimistic tinted realism to a more optimistic liberalism. A realist perspective tends to advocate the needs of the state over the individual as a matter of domestic or national security. A liberal viewpoint places the liberty of the individual higher with an emphasis on identifying and eradicating the causes of human insecurity. Another perspective is the environmental security point-of-view that places the earth and its ecosystems on an even higher priority level (Smith, 2015, pp. 12-30). Regardless of their differences, the inescapable link between each security perspective is the complex relationships among people, technology, and nature. In their own way, they all place people at the center of the security problem. The challenge for the all-hazards analyst is to balance human-centric, state-centric, and eco-centric perspectives while analyzing STE systems and their threats.

I believe the links among populations, technology, and the environment have become inseparable since the industrial revolution and the age of information (i.e., the internet age). The dependencies among environmental resources, cyberspace, economics, and society are meshed together as a single STE system. Thus, the need for a balanced human-centric and eco-centric meaning-making and decision-making process for homeland security that respects both human-centric and eco-centric views is self-evident.

In broad terms, the well-being of both people and the environment are ultimately linked to the safety and security of the individual person. This means human-centric policies and laws that ensure the dignity and well-being of the individual will lead to the respect and well-being of the planet (Hampson, 2013, pp. 279-294). The premise is that for both human systems and environmental systems to be safe, secure, and resilient, the civil liberties and civil rights of the individual should be respected first before moving on to the collective wants and needs of society and the world. This is the genesis of my homeland security worldview and of the homeland security and intelligence domains.

Homeland Security Operational Frameworks. Homeland security is one part of our overall national security framework. It is focused on ensuring the domestic safety, security, and resilience of our national interest and population from ACTN threats. The homeland security enterprise's partnership with the IC and other national defense institutions enhances the nation's domestic security and advances its national interest globally. From a federal government perspective, this framework places the DoD as the primary institution for national defense and the DHS as the primary institution responsible for domestic security. Arguably, law enforcement is a third security domain more narrowly focused on crime and criminals (i.e., all-crimes) therefore placing it within the homeland security's all-hazards domain which is a subdomain of the overarching national security domain (Carter, 2009, pp. 10-12).

As the lead department of the homeland security enterprise, DHS must coordinate the activities of numerous federal, state, local, tribal, and private sector agencies and organizations. The all-hazards STE setting of the homeland security enterprise is called the HSOE. Two look-angles helps describe the HSOE. The first is an institutional and operational-centric perspective (e.g., the DHS and the HSIE). The second is a threat-centric all-hazards environment viewpoint (i.e., the all-hazards HSOE).

The homeland security enterprise institutional and operational perspective. The homeland security enterprise consists of security entities at all levels of public service and private industry sectors. They are the enterprise stakeholders with vested interest in effective preparedness measures, generating response and recovery capacity, reducing risks, and increasing resilience. The collaborative effort of homeland security enterprise depends on the leadership and action of not only the DHS, but also other departments such as the Department of State, DoD, Department of Treasury, Department of Commerce, and the IC along with many other departments, agencies, and non-governmental organizations (NGOs) (Bullock et al., 2016, pp. 113-197).

The DHS's Office of Intelligence and Analysis "is the only element of the U.S. IC statutorily charged with delivering intelligence to our state, local, tribal, territorial and private sector partners, and developing intelligence from those partners for the Department and the IC" (DHS, 2018). As a DHS institution, this office facilitates all-hazards analysis, the production of intelligence products, and their dissemination to the network of state and urban area fusion centers, and public and private agencies where all-hazards analysts work.

The all-hazards homeland security operational environment perspective. All-hazards threats are defined as:

> an incident, natural or manmade, that warrants action to protect life, property, the environment, and public health or safety, and to minimize disruptions of government, social, or economic activities. It includes natural disasters, cyber incidents, industrial accidents, pandemics, acts of terrorism, sabotage, and destructive criminal activity targeting critical infrastructure. (National Response Framework, 2016, p. 7)

Additionally, all-hazards and their related crisis events are grouped into three categories: (a) natural, (b) technological/accidental, (c) and adversarial/human-caused (The strategic national risk assessment, 2011). Thus, the all-hazards approach is the focal point of homeland security preparedness goals, core mission sets, operational strategy, and the risk management process.

The all-hazards approach to homeland security serves as both a forcing mechanism for policy formulation and an enabling means for capacity generation. “Developing and maintaining an understanding of the variety of risks faced by communities and the Nation, and how this information can be used to build and sustain preparedness, are essential components of the National Preparedness System” (National Preparedness System, 2011). By identifying, analyzing, and assessing common hazards and threats through the intelligence synthesis and risk management process, the homeland security enterprise is forced to prioritize each threat and make preparedness policy and budgetary decisions. The next step of integrating the threat assessments into the preparedness system and homeland security framework is to formulate policy, develop plans, and to properly resource homeland security practitioners.

Personal and professional experience. The final two lenses that contribute my worldview and approach to homeland security are my personal experiences with human-caused and natural disasters, and my professional experience as a United States Army Military Intelligence Officer. Specifically, my local community and my parent's home flooded during Hurricane Harvey with significant un-insured property losses requiring federal assistance through the Federal Emergency Management Agency (FEMA). Other volunteer organizations and non-governmental organizations generously contributed labor and other resources to the response and recovery efforts in my neighborhood and for my parents.

While I was in the military, I served during Operation Desert Storm to protect critical military assets and I participated in Operation Provide Comfort to provide humanitarian assistance to the Kurdish people. As an intelligence officer in the Korea Theater of Operations, I directed the intelligence process, intelligence production management, analysts professional training, and the military decision-making process from various security and safety operational levels and management. During my nearly 22-year career, I was a recipient of risk-informed all-source intelligence assessments and I managed the production of both single-source and all-source products. I also have experienced personal loss that is similar to the loss experienced by others in crisis situations. I only call attention to these professional and personal experiences because they have significantly shaped my worldview of safety, security, and resilience at home and abroad.

Approach. My all-hazards analysis research approach narrows my worldview into a more focused homeland security perspective and guides how I will design my research methodology. I will approach all-hazards analysis research within the frameworks of balancing respect for human and natural systems, applied qualitative research with emphasis on the needs of the homeland security practitioner (i.e., all-hazards intelligence analysts), and a grounded knowledge in my own experience and scientific enquiry. This is a constructed research approach that is built on my personal worldview, my professional experiences, and with those I have adopted from other researchers and practitioners during my security studies and the literature review process (Maxwell, 2013, p. 41).

Human-centric and Eco-centric. There is no escaping an interconnected world of natural systems, human systems, and technological systems. I believe the best approach to sustaining the well-being of humanity today and posterity, is to advance complementary human-centric and eco-centric security frameworks, governmental policies, and operational action plans. World, national, and local leaders, both public and private, are obligated to ensure the safety, security, and resilience of people, wildlife, and natural resources. Consequently, human-centric and eco-centric policy decisions should be hard to make when the needs of one problem challenges the other. I believe struggles in problem-solving concerning humanity and nature are unavoidable if its grounded in the mutual respect for both. Otherwise, it would be too easy to choose one over the other and open the door for opportunistic exploitation. I also hold onto the optimistic belief that equity is possible and the sustainment of one system should not discount the prosperity of the other.

Applied research and the homeland security enterprise. "Applied research uses the scientific methodology to develop information to help solve an immediate, yet usually persistent, societal problem" (Bickman & Rog, 2009, p. x). My purpose in taking an applied research approach is to provide usable knowledge to produce a practical solution to all-hazards analysis in the HSIE. I also will take a United States DHS and HSIE research perspective. Thus, my findings will primarily be directed towards national level homeland security all-hazards analysts, their associated intelligence and information sharing communities-of-practice, and security studies researchers. I am concerned with real-world outcomes directly related to the problem of insufficient DHS all-hazards analysis frameworks and unifying conceptual models.

Qualitative, epistemological, and ontological research approaches. My research will be almost exclusively qualitative. I will focus my efforts on exploring and examining the works of other researchers and authors to better understand how all-hazards analysis is currently conducted in the HSIE. I will not concentrate on statistics or other quantifiable research data by itself because my approach is to qualitatively understand the structures, processes, and functions of the all-hazards intelligence synthesis system that is in use. I will draw upon my own experiences as an all-source intelligence officer and research the all-hazards analysis process to gain an empirical, ontological, and qualitative perspective of the research problem. This ontological realism perspective (i.e., there is a real world independent of our perception) and the epistemological constructivism perspective (i.e., we construct our own understanding of the world) is compatible with my pragmatic realist / critical realism worldview (Maxwell, 2013, p. 43).

The benefit of this approach is its “pragmatic compatibility” (Maxwell, 2013, p. 6) that allows me to design my research method around a flexible literature review framework. In this way, I can allow my research to flow from any source and into any direction that generates knowledge on my subject. By not following a rigid method, I am free to move among the different information sources that are available to me in peer-reviewed articles, documentaries, government publications, direct observation and experience, and textbooks.

Thus far in my research, I have followed leads from one author to another and one DHS publication to another only to discover new data points, references, and ideas on all-hazards analysis. This spontaneous and adaptive approach to qualitative research is known as bricolage and it already has helped me to create the baseline ISM and the AH-ISM. As a bricoleur, I adapt “to the situation, creatively employing the available tools and materials to come up with unique solutions to problems” (Maxwell, 2013, p. 42). So, what I will offer in chapter V will be a new and different way of looking at on old problem.

Design. My research design follows my multiple perspective, qualitative, homeland security, and applied research approach by fusing material and ideas from other author’s research, doctrinal publications, and professional experience. My literature review covered three broad topics of homeland security, intelligence, knowledge management, and risk management as well as other related subtopics. Additionally, I read textbooks and government documents on environmental security, technological hazards, terrorism, hazard analysis, research methods, structured analytic techniques, and their related publications. The result of this research is an overall design that fuses established qualitative research methods with a practical analysis model.

I concluded my literature review by forming a universal baseline ISM and an HSIE-centric AH-ISM that will be analyzed and discussed in chapters IV and V. Thus, I began my research and comprehensive literature review in an exploratory manner and concluded it with applied research products. My exploratory goal was to learn more about all-hazards, all-hazards analysis, and the potential application of intelligence analysis models in the HSOE. My confirmatory goal was to build upon my preliminary concepts of the intelligence synthesis and all-hazards analysis models. I will offer explanations of my findings and an all-hazards analysis prescription at the end of my applied research journey in the form of the two intelligence synthesis models. My research design combined reputable qualitative exploratory, confirmatory, and descriptive research methods with my own analysis model to offer a prescriptive conclusion (Maxwell, 2013; Miles et al., 2014; Newsome B. O., 2016; Onwuegbuzie & Frels, 2016).

The overall design of my research followed the qualitative research analysis approach and comprehensive literature review method presented by three research publications:

- *Qualitative research design* by Joseph A. Maxwell for his conceptual framework of qualitative research and design.
- *Qualitative data analysis* by Matthew B. Miles, A. Michael Huberman, and Johnny Saldaña for their focused, sequential, and visualized data analysis methods.

- *7 Steps to a comprehensive literature review: a multimodal and cultural approach* by Anthony J. Onwuegbuzie and Rebecca Frels for their methodological approach to conducting a multisource literature review.

I selected these references for their in-depth explanations, examples, and visualizations on qualitative research, methods, and data analysis. They are companion resources to my own analytic approach. Additionally, I applied the ISM that I created during my initial literature review to my final research product. In fact, these intelligence synthesis models comprised my orientating ideas that I intended to confirm during this research process (Miles et al., 2014, p. 23). My research design is a combination of qualitative data analysis methodologies and my own intelligence synthesis model. Together, they form the structure of my research methodology.

Common Terms and Definitions

Throughout my thesis, I use terms with definitions that I formed (i.e., synthesized) during my literature review. It is common for different authors and government institutions to use similar terms with varying meanings depending upon their contextual usage. These terms and their definition amalgamations, which I use, are intended to clarify their meaning throughout my research:

- Activator: the cause of an active threat resulting from its interaction with a dormant hazard (non-threatening hazard state).
- Analysis: the organized method of reducing, relating, and evaluating the components of an entity or system to generate synthesized information and actionable intelligence. It is essential to the intelligence synthesis system of meaning-making and decision-making.

- Assessments: an all-inclusive term for pre and postmortem analytic products, forecast, anticipatory intelligence reports, presentations, and other materials created for intelligence customers to be used in meaning-making and decision-making.
- Crisis Events: the realized consequence of the interaction between an active threat and a socio-technological-environmental system with the potential to cause harm to life, information, operations, property, and the environment.
- Entities: people, places, things, or concepts that have spatial, temporal, and identifiable attributes that are detectable and measurable.
- Framework: provides a uniform structure, taxonomy, and mindset within a community-of-practice to guide effective communication, collaboration, coordination, and productivity. A conceptual framework can be communicated to its audience in textual documents or visual models.
- HARTE: hazard-activator-relationship-threat-event (HARTE) all-hazards transition and analysis model.
- Hazard: the source of a potential threat in a harmless or dormant state.
- Homeland security enterprise: all public and private organizations directly involved in ensuring the safety, security, and resilience of the nation's socio-technological-environmental assets and resources.
- Homeland security intelligence enterprise: all DHS and other intelligence and information sharing entities of the Federal, state, tribal, regional, and

local levels of government. The homeland security enterprises' intelligence community-of-practice.

- Intelligence: the process and the products associated with the generation of knowledge for meaning-making and decision-making.
- Model: a communication tool for simplifying and visualizing a conceptual framework, system, structure, process, method, physical object, or idea. It is used for describing, explaining, or analyzing what it represents.
- Pluralistic intelligence: in a homeland security domain context, is defined as an interdisciplinary approach to generating all-hazards knowledge and providing risk-informed applied intelligence products to homeland security enterprise leadership and practitioners in support of the National Preparedness Goal
- Population: all people who are citizens, non-citizens, or transients present in a nation, state, region, territory, tribe, or municipality.
- Relationships: the links or connections among entities that give or strengthen their meaning, function, purpose, process, structure, or productivity.
- Socio-technological-environmental system: the interdependent assets and resources of the human, technological, and environmental systems of the world.
- Synthesis: the comprehensive and pluralistic fusion of relevant data, information, knowledge, and intelligence that is derived from multiple

intelligence and operational sources, disciplines, agencies, and jurisdictions for producing applied intelligence products.

- System: a dynamic, adaptive, nonlinear network of entities, relationships, elemental structures, and processes that has a function or purpose.
- Threat: the active source of a potential or realized crisis event.

CHAPTER II

Literature Review

My literature review of government publications, text books, and academic articles are grouped into nine topic areas that are relevant to domestic all-hazards intelligence analysis in the United States: (a) the homeland security domain, (b) the all-hazards homeland security operational environment, (c) the intelligence domain, (d) privacy, civil rights, and civil liberties, (e) knowledge management and information management, (f) risk management, (g) emergency management, (h) law enforcement, and (i) environmental sciences. I grouped the literature topics and their subtopics like this because each group is dependent upon the other to ensure our national population and ecosystems are safe, secure, and resilient according to the DHS's vision. Lastly, the literature review chapter is intended to serve as a backdrop for the overall research and analysis processes that I conducted. The information in this chapter summarizes key research points found in the literature; analysis is provided in chapter IV.

Within these nine interdisciplinary categories of all-hazards intelligence relevance, are numerous subtopics about public and private sector hazards and threats analysis approaches that are discussed by the authors in the contexts of domestic safety and security; national critical infrastructure security; business management; law enforcement; crisis management; and social and environmental vulnerabilities. Other topics focused on structured analytic techniques, data sources, national information collection platforms, and professional training and certification programs for practitioners. These literature sources were written for audiences ranging from new security studies students at the university level to career practitioners in self-study programs wanting to enhance their content knowledge or advance their careers in the safety and security fields.

The Homeland Security Domain

The DHS publishes documents that are written to advise, inform, and guide public and private sector practitioners in the public safety and security fields while highlighting the need for resilience at all levels of government from municipal to federal. These documents are publicly accessible on the internet and are doctrinal in their approach to the homeland security enterprise's all-hazards operational planning and mission execution tasks. They are written to define, describe, and explain the all-hazards security environment and to provide a common knowledge base on how the homeland security enterprises' public and private sectors communicate, coordinate, and collaborate to accomplish our nation's preparedness missions. They are intended to doctrinally unite multiple scientific disciplines, academic institutions, governing jurisdictions, and private and public departments, agencies, and sectors across the federal, state, local, tribal, and territorial (FSLTT) safety and security enterprises.

These publications also address the diversity of structures, processes, and functions that are inherent to the myriad of institutional and infrastructural systems that comprise the all-hazards homeland security enterprise. Altogether, the public-private partnership (P3) concept of a whole community-of-practice in the homeland security enterprise is thematic in these publications. However, often there is ambiguity in the usage of the terms regarding hazards and threats and all-hazards analysis methodology.

The following publications either directly contributed to or strongly influenced my preliminary findings and literature review of the homeland security enterprise, the

HSIE, and the all-hazards HSOE. I chose to review and summarize key points from DHS publications individually in my literature review chapter because of their direct influence on the homeland security intelligence and operations domains. On the other hand, in the subsequent literature review sections, I chose to provide a consolidated summary of the publications. Although I did not cite each one in the following sections of my literature review, all the reviewed publications should be recognized before proceeding:

- DHS *Risk Lexicon (2010).*
- DHS *Instruction Manual 262-12-001-01 DHS Lexicon Terms and Definitions (2017).*
- U.S. Army ATP 5-19, *Risk Management publication (2014).*
- DHS *Risk Management Fundamentals (2011).*
- DHS *National Preparedness Goal (2011).*
- DHS *National Preparedness System (2011).*
- DHS *National Incident Management System (2017).*
- DHS *Federal Interagency Operational Plans (2016).*
- DHS *Planning Frameworks.*
- DHS *Threat and Hazard Identification and Risk Assessment Guide (2013).*
- FEMA *Multi-Hazard Identification and Risk Assessment (1997).*
- FEMA *Understanding Your Risks* (2001).
- FEMA *Developing and Maintaining Emergency Operations Plans (2010).*
- DHS *Considerations for Fusion Center and Emergency Operations Center Coordination (2010).*
- *Homeland Security* by Charles P. Nemeth (2013).

- *Homeland Security and Terrorism* by James J. F. Forest, Russell D. Howard, and Joanne C. Moore (2014).
- *Introduction to Homeland Security* by Jane A. Bullock, George D. Haddow, and Damon P. Coppola (2016).

All-hazards lexicon and operational approaches. The terms *hazards* and *threats* are used extensively throughout the DHS's publications. Often, the two terms are used interchangeably (e.g., hazards and threats, or hazards/threats) indicating they are identical with similar characteristics in the context of safety and security. Although their definitions as stated in glossaries and risk lexicon publications separate the two terms in a distinct manner, this ambiguity in their usage within the text and in the provided context in DHS publications increases the risk of misunderstanding by the readers. Also, inter and intradepartmental miscommunication could result because of the inconsistent or inaccurate conceptualization of hazards and threats during analysis and in published assessments.

DHS Risk Lexicon publications. These publications, DHS Risk Lexicon and DHS Lexicon Terms and Definitions, defines the terms most commonly associated with homeland security and risk management by the DHS and the homeland security enterprise. Although the terms *hazards* and *threats* are often used interchangeably or together as a single entity in most DHS publications, these publications identify two common and one differing characteristic of hazards and threats. First, their origins are either natural or human caused. Second, they have a cause-effect relationship as either the cause of or having the potential to cause harm to "life, information, operations, the environment, and/or property" (DHS risk lexicon, 2010, p. 36). Third, they differ in that a threat is directed at an entity whereas a hazard is not (DHS risk lexicon, 2010, pp. 17, 36). Therefore, these definitions are indicative of a transformative change of state that occurs from a hazard into a threat. Stated another way, an identifiable change in condition is detectable from an objectiveless dormant hazard with hazardous potential when it becomes an active threat that is target-oriented. At this phase, the hazard becomes an actualized threat with increased potential to cause harm to a target.

U.S. Army ATP 5-19, Risk Management publication. The United States Army's approach to defining hazards and threats is explained in its 2014 risk management publication, Army Techniques Publication (ATP) 5-19 *Risk Management* that is approved for public release and available online. I reviewed this document because of the Army's extensive experience with inherently dangerous missions and operational environments. Thus, its risk management techniques are worthy for comparison to other security departments such as DHS.

To maximize unit capability, save lives, and preserve resources through its risk management process, the U.S. Army defines hazards as conditions with potential to cause injury, illness, or death of personnel; damage to or loss of equipment or property; or mission degradation, and create potential for harmful events (Department of the Army, 2014, pp. 1-2, 1-4). Additionally, hazards increase risk for specific events when they interact with people, equipment, or the environment. The term *threat* is not defined or used in this publication. Enemy actions and their effects, however, are considered and included in the Army's holistic all-hazards approach to risk assessments. For example, the effects of enemy artillery near possible snow avalanche slopes resulting in blocked routes is an example scenario used in the publication showing cause and effect possibilities (Department of the Army, 2014, p. 4-10). Understanding the historical and environmental context, having situational awareness of enemy effects and other hazards, and familiarity with the sequence of events in the state changes from a hazard to an event are essential to the Army's risk management process.

DHS Risk Management Fundamentals publication. The DHS Risk Management Fundamentals publication adheres to the hazard and threat definitions of the DHS Risk Lexicon publication. However, it offers more context by explaining the potential sources of hazards as either internal or external (Risk Management Fundamentals, 2011, p. 13). This is a mindset clarifier for analysts when choosing an analytic perspective to identify and assess hazards and threats. Another clarifier in this publication is categorizing hazards and risks as either strategic, operational, or institutional (Risk Management Fundamentals, 2011, p. 14).

Strategic hazards are directed towards an entity's higher-level assets such as an institutional or governmental hierarchy. An example is an adversary leveraging social media to sway national elections four years from now. Operational hazards are directed towards an entity's capacity responsible for the carrying out its tasks or missions. An example is a hurricane forecasted to hit a metropolitan area's thriving business district or a travel and tourism industry cruise ship. Institutional hazards and risk are primarily internally focused on an institution's capacity to carry out its mission or operational function. An example would be corrupt or flawed accounting practices that result in corporate bankruptcy or a non-governmental organization's loss of charitable contributions. These analytic perspectives of internal, external, strategic, operational, and institutional all contribute to the expanded understanding of hazards, threats, events, and their context.

Another contribution of the DHS *Risk Management Fundamentals* publication is that the 6-step risk management process emphasizes the significance of context in assessing hazards and risk. Context includes the historical, time, relational, political, and environmental aspects surrounding an entity or event. This publication list 9 contextual variables to be considered when analyzing hazards and designing hazard scenarios in the meaning-making phases as well as the decision-making phase (Risk Management Fundamentals, 2011, pp. 16-18). The significance of context variables is another cross-cutting theme throughout the reviewed literature.

The DHS risk management process can be divided into the first three steps dedicated to meaning-making and last three steps dedicate to decision-making (Risk Management Fundamentals, 2011, p. 15). These halves of the hazards and risk analysis process are a fundamental concept in all analytic frameworks that are driven by policy formulation, planning, and practical application. The DHS risk management process follows the meaning-making to decision-making to problem solving continuum.

DHS National Preparedness Goal publication. The National Preparedness Goal is to provide a secure and resilient nation across the whole community of the nation's population and practitioners. This publication establishes safety (implied), security, and resilience as national goals to be achieved by the whole homeland security enterprise community. The whole community is everyone with a stake in preserving our nation's way of life including volunteer citizens, elected officials, law enforcement officers, and all-hazards analysts. The whole community concept extends beyond the individual to just about any public, private, for profit, and not-for-profit organization that is either directly or indirectly involved with the five preparedness missions (e.g., prevent, protect, mitigate, respond, and recover) to hazards, threats, and crisis events at any level from local to national (National Preparedness Goal, 2015).

The National Preparedness Goal publication also explains the four types of hazards that our nation must be prepared to manage: (a) adversarial, (b) cyber, (c) technological, and (d) natural (National Preparedness Goal, 2015, pp. 4, 5). The examples of each type of hazard given in the National Preparedness Goal include weather related storms, infectious diseases, accidental hazardous materials, terrorism and crime, and cyberattacks on critical infrastructure. These four types of hazards have the potential to become threats to our nation's social systems, technological infrastructure, and environmental resources.

DHS National Preparedness System publication. The National Preparedness System builds upon the logical and sequential relationship between meaning-making and decision-making with its 6 mission area components that are focused on capacity generation. These capacity-centric mission areas are preceded by the analytic task of hazard and risk identification and assessment. Identifying and understanding the ACTN hazards and threats to the national preparedness capacity generation institutions and process are critical to overall national resilience efforts.

It is in this National Preparedness System publication that the purposes of the *Threat Identification and Risk Assessment* (THIRA) and the Strategic National Risk Assessment (SNRA) publications are introduced to the homeland security enterprise. These documents, along with specialized risk assessments, "provide an integrated picture of the risks facing our Nation" (National Preparedness System, 2011, p. 2). National safety, security, and resilience capacity generation is the focus of the National Preparedness System that is driven by risk-informed applied intelligence that is based upon threat identification and risk assessments.

DHS National Incident Management System publication. The *National Incident Management System* (NIMS) publication is a detailed set of guidelines for the whole community of public and private sector security practitioners who implement the five preparedness missions of the National Preparedness Goal. This document specifically addresses operational systems such as the Incident Command System (ICS), Emergency Operations Center (EOC), and Multi-Agency Coordination Groups (MAC Groups). It guides homeland security enterprise in resource management, command and coordination, and communications and information management (National Incident Management System, 2013, pp. 1-2).

It is in the NIMS document that variations of the terms *hazards*, *threats*, and *events* are identifiable. The NIMS glossary defines hazards and threats the same way as the Risk Lexicon publication and the two terms are often used together. However, the significant term difference is with the use of the word *event*. In NIMS, an event is a planned non-emergency activity and it is replaced by the term *incident* as a realized crisis (National Incident Management System, 2013, p. 68). In my literature review, the use of the term *event* also could indicate an emergency, incident, disaster, or catastrophe so I will clarify its usage with the all-inclusive term *crisis event*. A crisis event, whether an incident, disaster, or catastrophe, requires a coordinated response to protect life, information, operations, property, and the environment.

Another key term that is important to the all-hazards analyst is defined in the NIMS publication. The process of *analysis* is explained in the context of incident management with clearly identified tasks of data validation, support to decision-making, reductional analysis, relational analysis, timeliness, and awareness of information gaps. Like the concept of hazard maturation and transformation into a crisis event over a period of time, the NIMS definition of analysis points out the need to "turn raw data into information that is useful for decision-making" (National Incident Management System, 2013, p. 56). The explanation about analysis that is found in the NIMS document indicates a narrowing of doctrinal and policy emphasis by DHS in its publications from a macro to micro viewpoint.

DHS Federal Interagency Operational Plans. The Federal Interagency Operational Plans (FIOP) tie together the roles and responsibilities of the federal homeland security community to accomplish the five preparedness missions. They are written to guide the collective response across the public and private sectors and within the governmental hierarchy of federal, state, local, tribal, territorial, and insular areas. They also address core responsibilities, critical tasks, and resourcing requirements at the Federal level (Overview of the Federal Interagency Operational Plans, 2016). The core capabilities of the preparedness missions that are identified in the FIOPs also highlight the importance of the Intelligence and Information Sharing core capability that supports each mission area. The essential need for comprehensive all-hazards intelligence analysis and multidisciplinary all-hazards analysts is reiterated in the FIOPs.

DHS Protection Federal Interagency Operational Plan. The Prevention FIOP is a For Official Use Only (FOUO) document and is not available online. However, the seven prevention core capabilities (e.g., planning, public information and warning, operational coordination, forensics and attribution, intelligence and information sharing) are briefly discussed in the FIOP overview publication with Intelligence and Information Sharing being one of them. The Prevention FIOP is primarily focused on terror threats and includes prevention measures directed towards chemical, biological, radiological, nuclear, or explosive (CBRNE) weapons and cyberattack methods as well as countering radicalization and violent extremism (Overview of the Federal Interagency Operational Plans, 2016, p. 1).

DHS Protection Federal Interagency Operational Plan. Appendix 3 to Annex B of the Protection FIOP explains the Intelligence and Information Sharing core capability. It is one of 11 protection core capabilities along with cybersecurity. The eleven protection core capabilities are: (a) planning, (b) public information and warning, (c) operational coordination, (d) access control and identity verification, (e) intelligence and information sharing, (f) interdiction and disruption, (g) screening, search, and detection, (h) physical protective measures, (i) risk management for protection programs and activities, (j) cybersecurity, (j) supply chain integrity and security. This appendix delves deeper into the specific tasks and responsibilities of all-hazards analysis and analysts in the federal agencies that are dedicated to identifying and assessing hazards and threats to public safety and security. These critical tasks include information sharing, collaboration, coordination, training, analysis, and production of actionable intelligence. These tasks validate the all-hazards analysts' responsibility to turn raw data into actionable intelligence for decision-makers as well as the need for training programs to teach multidisciplinary analyst in all-hazards analysis methodologies (Protection Federal Interagency Operational Plan, 2016, pp. B.3-1).

DHS Mitigation Federal Interagency Operational Plan. Appendix B of the Mitigation FIOP identifies the critical tasks of Threats and Hazards Identification (THID) and Risk and Disaster Resilience Assessment (RDRA) in support of the mitigation core capabilities (e.g., planning, public information and warning, operational coordination, community resilience, long-term vulnerability reduction, risk and disaster resilience assessment, and threats and hazards identification). Aside from the THIRA document, this is the first appearance of specific instructions and tasks from DHS on how to perform all-hazards analysis in a publicly accessible operational level document.

The THID and RDRA process are two of the seven mitigation core capabilities and are cross-cutting capabilities that support all five preparedness mission areas' core capabilities. THID and RDRA also are conceptual models that are at the heart of all-hazards intelligence, meaning-making, and decision-making in the homeland security environment. Specifically, the mitigation FIOP states THID and RDRA "will inform and drive operational guidance in the other National Planning Frameworks" (Mitigation Federal Interagency Operational Plan, 2016, p. 7).

This document also explains the differences between steady state operations and incident-driven operations. This means intelligence support also is conducted in a steady state and in a reactionary state to support the National Preparedness Goal. Additionally, three elements of consideration are identified for integration of intelligence and operations: (a) internal, (b) horizontal, and (c) vertical. These integration considerations are meant to ease the unity of effort among HSIE partners within their organizations (i.e., internal), across communities-of-practice (i.e., horizontal), and up and down the hierarchical organizations (i.e., vertical). Altogether, these operational states and integration considerations are easily integrated into the framework of intelligence analysis and product dissemination within the HSIE (Mitigation Federal Interagency Operational Plan, 2016, p. 29).

The Mitigation FIOP provides an in-depth explanation on how and why the THID and RDRA conceptual models and process are integrated into each preparedness mission area. This FIOP's emphasis on the reliance of all mission areas on actionable intelligence to achieve safety, security, and resilience is apparent. The Mitigation FIOP and the THIRA document are closely related in their intent to guide all-hazards analysis and offer analysts with conceptual models and methods to follow in their work.

DHS Response Federal Interagency Operational Plan. The Response FIOP identifies 15 core capabilities all requiring all-hazards analysis and assessment support. Although Intelligence and Information Sharing is not specifically identified as a response capability, all the response capabilities and their associated Emergency Support Functions (ESF) need it. Situational Assessment is the one response core capability that requires a direct link to all-hazards analysis and assessment. This is an incident-driven operation that must have real-time intelligence support to assess the current situation and its immediate threats and likely causes.

Table B.1-1 on page B.1-2 of the Response FIOP identifies common natural, technological, and human-caused hazards and threats at the national strategic and operational levels in accordance with the SNRA and THIRA. These are some of the hazardous incidents that are likely to require implementing the National Incident

Management System and the Incident Command System (ICS). Incident Commanders and emergency response personnel rely upon incident-driven tactical intelligence, which is backed by on-going steady-state intelligence assessments, to understand their response requirements to save lives, protect property, and the environment (Response Federal Interagency Operational Plan, 2016). The response preparedness mission area is almost exclusively incident-driven because its framework is "based upon a no-notice incident" (Response Federal Interagency Operational Plan, 2016, pp. B-12). The mitigation and recovery mission areas are primarily steady-state intelligence centric whereas the prevention and protection mission areas depend on both steady-state anticipatory assessments and quick-response tactical intelligence information to interdict or eliminate threats before a crisis event occurs.

DHS Recovery Federal Interagency Operational Plan. The Recovery FIOP identifies eight core capabilities (e.g., planning, public information and warning, operational coordination, economic recovery, health and social services, housing, infrastructure systems, natural and cultural resources) and, like the other FIOP core capabilities, requires actionable all-hazards intelligence for it to be carried out. An intelligence specific capability is not recognized in the recovery phase. However, coordination, planning, warning, and other recovery oriented public services cannot begin without an informed decision-making process that is backed by a systemic meaning-making process as well as action-based intelligence assessments of the environment, population, resources, and infrastructure (Recovery Federal Interagency Operational Plan, 2016).

DHS Threat and Hazard Identification and Risk Assessment Guide publication. The THIRA publication provides the all-hazards intelligence community-of-practice with a broad doctrinal approach to all-hazards identification, analysis, and assessment. The key points for all-hazards analysts in this publication are included in the 4-step THIRA process: (1) identify threats and hazards, (2) give them context, (3) establish capability targets, and (4) apply the results. Additionally, THIRA emphasizes the whole-community approach to understanding hazard and threat categories as well as emphasis on understanding their context (e.g., timing, location, history, conditions) for communities to build emergency management, economic, and overall preparedness capacity [THIRA Guide, 2013, p. 9].

FEMA Multi-Hazard Identification and Risk Assessment publication. The FEMA publication on multi-hazards is over 20 years old but it is still available online. The *multi-hazards* term is now replaced with *all-hazards* and is the term I will continue to use. The publication is an excellent source of knowledge for arranging natural hazards into types and source regions such as atmospheric, geologic, hydrologic, seismic, volcanic, wildfire, and technological hazards. It also addresses these threats in the context of the STE relationship between human engineering and nature.

FEMA Understanding Your Risks publication. The FEMA publication 386-2 *Understanding Your Risks* also is outdated but it serves as a guideline for all-hazards analysts and practitioners in their understanding of systemic processes that incorporate analysis and assessments in the mitigation of crisis events. A *note of interest* is this document identifies four important characteristics in all-hazards analysis and risk assessments in four clearly stated statements on page iii: (a) threat interaction with communities, (b) types of assets, (c) vulnerabilities, and (d) consequences. These four points emphasize the need for understanding the consequences of an active target-oriented threat when it encounters a community or other natural resource vulnerabilities.

FEMA Developing and Maintaining Emergency Operations Plans publication. The Comprehensive Preparedness Guide (CPG) 101 is a FEMA publication guiding the whole community of the homeland security enterprise on the development of emergency operations plans. The significance of this planning document is its emphasis on the community-based planning process that considers the nation's population. This guide expands upon nearly all preparedness, planning, operational execution, and intelligence and information capabilities that are discussed in the collective DHS and FEMA documents that I have reviewed so far. Developing and executing emergency operations plans, as explained in this publication, requires the whole community of meaning-makers, decision-makers, and problem-solvers. The next set of DHS publications are guiding frameworks based on the five preparedness missions for the whole community in its safety, security, and resilience efforts.

DHS Planning Frameworks. The five national preparedness mission areas of prevent, protect, mitigate, respond, and recover that are outlined in the DHS *National Preparedness Goal* publication are explained in more detail in separate national framework publications. Each of the frameworks outlines a common conceptual understanding of the collaboration, planning, and operational efforts for all-hazards practitioners. Similarly, the risk management framework is published by the DHS for the same purpose. The nesting of these frameworks within overarching doctrinal concepts gives the whole community of diverse homeland security practitioners a common set of principles to follow. In turn, this allows for more cohesive safety, security, resilience, and preparedness policy and procedures that are based on proven conceptual models, effective continuity plans, and valid decision points. Together, these frameworks guide the building of national preparedness capacity.

National Prevention Framework. The *National Prevention Framework*, like all DHS framework publications, is a whole community approach guideline that spans across all public, private, and non-profit sectors of our nation's communities of populations and practice in their prevention mission area efforts. This publication identifies the numerous federal, state, local, tribal, regional, metropolitan, and territorial organizations and agencies that contribute to intelligence analysis and their coordination structures. It is one of the many DHS documents that includes orientational information for all-hazards analysts who need to understand the HSOE.

The *National Prevention Framework* is terrorism centric with a law enforcement emphasis on all-crimes. It identifies cyber threats as a unique security threat because cyberspace now is essential to the homeland security enterprise's preparedness efforts. The National Prevention Framework recommends integrating cyber-threat analysis tasks in its core capabilities (National Prevention Framework, 2016, p. 4). Although the threat of terrorism is central to the prevention mission set, an all-crimes approach serves as a reminder to analysts that other types of crimes and criminals threaten domestic tranquility daily.

National Protection Framework. The *National Protection Framework* offers similar lessons for the all-hazards analyst as the prevention framework with added emphasis on steady-state and incident-driven operations. While prevention looks outward and is threat target-focused, protection looks inward at threatened social, technological, or environmental targets to be more risk-based. This operational distinction is important for all-hazards analysts to better understand their analytic approach and role in intelligence support to the preparedness mission areas.

*National Mitigation Framework***.** The *National Mitigation Framework*, like the Mitigation FIOP, is an informative and explanatory DHS publication. It has visual depictions of the coordinating structures, concepts, procedures, hazards and threats, of the whole community that are ideal for informing the all-hazards practitioner of the public and private sector's mitigation efforts (National Mitigation Framework, 2016). Moreover, it is the DHS document that robustly addresses the necessity of creating resilience within the nation's communities.

National Response Framework. The *National Response Framework* provides information about the Emergency Support Functions as well as planning, operational, and intelligence support to the entire homeland security enterprise. The Emergency Support Functions are the coordinating structures at the federal government level for managing response resources. The NRF reminds the all-hazards analysts of their role in providing steady-state and incident-driven intelligence assessments to the whole community-of-populations and practice at all levels of government (National Response Framework, 2016, p. 49). The nesting of operations plans and frameworks, including the *Strategic National Risk Assessment*, emphasizes the importance of an established federal, state, local, tribal, territorial, and regional all-hazards analysis structure with codified common functions and processes.

National Disaster Recovery Framework. The *National Disaster Recovery Framework's* (NDRF) significance to an all-hazards analyst is its focus on post crisis event planning and operations requiring real-time intelligence assessments and information. This is an operational move beyond normal steady-state and incident-driven intelligence because it introduces a third type of intelligence. It requires a return to *normal* steady-state intelligence, yet it also is reactionary by way of anticipating and assessing secondary and tertiary post event hazards during on-going recovery operations. For example, water-borne disease, respiratory ailments, and unsafe infrastructure posing risk to first responders and survivors while they are treating survivors, conducting mortuary affairs tasks, and clearing debris.

DHS Considerations for Fusion Center and Emergency Operations Center Coordination publication. The Comprehensive Preparedness Guide (CPG) 502 is about the internal and external coordination activities of fusion centers and emergency operations centers (EOCs). It provides all-hazards analysts with another insight into their role and responsibilities within the coordinating structures of their centers. Although this publication is intended to establish a coordination and cooperation concept of operations between two types of operations centers, much can be garnered from it from an analytic perspective.

Like the previously reviewed DHS and FEMA publications, CPG 502 emphasizes the all-hazards multiagency environment; intelligence and information organizational and coordination structure; intelligence process; data maturation and actionable intelligence process; the all-hazards operational environment; and the analytic process (Considerations for fusion center and emergency operations center coordination, 2010).

It is within the fusion center that true all-hazards, all-crimes, all-jurisdictions, and all-disciplines unite.

The All-Hazards Homeland Security Operational Environment

The DHS vision and mission statement "is to ensure a homeland that is safe, secure, and resilient against terrorism and other hazards" (Our Mission, 2018). Similarly, the National Preparedness Goal is "a secure and resilient Nation with the capabilities required across the whole community to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose the greatest risk" (National Preparedness Goal, 2015, p. 1). Fusion center mission sets range from a terrorism, all-crimes, or all-hazards approach tailored to their geographic region of responsibility (Considerations for fusion center and emergency operations center coordination, 2010, p. 9). Lastly, the types of hazards and threats are variously explained as adversarial / human-caused, technological / accidental, or natural (National Mitigation Framework, 2016, p. 7) or as natural, intentional, and technological (Considerations for fusion center and emergency operations center coordination, 2010, p. 19).

The following publications, in addition to the above-mentioned materials, either directly contributed to or strongly influenced my preliminary findings and literature review of the all-hazards, threats, events, STE systems, and critical infrastructure topics. Although I did not cite each one in the following sections of my literature review chapter, they should be recognized before proceeding:

- *Hazards Analysis* by John C. Pine (2015).
- *Hazard Analysis Techniques for Systems Safety* by Clifton A. Ericson II (2016).

- *Natural Hazards* by Keller and DeVecchio (2015).
- *Inside Terrorism* by Bruce Hoffman (2006).
- *Weapons of Mass Destruction and Terrorism* by James J. F. Forest and Russell D. Howard (2013).
- *Disasters by Design* by Dennis S. Mileti (1999).
- *Cybersecurity and Cyberwar* by P. W. Singer and Allan Friedman (2014).
- *The Basics of Information Security* by Jason Andress (2014).
- *Critical Infrastructure* by Robert Radvanovsky and Allan McDougal (2013).
- *Critical Infrastructure Protection in Homeland Security* by Ted G. Lewis (2006).
- *All-hazards Risks and Resilience* published by the ASME Innovative Technologies Institute (2009).

Adversarial systems: hazards, threats, and events. Adversarial hazards and threats differ from technological and natural because of their inherent human trait of having intent. Thus, adversarial threats are intentionally carried out against a target or victim to cause harm. This is the crime and criminals' characteristics of the all-crimes approach to crime analysis. It is important to note that humans are typed as purposeful systems meaning their behavior is goal oriented and decision based with a cause and effect relationship (Ackoff & Emery, 2017). And, like other systems, human purposeful systems live and act within the triad of structure, process, and purpose. This means adversarial systems are triadic systems that an analyst can study from a systems perspective.

A cyber-attack, biological attack, school shooting, or an arsonist's wildfire can be classified as adversarial because of the intentional or purposeful action of the perpetrator. Moreover, the decision-making process, a bomb-making process, and physical and virtual structural characteristics of facilities, networks, and resources are considered alongside the human intent—purpose—forming a systems triad. A systems triadic perspective of hazards and threats helps the all-hazards analyst to better understand the sources, characteristics, and effects of threats and crisis events (Osborne, 2006; Vellani & Nahoun, 2001).

Cyber systems: hazards, threats, and events. Cyber threats differ from adversarial threats primarily by the complex cyberspace environment in which they operate. Within cyberspace are purposeful systems—people—acting with the intent to cause harm. Indeed, in cyberspace there are people inside the machines, the problems, and the solutions (Singer & Friedman, 2014, p. 10). This means cyber-hazards and threats are a hybrid of adversarial and complex technological systems. They are cognitive, digital, and physical at the same time (Singer & Friedman, 2014, p. 14).

Within cyberspace, all-hazards analysts will find advanced persistent threats (APT), part-time hackers, and professional nation-state spies conducting a range of crime from terrorism, ransom hijacking, espionage, theft of intellectual property, voyeurism, and even acts of war. Like people in the physical world, they can leave an evidence trail of data and digital fingerprints that reveal their modus operandi and identity. Additionally, like adversarial and other criminal threats, cyber threats also fit into the law enforcement problem triad of offender, victim, and vulnerability (Osborne, 2006, p. 74; Walker & Drawve, 2018, p. 42). Adversarial and cyber threats share similar characteristics, yet cyberspace is a unique and complex realm for security practitioners. Aside from its security concerns, it also is the host for many legitimate and legal activities that are critical to our nation's economy, politics, military, and critical infrastructure sectors.

Technological systems: hazards, threats, and events. Technological threats evolve from human created systems that have inherent hazards due to their complex system characteristics. For example, hardware and software can wear out and fail causing safety hazards or life-threatening incidents. Technological hazards are unintentional thus accidental events or called mishaps. This is not to imply the absence of legal fault or responsibility because people make mistakes. Furthermore, adversaries also can intentionally, and covertly, activate or initiate a cascading sequence of events anywhere in the system leading to a technological crisis event.

Accidental technological hazards and threats are triad-based systems. All three elements of structure, process, and function comprise a technological system too. The term *function* is used in lieu of purpose in technological systems. For example, a nuclear reactor is a physical structure at a specific location, it performs a controlled process of nuclear fission, and its function is to produce energy for cities, industries, homes, and businesses. A nuclear reactor, if it were to leak radiation, would become a hazard source in the triad of hazard source, initiating mechanism, and the target / threat outcome (Ericson, 2016, p. 35).

Natural systems: hazards, threats, and events. Natural hazards, threats, and events cover a wide range of origin sources or spatial zones. These types of hazard zones and sources are, according to FEMA's Multi-Hazard publication, (a) atmospheric, (b) geologic, (c) hydrologic, (d) seismic, (e) volcanic, and (f) wildfire. Another grouping of natural hazard zones and sources are (a) the atmosphere, (b) hydrosphere, (c) biosphere, (d) lithosphere, and (e) seismic zones (Keller & DeVecchio, 2015). A third grouping of natural hazard zones and sources are atmospheric, geologic, hydrologic, and biologic (Pine, 2015, p. 15). The fourth grouping of natural hazards is narrower, and it also includes human-caused sources: (a) climatological, (b) geophysical, and (c) technological (Mileti, 1999). Finally, another source is the anthrosphere zone consisting of humans, their habitats, and their activities (Montello & Sutton, 2013, pp. 77, 87).

Although some natural hazards are human-caused, the term *natural-hazards* typically refers to natural processes and events that potentially threaten environmental resources and populations (Abbott, 2017; Keller & DeVecchio, 2015; Pine, 2015). An eco-centric approach to homeland security considers a natural event's impact on the environment and natural resources (Hough, 2015, pp. 211-224). A human-centric approach considers a natural event's impact on society and human resources (Hampson, 2013, pp. 279-294). Accordingly, a balanced socioecological approach considers how natural events affect the resilience and sustainability of both the natural and human domains because, keeping with a systems-thinking perspective, they are interdependent.

Socio-technological-environmental systems. The whole community approach to all-hazards safety, security, and resilience preparedness involves the entire homeland security enterprise as well as our nation's communities-of-population and practice. The whole community consist of all individuals of diverse demographics, non-profit and non-governmental organizations, religious communities, business communities, law enforcement and military agencies, government, academia, utilities, and even mineral resources and wildlife of the environmental domain. In the combined social and environmental systems context of all-hazards, it not only is the human domain, it also is the natural domain that must be considered.

The human ecology approach to the pairing of human and environmental considerations in crisis management is based on the philosophy that human insecurity is the result of innate hazards in the coexisting human and the natural worlds (Mileti, 1999, p. 18). The STE systems view complements human ecology philosophy as an all-inclusive all-hazards approach to human and environmental security. It considers the full-spectrum of hazards, threats, and events alongside the full-spectrum of societal and environmental system elements. By adding the unique technological characteristic of our world because it stretches from beneath the land well into outer space, the combined STE system view is more accurate.

Critical Infrastructure and Key Resources. All-hazards analysts support critical infrastructure protection (CIP) efforts across the nation as public and private sector security practitioners. The nodes, links, and network of interdependent infrastructure that are critical to the nation's prosperity are at risk of ACTN hazards and threats daily. An all-hazards analyst must understand the threats, the systemic nature of the critical asset, its components, and their relationships with each other as well as with the nation's population, infrastructure, institutions, economy, and the environment.

Critical infrastructure assets range from national monuments of cultural heritage significance to industrial and military defense capacity. Accordingly, all-hazards analysts should have a working knowledge of multiple scientific disciplines and business-related fields. It is not feasible for an all-hazards analyst to earn multiple degrees and to be educated as a civil engineer or as a petroleum engineer as well as extensive experience in legislative and cultural history or natural resources. For this reason, the DHS training guidelines emphasize the importance of an all-hazards analyst to become a subject matter expert on one or a few hazards areas that are relevant to their critical infrastructure sector or geographic region (Global Justice Information Sharing Initiative, 2007, 2010). The range of Fusion Center missions, Information and Analysis Center (ISAC) focus areas, and critical infrastructure protection requirements highlight the risk of setting expectations too high for an all-hazards analyst to be an expert in all career fields and disciplines related to STE assets and all-hazards. It is more practical for HSIE all-hazards analysts to be familiar with the transdisciplinary nature of their analytical and collaborative work which is a goal of the AH-ISM.

The Intelligence Domain

Intelligence experts and academic researchers' resident in the DHS, the IC, university centers of excellence, and other research and development think tanks, frequently publish books and articles. Their topics cover hazards analysis, threat analysis, the intelligence cycle, national intelligence collection assets, research methodologies, law enforcement crime analysis techniques, cognitive and critical-thinking methods, business intelligence analysis, and commonly used structured analytic techniques. In some form, these publications contribute to the body of knowledge that is required within the intelligence domain of security institutions, information sharing infrastructure, and intelligence analysis capacity. These references are easily obtained on internet sites, public bookstores, and university bookstores as open-source publications.

The following publications, in addition to the above-mentioned materials, either directly contributed to or strongly influenced my literature review and research of the intelligence domain. Although I did not cite each one in this section of my literature review chapter, they should be recognized before proceeding:

- *Data Fusion Support to Activity-Based Intelligence* by Richard T. Antony (2016).
- *Activity-Based Intelligence Principles and Applications* by Patrick Biltegen and Stephen Ryan (2016).
- *Analyzing Intelligence* by Roger Z. George and James B. Bruce (2014).
- *Intelligence Analysis: A Target-Centric Approach* by Robert M. Clark (2017).
- *The 5 Disciplines of Intelligence Collection* by Mark M. Lowenthal and Robert M. Clark (2011).
- *The Thinker's Guide to Analytic Thinking* by Linda Elder and Richard Paul (2012).
- *Psychology of Intelligence Analysis* by Richards Heuer (2017).
- *Analytic Culture in the U.S. Intelligence Community* by Rob Johnston (2005).
- *Summary: Thinking Fast and Slow* by Daniel Kahneman (2018).
- *Intelligence: From Secrets to Policy* by Mark M. Lowenthal (2015).
- *Structured Analytic Techniques for Intelligence Analysis* by Richards J. Heuer and Randolph H. Pherson (2011).

- *Critical-thinking for Strategic Intelligence* by Katherine Hibbs Pherson and Randolph H. Pherson (2017).
- *Analyst's Guide to Indicators* by Randolph H. Pherson and John Pyrik (2018).
- *The Back of the Napkin* by Dan Roam (2009).
- *Intelligence for an Age of Terror* by Gregory F. Treverton (2009).
- *Critical-thinking and Communication* by Edward S. Inch and Barbara Warnick (2010).
- *Be-Know-Do Leadership the Army Way* extracted from the Army's leadership manual (2003).
- *Minimum Intelligence Training Standards for Law Enforcement and Other Criminal Justice Agencies in the United States* by the Global Justice Information Sharing Initiative (2007).
- *Analyst Toolbox: A Toolbox for Intelligence Analyst* by the Global Justice Information Sharing Initiative (2006).
- *Law Enforcement Analytic Standards* by the Global Justice Information Sharing Initiative (2012).
- *Analyst Professional Development Road Map* by the DOJ (2015).
- *The National Criminal Intelligence Sharing Plan* by the Global Justice Information Sharing Initiative (2003).
- *JCAT Intelligence Guide for First Responders* by the Joint Counterterrorism Assessment Team (2014).
- *Department of Homeland Security Target Capabilities Lists* by the DHS.

- *Common Competencies for State, Local, and Tribal Intelligence Analysts* by the Global Justice Information Sharing Initiative (2010).
- *Reviewing the Department of Homeland Security's Intelligence Enterprise* published by the Homeland Security Committee (2016).
- *Homeland Security Intelligence* by James E. Steiner (2015).

The intelligence cycle. The intelligence process is how an analyst accesses single-source and all-source datum that was previously collected and then analyze it to produce meaningful information. Analyst further evaluates the data and information to produce actionable intelligence assessments that meets the needs of a decision-maker or policy maker often referred to as either a client, customer, or consumer of the intelligence products. Once the intelligence product is decided to be actionable, it is integrated into the planning documents, policies, or the practitioner's operations. The intelligence process follows the applied intelligence path of meaning-making to decision-making to problem-solving.

The intelligence process is not linear because many actions are taken simultaneously to process information. A talented analyst can simultaneously evaluate data and information for its meaning and usefulness while analyzing its entity components and drafting a structured argument for the final assessment. Likewise, a team of analysts can delegate the intelligence process tasks and cross-talk as one group researches historical and contextual information while another group coordinates with the customer on the integration process. Whether it's an individual or group effort, time is a factor to be considered in the daily steady-state and the moment-by-moment incident-driven state when minutes matter for first responders and survivors.

The intelligence process is multilayered and is glued together by feedback loops that ensure smooth transitions or even simultaneous execution of each phase of the process. Collectors, analysts, producers, clients, customers, and consumers are all stakeholders of varying degrees in the intelligence domain and they must continuously communicate, coordinate, and cooperate throughout the system's life-cycle. Each actor in the system must tend to their own collection, analysis, processing, and dissemination subsystem to ensure the whole system's structure, process, and function are balanced and productive. Whether it is a private-sector corporation managing critical infrastructure assets or a public-sector homeland security agency studying climate change, the intelligence synthesis system for each is essentially a system-of-systems consisting of interconnected people, technology, organizations, networks, and goals.

All-source national and domestic intelligence. All-source intelligence is used by national and domestic intelligence analysts in the intelligence synthesis system. This type of intelligence is derived from multiple sources of collection such as images taken by satellites, confessions, intercepted conversations, news articles on the internet, annotated maps, and scientific measurements. Each collection source is the origin of the five disciplines of intelligence known as the 5-INTs: (a) open source (OSINT), (b) human (HUMINT), (c) signals (SIGINT), (d) geospatial (GEOINT), and (e) measurement and signature (MASINT) [Lowenthal & Clark, 2016]. Each one can be processed as single-source of data, information, and intelligence. However, as single-sources their products may be narrowly focused, limited in scope and contain unverifiable data points. All-source intelligence, which combines as many INTs as possible, maximizes the benefits of each INT and provides better context and clarity to the finished intelligence product.

Within intelligence collection are sources of depth and breadth (Lowenthal, 2015, p. 91) allowing all-hazards analysts access to diverse categories of data. Both national defense and domestic homeland security departments and agencies, public and private, benefit from 5-INTs “all-source” fused (i.e. integrated) intelligence.

All-hazards homeland security intelligence. All-hazards intelligence synthesis draws from all-source, all-crimes, and all-disciplines intelligence sources**.** All-discipline sources of intelligence are derived from the engineering and science disciplines of chemical, civil, electrical, mechanical, biomedical, software, aerospace, agriculture, environmental engineering as well as mathematics, physics, architecture, psychology, criminology, sociology, and organizational management. This is considered pluralistic intelligence—the nexus of multiple disciplines, jurisdictions, and sources to create meaning for decisions to solve problems (McEntire, 2006).

All-hazards intelligence synthesis is an all-inclusive process that spans the hierarchical and horizontal planes of public and private institutions, government, organizations, academic, and scientific fields of study. At any given time, an all-hazards analyst may be called upon to analyze an individual person’s motive for committing an act of terror or the safety and security issues surrounding a national movement arising from a mass-shooting. In the context of homeland security, *all* really means all-dimensions, all-disciplines, all-sources, all-crimes, and all-hazards. Again, the homeland security’s all-hazards intelligence domain is pluralistic.

Privacy, Civil Rights, and Civil Liberties in the Intelligence and Security Domains

“DHS is required by law to execute its mission in a manner that protects civil rights and civil liberties” (Civil Rights / Civil Liberties Impact Assessment: DHS Support to the National Network of Fusion Centers, 2013, p. ii). Furthermore, DHS is required to ensure its departmental activities, programs, and efforts do not diminish the civil rights and civil liberties, as well as lawful privacy, of persons. The department has, therefore, adopted the stance of safeguarding and providing enhanced compliance with privacy, civil rights, and civil liberties (PCRCL) guaranteed by the constitution, statutory laws, other regulations, and policies rather than mere minimal legal compliance (Civil Rights / Civil Liberties Impact Assessment: DHS Support to the National Network of Fusion Centers, 2013, p. 28).

The specific PCRCL's addressed by the DHS are the "First, Fourth, Fifth, and Fourteenth Amendments to the Constitution; the Privacy Act of 1974; 28 C.F.R. Part 23; Executive Order (EO) 12333; and the Department's *Guidance on the Use of Race in Law Enforcement Activities*" (Civil Rights / Civil Liberties Impact Assessment: DHS Support to the National Network of Fusion Centers, 2013, p. 2). These are the foundational PCRCL constraints set upon the intelligence and law enforcement activities of the HSIE for the rightful purpose of guaranteeing governmental respect and assurance of the population's privacy and rights. Compliance of PCRCL is always required during the conduct of collection, analysis, synthesis, and application of intelligence within the homeland security and intelligence domains and their associated disciplines and programs.

The following publications, in addition to the above-mentioned materials, either directly contributed to or strongly influenced my literature review and research of the PCRCL requirements in the homeland security and intelligence domains. Although I did not cite each one in this section of my literature review chapter, they should be recognized:

- *DHS Civil Rights / Civil Liberties Impact Assessment: DHS Support to the National Network of Fusion Centers (2013.*
- *National Security and Civil Liberty* by Michael Geary (2014).
- *Recommendations for First Amendment Protected Events for State and Local Law Enforcement Agencies* published by The Global Justice Information Sharing Initiative (2011).
- *The Constitution: An Introduction* by Michael Stokes Paulsen and Luke Paulsen (2015).

Knowledge, Information, and Professional Management Programs

The management of data, information, and knowledge is the purpose of institutional knowledge management (KM) programs. It includes the people, processes, tools, systems, and supporting technologies to discover, capture, share, and apply knowledge at the individual and institutional levels as well as ensuring longevity and continuity of knowledge for future use (Becerra-Fernandez & Sabherwal, 2015, pp. xi-xiii). Closely related to KM is information management (IM). IM is primarily focused on the technology, system processes, and technicians who support KM by way of collecting, processing, storing, displaying, disseminating, and protection of data, information, and knowledge products (Department of the Army, 2014, pp. 3-6). Together, KM and IM underlie the knowledge generation and intelligence production cycle of intelligence analysts regardless of their employing organization. Each subfield of KM and IM are distinct domains requiring skilled technicians, practitioners, system applications of software and hardware, and methodologies to accomplish. For example, collectors of data require unique knowledge, skills, and abilities to conduct the collection activity “that synchronizes and integrates the planning and employment of sensors and assets as well as the processing, exploitation and dissemination of systems in direct support of current and future operations.” (Department of the Army, 2012, pp. 1-1)

The following publications either directly contributed to or influenced my literature review and research of the KM and IM programs in the homeland security and intelligence domains. Although I did not cite each one in the literature review chapter they should be recognized:

- *Knowledge Management: systems and processes by Irma Becerra-Fernandez and Rajiv Sabherwal (2015).*
- *Commander and Staff Organizations and Operations* published by the Department of the Army (2014).
- *Information Collection* published by the Department of the Army (2012).
- *Training Units and Developing Leaders* published by the Department of the Army (2012).
- *World Class: How to Build a 21st-Century School System* by Andreas Schleicher (2018).
- *Neuro Teach: Brain Science and the Future of Education* by Glenn Whitman and Ian Kelleher (2016)

The data, information, knowledge, intelligence continuum. Knowledge management offers a conceptual framework in the form of a continuum about the maturation process of data to information to knowledge to intelligence. This knowledge generation conceptual model of intelligence production and is one of four primary KM tasks conducted by intelligence analysts. The other three are organizing, applying, and transferring knowledge (Department of the Army, 2014, pp. 3-6). This knowledge generation process, based on critical reasoning, is a foundational concept in my thesis research and it will be discussed and referenced throughout chapters IV and V because of its interdisciplinary applicability within the HSIE.

Information and evidence are useful in the structuring or formatting of effective communication products when it is processed through pattern, theme, contextual, or statistical analysis methodologies. Once again, this is the continuum of gaining knowledge referred to as the data, information, knowledge, and intelligence (DIKI) continuum (Ratcliffe, 2016, p. 71). The terms *data fusion*, *analysis* and *synthesis* have somewhat different meanings and will be explained later in this section. To be sure, all are integral in the management of knowledge in the intelligence synthesis process.

A similar continuum of gaining knowledge is found in the research and communication fields. Using the Toulmin model (Inch & Warnick, 2010, p. 42), a claim is derived from data that is grounded in supporting evidence in the forms of warrant and backing. This is both a structure and a process flow of knowledge. The data, warrant, backing, and claim sequence provides both a knowledge continuum model and a structured form for a written product—structured communication. Similarly, evidence follows the same path as data for it to become a factual claim. To summarize, regardless of the all-source, all-crimes, or all-hazards analysis environment, analyst use the DIKI knowledge generation continuum as both a functional process and as a communication structure to achieve an applied intelligence purpose.

Critical-thinking and synthesis. Generating content knowledge about a subject requires the organized synthesis of multiple information sources and then sharing that synthesized intelligence with others for application. These tasks are the products of knowledge management and information management convergence. In other words, one program manages the creation and retention of individual and institutional knowledge while the other manages the technological enablers and sharing systems needed for its use by individuals and institutions. Both KM and IM disciplines are linked together by the critical reasoning process of analysis, fusion, and synthesis (i.e., intelligence analysis).

These following common knowledge management and information management terms and their definitions help with the understanding of these two disciplines and their contribution to pluralistic intelligence. Synthesis is the process of "putting together parts or elements to form a whole" (Clark, 2017, p. 80). Fusion "results in meaningful and actionable intelligence and information" when combined with analysis (Considerations for fusion center and emergency operations center coordination, 2010, p. 10). Fusion also includes data from all-sources of intelligence collection platforms as well as their single-intelligence analytic products (Lowenthal, 2015, p. 91). Analysis is "breaking an entity into its component parts" (Pherson & Pherson, 2017, p. 24). And, critical-thinking is structured systematic thinking used to "answer questions, solve problems, and resolve issues" (Elder & Paul, 2012, p. 5). These four forms of intelligence production—critical-thinking, analysis, fusion, and synthesis—are closely related and "complementary and necessary for successful outcome" (Pherson & Pherson, 2017, p. 24).

Risk Management in the Homeland Security Domain

Authors of risk management text books and governmental risk guidelines offer an integrated all-discipline and all-hazards approach to risk, vulnerability, and consequence analysis. It is the risk manager's responsibility to integrate all-hazards intelligence synthesis products into the risk management process to reduce adverse risk, increase resilience, and, for entrepreneurs, to increase opportunities. The risk management process includes vulnerability analysis, consequence analysis, and risk analysis supported by comprehensive all-hazards analysis. In the context of homeland security this process is designed to provide risk-informed applied intelligence to decision-makers.

The following publications either directly contributed to or strongly influenced my literature review and research of the risk management process. Although I did not cite each one in the literature review chapter they should be recognized before proceeding:

- *A Practical Introduction to Security and Risk Management* by Bruce Newsome (2014).
- *Risk Management* by Carl L. Pritchard (2015).
- *A Guide to the Project Management Body of Knowledge—PMBOK Guide* published by the Project Management Institute (2017).
- *Project Management for Dummies* by Stanley E. Portny (2017).
- DHS publications incorporating intelligence into the risk assessment and management process.

Intelligence and the risk assessment process. Risk management is a process that closely follows the intelligence process to identify hazards, threats, and the risks that may be associated with an asset or an activity (Department of Homeland Security, 2011; Department of the Army, 2014; Pritchard, 2015). Businesses assess the risk of investment and expanding their product line, corporations assess the risk of operating facilities near the coastal ports or away from established transportation routes, whereas government agencies assess the risk of immigration policy, climate change, and the opioid epidemic. Many assess the risk of operating in cyberspace, social media, the global economy, and a polluted environment. Certainly, all sectors assess the risk of the all-hazards HSOE on their operations and assets.

Approaching risk from the perspective of an all-hazards analyst in either the public or private sectors, the purpose of their efforts is to produced risk-informed intelligence analysis assessments. Risk analysis may not be the client's priority in target-centric (Clark, 2017) or activity-based (Antony, 2016; Biltgen & Ryan, 2016) analysis that is intended to assess capabilities, capacity, and intent of a terror cell or crime organization. Risk, however, is a client's priority in analysis that is intended to assess a valued resource, asset, technology, or even intellectual property's vulnerability to a threat and the consequences of an attack or interaction. Risk-based intelligence places the valued STE resource or entity at the center of the problem and then assesses its vulnerability and likelihood of it becoming the target of a threat.

DHS all-hazards risk management. The DHS risk management process is 6 steps evenly divided between meaning-making and decision-making phases. The all-hazards analyst is the lead actor in defining context, identifying potential risk, and assessing and analyzing risk in the first three steps. The next three steps are primarily the responsibilities of the risk manager and decision-makers. The DHS risk management process places the mission sets of safety, security, and resilience alongside the homeland security asset (e.g., critical infrastructure and key resource, or community) to be assessed. However, like all other intelligence and risk processes, it is not a purely linear method and is better done with feedback loops and threat reassessments to ensure quality risk assessment products are provided (Risk Management Fundamentals, 2011).

U.S. Army all-hazards risk management. The U.S. Army's risk management process similarly allows for all-hazards analyst to begin the process with identifying and assessing hazards while risk managers and military leaders develop control measures, make decisions, and implement controls. These are the first four steps of the process with the final step emphasizing the need for feedback loops in the form of supervision and evaluation (Department of the Army, 2014). The U.S. Army's risk management process is implemented to protect the combat force, its military communities of family members and institutions, and all other assets of significant operational value. Also, these risk-informed assessments are routinely integrated into the intelligence cycle and the commander's decision-making process.

Business community risk management. In the business community, project management's risk management input is a 7-step process (e.g., plan, identify, qualitative analysis, quantitative analysis, response, implement, and monitor) that also includes identification and assessment of hazards as critical initial steps. However, a difference between it and the DHS risk management process is that the assessment step is split into two separate steps of qualitative and quantitative assessments. These two steps are all-hazards focused and include technical, managerial, commercial, and external risks. Like the U.S. Army, the PMBOK Guide's risk management process includes specific steps that are focused on feedback loops and monitoring the risk to ensure the process is continuous and not linearly limited (Project Management Institute, 2017).

Law Enforcement in the Homeland Security Domain

All-crimes intelligence analysis is law enforcement’s process and product of analyzed crimes and criminals based on data and information that has been collected and compiled to prevent and monitor criminal activity (Ratcliffe, 2016, p. 69). It includes crime pattern, association, network, demographic, financial, and many other crime and criminals related analysis methods. The relevance of this all-crimes analysis focus to an all-hazards operating environment is that the DHS all-hazards analyst training program is law-enforcement centric with a crime-fighting approach. It is based on the International Association of Law Enforcement Intelligence Analysts (IALEIA) and DOJ standards outlined in the Law Enforcement Analytic Standards, and Global Justice Information Sharing Initiative’s Analyst Toolbox, and Target Capabilities List (TCL) published by DHS. This law enforcement focus of crime and terrorism may diminish the importance of and the opportunities for common core all-hazards training that includes emphasis on technological and natural threats.

The following publications either directly contributed to or strongly influenced my literature review and research of law enforcement crime analysis. Although I did not cite each one in the literature review chapter they should be recognized:

- *Law Enforcement Intelligence* by David L. Carter (2009).
- *Intelligence Analysis for Problem Solvers* by John E. Eck, Ronald V. Clarke, and Gohar Petrossian (2018).
- *Applied Crime Analysis* by Karim H. Vellanni and Joel D. Nahoun (2001).

- *Fundamentals of Crime Analysis* by Jeffery T. Walker and Grant R. Drawve (2018).
- *Intelligence-Led Policing* by Jerry H. Ratcliffe (2016).
- *Out of Bounds* by Deborah Osborne (2006).

Emergency Management and Critical Infrastructure Protection in the Homeland Security Domain

Emergency management, or crisis management, of crisis events that originate from hazard sources and threats interacting with society requires a comprehensive approach to all-hazards risk assessments. Regardless of "public, policy, and media agendas, emergency management must be guided by scientific and statistical risk analysis" (Bullock et al., 2014, p. xvii). Scientific and statistical risk analysis, as this statement implies, must derived from the systematic critical-thinking methodologies that produce risk-based data, statistics, and ultimately intelligence products for emergency managers who prepare emergency plans, FSLTT policies that are in support of the National Preparedness Goal, and implement these plans and policies in their field practice.

Emergency management is grounded in the safety and security goals to protect property, environmental resources, and save lives. This is the foundation of the DHS NIMS publication and system as well as the Incident Command System (ICS) (Department of Homeland Security, 2013; FEMA, 2008; Ferlemann, 2015). Emergency management practitioners include public services ranging from police, ambulance service providers, health care providers, fire departments, voluntary organizations active in disaster (VOAD), and any other public and private first responder to an incident, disaster, or catastrophe (Bullock et al., 2014, pp. 181 - 187). Emergency management practitioners and academics contributes to the all-hazards intelligence through applied research and practical application through their focus on understanding the discipline's dangerous operational environment and missions.

Critical infrastructure protection (CIP) is focused on supporting the *protect* preparedness mission and emergency management is primarily focused on supporting the *response* and *recovery* missions. Like emergency management, CIP is a risk-based endeavor to ensure national social, technological, or natural infrastructure resources (e.g., transportation, energy production, or health services) are not disrupted, dismantled, or destroyed by a threat. Indeed, critical infrastructures are both physical and logical systems and functions that are derived from people, physical assets, and cyber systems (Radvanovsky & McDougall, 2013, p. 4). Similar to CIP is critical infrastructure assurance (CIA) that is focused on assuring critical infrastructure resilience and capacity to function during a crisis (Radvanovsky & McDougall, 2013, p. 6). Homeland security's emergency management, CIP, and CIA are both concerned with applying risk-informed intelligence to protect, respond, and recover from hazards, threats, and crisis events.

The following publications either directly contributed to or strongly influenced my literature review and research of emergency management's contribution to all-hazards intelligence synthesis. Although I did not cite each one in the literature review chapter they should be recognized:

- *An Introduction to Emergency Management* by George D. Haddow, Jane A. Bullock, and Damon P. Coppola (2014).

- *Technology and Emergency Management* by John C. Pine (2018).
- *A Practical Introduction to Homeland Security and Emergency Management From Home to Abroad* by Bruce O. Newsome and Jack A. Jarmon (2016).
- *Emergency Management and Social Intelligence: A Comprehensive All-Hazards Approach* by Charna R. Epstein, Ameya Pawar, and Scott C. Simon (2015).
- *Incident Command System (ICS)* by Kyle Ferlemann (2015).
- *Incident Command System Training* published by FEMA (2008).
- *Critical Infrastructure: Homeland Security and Emergency Preparedness* by Robert Radvanovsky and Allan McDougall (2013).
- *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation* by Ted G. Lewis (2006).
- *All-Hazards Risk and Resilience: Prioritizing Critical Infrastructure Using the RAMCAP Plus^{SM}Approach* published by ASME Innovative Technologies Institute, LLC (2009).

Ten safety and security domains where covered in my literature review: homeland security; its all-hazards operational environment; intelligence; the domain of privacy, civil rights, and civil liberties; knowledge management; information management; risk management; law enforcement's crime analysis; emergency management; and critical infrastructure protection. The literature review answered five of the six research questions (research questions 1-5) that I posed because my research was conducted almost solely from the exploratory review of government publications and academic textbooks. The central research question and research question six are synthesis-centric thus they are answered in the analysis and discussion chapter's IV and V respectively. And, research questions one through five are answered in chapter V's CORE Reflexivity Discussion section where I address each research question in my evaluation of the research process and its products.

My literature review relied upon media sources like websites, my personal observation from my experiences, and, most significantly, documents and publications by the U.S. government and non-governmental education and academic publishers. Fifty percent of my literature review came from non-governmental publications, textbooks, and other academic articles. Forty-five percent came from governmental publications, documents, doctrine, and websites. And, five percent came from non-governmental websites.

CHAPTER III

Methodology

The literature review discovered, or more accurately *revealed*, how the homeland security and intelligence domains historically viewed and currently approach the all-hazards operational environment and its analytical challenges. The range of hazards, threats, crises, and their social, technological, and environmental impacts are well documented in governmental and academic publications. However, my preliminary findings discovered the need for and the structure of two conceptual models for an all-purpose and all-hazards intelligence synthesis focus. Also, throughout the literature review process, institutional and individual analysts core competency traits became apparent. I further researched the commonality of these competency traits and their relationships to the two preliminary intelligence synthesis models during my subsequent research. The results of my research into institutional and professional analytical core competencies and intelligence synthesis models will be presented in chapters IV and V. At this time, I would like to note that my qualitative research methodology was derived from five research and analysis methods sources:

- *Research design* by John W. Creswell for his qualitative methods outlined in chapter nine of his book (2014, pp. 183-213).
- *7 Steps to a comprehensive literature review* by Anthony J. Onwuegbuzie and Rebecca Frels for their step-by-step methodology on conducting a literature review as a research method (2016, pp. 62-63). The comprehensive literature review methodology is central to my research as a process and product. It will inform my research during each phase by

relying on “multimodal texts and settings in a systematic, holistic, synergistic, and cyclical process of exploring interpreting, synthesizing and communicating published and/or unpublished information” (Onwuegbuzie & Frels, 2016, p. 4).

- *An introduction to research, analysis, and writing* by Bruce Oliver Newsome for his explanations on how to analyze evidence and data (2016, pp. 259-282).
- *Qualitative data analysis* by Matthew B. Miles, A. Michael Huberman, and Johnny Saldaña for their focused, sequential, and visualized data analysis methods (2014).

The Researchers Role

I was the only researcher throughout my research process. As I stated in my research design and approach sections, I took a qualitative pragmatic realist approach in my research. My methodology was bricoleur in its style, but I also was rigorous in my efforts. I conducted it almost exclusively from my home because nearly all my literature sources and materials are publicly available online or located at my home in print version. As the sole researcher, I collected, analyzed, synthesized, and am now reporting on my findings without the help of research assistants or other secondary research or review sources. My personal, academic, and professional experience guided my selection of topics and reference materials. Any personal biases I may have are grounded in my experiences of personal loss, which is expressed as an empathy for others during times of crisis, and a first-hand understanding of post-flooding recovery challenges after my parents’ home was flooded during Hurricane Harvey. My professional biases are rooted in my military career of ensuring national security and, more specifically, our nations constitutionally protected privacy, civil rights, and civil liberties. My security studies academic bias is based on balancing these human rights with scientifically informed environmental security policy and practice.

Bounding the Research

Setting, audience, process, and ethical considerations. I conducted my research primarily from my home in Houston, Texas, and I accessed publicly available literature and media sources through my home internet provider on my personal laptop, iPad Pro, iPhone, and television cable provider. My audience is the homeland security and intelligence domain practitioner, specifically, those in employed within the HSIE, and academic researchers and students of security studies and all-hazards crises. My research only used publicly available unclassified resources.

My research process integrated the collect, analyze, synthesize, and apply (i.e., evaluate and report) process, referred as CASA, that is based on my preliminary findings. The CASA process is a synthesis of commonly used intelligence and research methods derived from government and academic intelligence analysis publications. I collected data and information primarily from public and academic sources, analyzed it following the RREI steps (e.g., reduce, relate, evaluate, integrate), synthesized my findings into this text report with illustrative figures, evaluated my findings for any discrepancies, and provided my research findings to my thesis committee. The structure of my research findings will follow the Toulmin structured argumentation format (Inch & Warnick, 2010, pp. 22, 42; Onwuegbuzie & Frels, 2016, pp. 162-164) and it is compliant with the *Publication Manual of the American Psychological Association* (2010). Moreover, there are no other participants so my main ethical considerations during my research are avoiding unintentional plagiarism or misrepresentation, and ensuring I only use open-source unclassified material.

Data Collection Procedures

Types of data sources. The homeland security all-hazards operational environment is a multidisciplinary, multiagency, and multijurisdictional domain. Therefore, access to open-source literature databases that represent multiple career fields and scientific disciplines was required (Onwuegbuzie & Frels, 2016, p. 88). The types of data sources that I used consisted of audio and visual media; my personal experiences and observations an intelligence officer; publicly accessible documents; the expertise of other authors and researchers derived from media and documents; and publicly available secondary data collected by other researchers in the form of textbooks and research publications. This is the MODES method of collecting multidisciplinary, interdisciplinary, and transdisciplinary literature sources (Onwuegbuzie & Frels, 2016). All literature sources provide authoritative data or an alternative interpretation of the topic. This separation is aligned with my critical realist world view.

Media. I viewed and recorded pertinent information from documentaries and interviews (e.g., Public Broadcasting Station, Home Box Office) about homeland security, national and domestic intelligence processes, ACTN disasters, and risk management to better understand them from a systems, participants, and documentary contextual perspective. For example, journalistic interviews with current and former homeland security officials, first responders, and other practitioners as well as documentaries of past disasters. I understand that the selection of visual and audio media that I considered to be valid was subjective and required my utmost scrutiny to ensure its veracity.

Observations. Direct observations incorporated into my research were my own and based on either my professional expertise as an intelligence officer in support of military intelligence and operational missions across the world, or my personal experiences during Hurricane Harvey's flooding in the Houston metropolitan area. I relied upon my experience with planning and conducting all-source and counterintelligence support to the United States Eighth Army and Republic of Korea forces opposed to North Korea and other Foreign Intelligence Services operating in South Korea; Turkey during Operation Desert Storm as a PATRIOT Air Defense Officer and briefly supported Operation Provide Comfort humanitarian mission to the Kurdish population; and also my command experience of an imagery intelligence unit in support of U.S. Central Command. My observations, and potential biases, about intelligence synthesis and crisis management are grounded in these national security experiences.

Documents. Publicly accessible U.S. Government and United Nations publications, non-governmental organization references, academic textbooks, peer-reviewed journals, and investigative reports were my primary literature sources. These sources were selected for their relevance to the topics of domestic safety, security, resilience, intelligence analysis, risk, and crisis management in the all-hazards HSIE. Mapping services (e.g., Google Earth or Google Maps) and their products were utilized as references in support of my understanding of document and media sources content. My interpretation of these mapping products should be considered my own observations. I did not request any legal or public records for my research.

Experts. Expert opinions of authors and other researches came from my selected literature sources and they are cited appropriately. There are no other participants in my research.

Secondary data. Additional research data collected by others was derived from my literature sources. I did not request or access secondary quantitative data from any other sources because my research was primarily qualitative.

Data collection sensors and instruments. I used the public internet (e.g., Safari, Google, and Google Scholar) as my primary research instrument to obtain publicly available literature materials from government, academic, and private websites. I accessed the Homeland Security Digital Library, the FEMA Emergency Management Institute (EMI) Academic Emergency Management and Related Courses (AEMRC) online resource library, the Center for Homeland Defense and Security's (CHDS) University and Agency Partnership Initiative's (UAPI) online educational resources, and the Sam Houston State University Newton Gresham Library (e.g., EBSCOhost access to 386 databases) through their websites using my own student subscription accounts. I used key term, keyword, and Boolean search strategies on the internet and library sites. The key references I have listed in my research methods introduction paragraph offer numerous tables and lists of open-source websites I used when choosing literature sources.

Data Recording and Storage Procedures

I used the Microsoft Office 365 suite of word processing, data organization, and presentation software to record and display my research. MS Word, Excel, and PowerPoint were my primary electronic data recording tools; however, I took written notes and sketches on loose-leaf paper, white-board, and in a note taking application on my personal iPad during my research. I stored my research files and documents on my personal laptop computer (e.g., my documents folder), iPad, and they were backed-up in my Drop Box and OneDrive cloud folders. I have sole access to these storage devices and files using a personal login and password.

Data Validation, Analysis, Synthesis, and Interpretation of Collected Information

Collected data validation. I used multiple literature sources (i.e., MODES) to validate the accuracy of the research data and information. I do not use quantitative data to triangulate my collected data and my findings because I used the qualitative literature review as my research method. Therefore, I relied upon the different modes of data sources for validation. For example, I compared documentary evidence, government publications, and independent reports to verify the accuracy and acceptability of data, claims, and findings.

Analysis of data and information. I separated analysis from synthesis in accordance with my preliminary findings about intelligence synthesis methods. Analysis is the systematic breaking down of information into its constituent parts and synthesis involves making connections among the parts (Onwuegbuzie & Frels, 2016, p. 224). Moreover, research is acquiring knowledge (Newsome, 2016, p. 129). Therefore, I simultaneously conducted research, analysis, and synthesis using the four analysis phases of reduce, relate, evaluate, and integrate (RREI). I also drew from the data analysis display and application methods of *Qualitative Data Analysis* as a primary source.

As I read and collect data and information, I recorded the results of the RREI phases and applied appropriate analytic techniques of reductional and relational analysis.

My general analytic approach was intended to be descriptive, analytical, and evaluative (Newsome, 2016, p. 124) to accomplish two objectives: apply the RREI analysis phases as a method of research and continue to refine it as a proven product of my research. This method helped me classify and group qualitative data and determine its level of analysis (e.g., hierarchy) [Newsome B. O., 2016, pp. 266-270]. In my research I drew upon qualitative data analysis and coding techniques to add rigor to my analysis and synthesis efforts.

Reductional analysis. By conducting reductional analysis, I reduced the studied source or entity into keywords, topics, concepts, subentities, subsystems, and system elements of structure, process, and function or purpose. This task categorized and recorded basic attributes, variables, and identifying characteristics. I focused on ACTN hazard sources and STE entities. Throughout my research I collected data that related to my central research question and created acronym codes to categorize, label, and summarize the data as general method of reductional analysis (Miles et al., 2014, pp. 73-75).

Relational analysis. By conducting relational analysis, I related the basic components of my data to discover sequences, patterns, themes, links, associations, relationships, and likely meanings between STE entities and ACTN hazard sources. This task connected and combined entities, concepts, interdependence, anomalies, and context. This was the production phase of organized research information. Throughout my research I identified relationship types and characteristics such as values, attitudes, beliefs, conflicts, emotions (Miles et al., 2014, p. 75), transactions, activities, and networks as a general method of relational analysis.

Evaluative analysis. I conducted evaluative analysis to continue the refinement, understanding, relevance, and the impact of systemic elements, entities, themes, concepts, context, and their relationships to my central research question. This was the final phase of meaning-making regarding my research findings. Evaluative analysis is the collation and comprehension of researcher-accepted organized information into actionable intelligence or applied knowledge. It is important to note that the evaluation phase serves as a reminder to the researcher to pause and reflect on the findings and determine its usefulness, replicability, and potential application. In other words, this is when I asked *so what?* about my findings to test its usefulness for my intended audience. Throughout my research, I assigned "judgements about the merit, worth, or significance" (Miles et al., 2014, p. 76) of my organized information, conclusions, and findings as a general method of evaluative analysis.

Integration and synthesis. Integration and synthesis of my research findings into policy formulation, legislation, operational planning, decision-making, and problem-solving practice is the final phase of my analysis. This task of advising, informing, and acting on the "assertions and propositions, or connected sets of explanations, reflecting the findings and conclusions of the study" (Miles et al., 2014, p. 99) were done by creating five complete interdisciplinary all-hazards intelligence synthesis models. I will display my data, information, conclusions, and findings in this written report that includes illustrative figures. As stated previously, the practical application of these models within the HSIE are recommended for future research. My analysis and discussion in chapters IV and V build the intelligence synthesis models and integrate them in an interdisciplinary way, but it does not apply them in practice for validation.

The CORE Method for Validity and Reliability of the Findings

I used the comprehensive literature review methodology in my research because it helped me accomplish five purposes during my research. These reasons are topic-driven, method-driven, and connection-driven (Onwuegbuzie & Frels, 2016, p. 15):

1. To inform me and contribute to the body-of-knowledge on all-hazards analysis.
2. To narrow my topic to ensure its relevance to the all-hazards community-of-practice.
3. To discover new multidisciplinary perspectives on my topic.
4. To explore new methods of all-hazards analysis.
5. To understand the interdisciplinary relationships on my topic.

As my own research instrument, I worked towards my objectives with these reasons in mind. Accordingly, I was in a more advantageous position to validate my findings, determine their reliability, and their potential application within the HSIE. An explanation of the CORE reflexivity method, which I used, is in the next section.

CORE reflexivity method. I applied the CORE reflexivity method during each phase of my research process (e.g., collect, analyze, synthesize, and report). The CORE process helped me recognize potential biases and reflection opportunities, and to critically examine both the process and the product of my research (Onwuegbuzie & Frels, 2016, pp. 20-21). In a multimodal context, the CORE process helped with the triangulation of data, information, and analytic findings by cross-examination of my MODES literature sources. It also will help me flush out any biases and discrepant information. The CORE process of critical examination is:

- Critical examination: What did I learn and why?
- Organization: How can I organize and display the content of what I learned?
- Reflection: What was the research process or analysis method like (i.e., did it work?) and how does it relate to the central research questions? Where there any biases or discrepancies?
- Evaluation: What is my conclusion and how can it be integrated into my overall research?

CHAPTER IV

Analysis

My literature review drew from all-hazards, all-crimes, all-sources, and all-disciplines resources related to homeland security, risk management, academic research, and intelligence. This multidisciplinary resource collection of scientific disciplines, academic perspectives, institutional knowledge, and experienced practitioners in the homeland security domain are the data and information sources of the pluralistic HSIE. Accordingly, my analytic approach and conceptual framework about homeland security intelligence synthesis is influenced by this diverse environment and its interrelated concepts of systems, networks, relationships, synthesis, and context. These pluralistic aspects, combined with my security studies education, military intelligence training, and my personal experiences with natural disasters, undoubtedly shaped my analysis and research findings.

In this chapter, I will begin with a reductional analysis approach and deconstruct the United States' homeland security domain's operational environment to identify its essential elements that are important for understanding the homeland security intelligence domain and all-hazards analysts—answering research questions four and five. Next, I will take a relational and integrative analysis approach and explain how the HSIE fits into its operating environment to support the National Preparedness Goal and Department of Homeland Security missions from a pluralistic intelligence perspective—answering research questions one and three. Lastly, I will explain the institutional and professional core competencies essential to the training and development of an all-hazards intelligence analyst—answering research question two. The conceptual framework derived from the

HSOE, the HSIE, and the competencies of all-hazards intelligence analyst will then be evaluated and synthesized in chapter V to create the AH-ISM—answering research question six and the central research question.

Deconstructing the Homeland Security Operational Environment

The HSOE is a security domain within the larger national security domain that encompasses national, international, and global security issues. National security agencies are focused on both external and internal threats to national interests. The international security domain includes threats such as another nation's military, their sponsored militant proxies, transnational terror organizations, organized crime syndicates, or the effects of climate change. The HSOE is primarily focused on domestic threats and it is comprised of three distinct hazard and threat subdomains that overlap in inventive, complementary, and even destructive ways.

These three HSOE subdomains are comprised of people, technology, and nature. Certainly, each of these subdomains are associated with necessary and beneficial critical infrastructure sectors, vital natural resources, and public safety and security assets. Because the U.S. national population depends upon all three domains for survival and prosperity, DHS is mandated to keep the homeland safe and secure. However, these domains also are sources of hazards and threats to the U.S. homeland.

In their own unique ways, the human, technological, and natural worlds have the capacity to create new life, sustain it, and even kill it. From a systems viewpoint, each domain is made of systems within systems (i.e., a system-of-systems) and they are intertwined by complex and wide-ranging networks of independent persons, virtual communities, national institutions, economic partnerships, interstate highways, internet cables, and wireless information sharing intranets. The array of STE systems within the HSOE are seemingly countless. Accordingly, the DHS mission set of providing national safety, security, and resilience applies to the STE systems of the HSOE. DHS and the HSIE also are charged with identifying and countering inherent STE hazards and threats within the framework of the five National Preparedness Missions (e.g., prevent, protect, mitigate, respond, recover).

The HSOE not only consist of STE systems, it also is the territory of DHS operational missions and intelligence activities. The functional and hierarchical organization of DHS is designed to carry out its missions. The DHS operational missions are: (a) prevent terrorism and enhance security, (b) secure and manage our borders, (c) enforce and administer our immigration laws, (d) safeguard and secure cyberspace, (e) ensure resilience to disasters (Our Mission, 2018). These five departmental missions are the operational activities carried out daily by DHS organizational and support components within the United States and in coordination with other FSLTT entities.

Supporting these operational components are DHS intelligence activities that are coordinated with the other 16 members of the intelligence community (IC). This is the HSIE. Through various component intelligence programs (CIP) mission support and intelligence sharing networks, HSIE agencies and private sector organizations work together in this collective national and homeland security domain. Altogether, the domestic STE systems and these operational and intelligence activities comprise the HSOE. Before continuing the discussion about the HSOE's STE systems and ACTN threat systems, an explanation about what comprises a system is necessary.

Systems in the security domain. The HSOE, like all other security domains, must identify what must be secured, what threatens its security, and then how to secure it. Considering the principal theory of a systems view of life, that everything is connected, one can determine that the safety and security fields are primarily concerned about securing STE systems that provide essential services to and have vital resources for the national population (i.e., critical STE infrastructure). Also, security practitioners must understand the STE origins of hazards and threats systems. A breakdown of a system into is functional components and identifiable characteristics helps security practitioners to understand the security problem.

Systems components and characteristics. There are four types of systems: (a) mechanistic (i.e., technology), (b) animate (i.e., people), (c) social (i.e., institutions), and (d) ecological (i.e., environmental) (ACASA, 2018). These types of systems are hierarchical because, for example, the natural or ecological system of the world includes the social systems of humans. And, human created social systems include individual people as well as the technological achievements and activities that are invented by people. I will refer to these systems more concisely as STE systems by combining the animate and social systems into one *social* grouping.

Systems consists of components and characteristics that form the baseline of analytical understanding in the HSOE. To understand the homeland security problem and its context, practitioners must first understand the nature of the systems within the HSOE. For example, preventing a potential flood hazard (e.g., a water reservoir) from ever becoming a threatening flood to a nearby community of homes and businesses, requires an understanding of natural systems (e.g., hydrology and meteorology), social systems (e.g., economics and public administration), and technological systems (e.g., hydraulic engineering and architecture). The basic components and characteristics of systems are multidisciplinary and applicable to the security domain.

Systems Components. Systems have three basic components that must be present for the system to exist: (a) structure, (b) process, and (c) a function and / or a purpose (Ackoff & Emery, 2017, pp. 13-32; Clark, 2017, p. 39; Meadows, 2008, pp. 11-43). The structure of a system can be its physical or tangible shape and size, identifiable boundaries, and its subelements (e.g., a factory or a person) and their relationships. Also, the structure of a system can be intangible elements such as tacit knowledge or esprit de corps (Meadows, 2008, p. 13). Examples of systems structures are the formal and informal information networks of people and machines, the hardline and wireless infrastructure of an office building, the neurotransmitters of the human brain, or the physical structure of a nuclear reactor.

Technically, the processes of a system are the transformational activities that occur in support of the system's objective. A system's objective is its technological function or goal-oriented purpose (e.g., smelting steel or critical reasoning). In other words, a system's process is the "sequence of events or activities that produce results" (Clark, 2017, p. 39). This can be a mechanistic process like the temperature control process of a home's air conditioner that measures, adjusts, and regulates air flow and temperature (Ericson, 2016, p. 20; Meadows, 2008, p. 20). Process also can be cognitive such as the critical thinking steps (Elder & Paul, 2012). Furthermore, it can be a combination of technologically enabled processes and cognitive process. The intelligence cycle illustrates this hybrid process as both an analytical synthesis process aided by technical collection systems and data exploitation software. As a matter of practicality, the technical process and the functional stages or phases of a system work together towards the purpose or objective of the system.

The function of a system is the technological reason or the human purpose of the system (e.g., produce steel for building construction or generate intelligence products for decision-makers). The function or purpose of a system is best identified from its behavior, actions, or products rather what is stated or said (Meadows, 2008, p. 14). It is noteworthy that functions and purposes can be nested as essential subsystems within larger systems to accomplish, for example, a higher-level technical function or a greater humanitarian purpose.

Although function is generally associated with technological systems (i.e., objective driven systems) and purpose with human systems (i.e., purposeful systems), both can be combined in a hybrid function-purpose (Ackoff & Emery, 2017, p. 31; Ericson, 2016, p. 10). For example, knowledge generation in the intelligence domain, like technical collection or cognitive analysis processes, requires the functional and purposeful transformation of data into structured knowledge through the application and interaction of both human minds and software applications.

Systems Functional components. As mentioned above, the technical processes and functional stages of a system work together to achieve the objective or purpose of the systems. Because systems are either machines or people, or a symbiotic hybrid of both, they are objective and goal driven. Open functional systems are characterized by three essential components: (a) input, (b) transformation, and (c) output (ACASA, 2018; Clark, 2017; Bejan & Zane, 2012; Ericson, 2016; Meadows, 2008). The functional and purposeful objective of either mechanistic or human systems requires an input typically of either energy, a stock, or information. Then, a transformational or synergistic change occurs to produce an output from the system. That output is the product of the systemic process and function. Simply put, something goes in, something transformational happens to it, and then something different comes out.

The functional components of a system, whether it is a money laundering scheme, industrial chemical spill, or a hurricane, requires a process supported functional transformation (i.e., a state change) in its stock. The stock of a system are the elements, or entities, of a system that can be identified and measured as input flows, transformational activities, and output flows (Meadows, 2008, pp. 18-19). For example, "dirty" money acquired from criminal activities is invested into a financial institution (i.e., inflow stock). Then, it is transferred to multiple investments and organizations to hide it (i.e., transformational stock). Finally, the "clean" money is reinvested into different financial institutions under the guise of legitimate earnings (i.e., outflow stock). This same functional process can be applied to the inflow, synthesis, and outflow of ideas, knowledge, and intelligence products. In summary, the three basic system components and the three functional components are interrelated and interact to form a complex and unified whole that has a specific function or purpose that is greater than the individual parts, entities, or components of the system (Ericson, 2016, p. 11).

Systems Characteristics. In addition to structure, process, function, and purpose components and the inflow, transformation, and outflow functional components, a system has three distinguishing characteristics about each of its components. System components, tangible or intangible, are: (a) identifiable, (b) detectable, and (c) measurable (ACASA, 2018; Clark, 2017; Bejan & Zane, 2012; Ericson, 2016; Meadows, 2008). This means systems can be perceived, located, and studied by researchers and analysts.

The identifying characteristics of a system encompass its size, color, shape, odor, or any other descriptive characteristic based on the senses of sight, smell, touch, sound, or taste. People can distinguish the similarities and differences among entities and systems by their senses as well as by technical means. Sensors and instruments are designed to replicate human senses at a higher level of fidelity to detect and measure an entity's identifiable characteristics. For example, satellites can take pictures of objects on the earth's surface from great distances in outer space that are undetectable by the human eye.

These finely calibrated sensors and instruments are instrumental in the detection and measurement of systems for further research and analysis. In the safety and security domain, the detection of a toxic chemical in the air, that is measured at a life-threatening level, is an example of detection and measurement. Coupled with the understanding of a chemical plant's operating process, functional components, and products, an analyst could then identify the source of the hazard or threat. Analysts who know STE system components and characteristics that are identifiable, detectable, and measurable are better positioned to carry out safety, security, and resilience efforts within the HSOE. Figure 1 illustrates an open system and its components and characteristics.

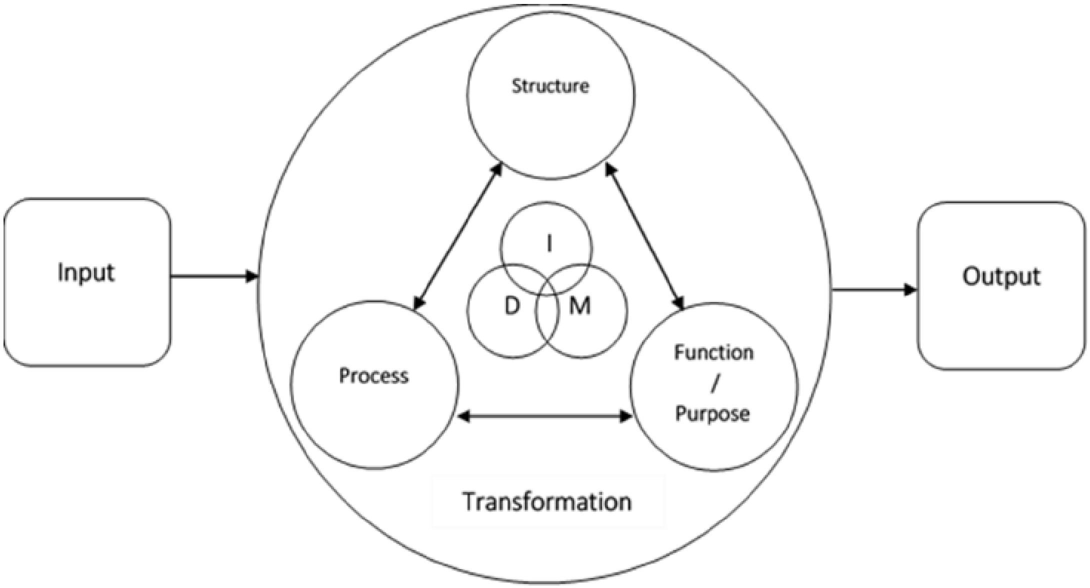

Figure 1. An Open System. A system is comprised of three components: (a) its tangible or intangible structure, (b) its sequential or cyclic process, and (c) its functional and / or purposeful objective. A system's three sequential functional components are: (1) input, (2) transformation, and (3) output. The functional components are supported by the system's process to achieve its objective output. Additionally, a system's components are (a) identifiable, (b) detectable, (c) and measurable. This means a social, technological, or environmental system can be perceived, located, and analyzed. This figure is an amalgam of systems descriptions from The systems view of life by Capra & Luisi, (2014), Intelligence analysis: a target-centric approach by Robert M. Clark (2017), Thinking in systems by Donnella H. Meadows (2008), and Hazard analysis techniques for system safety by Clifton A. Ericson (2016).

Entities. Systems can be further deconstructed into smaller elements or entities; whole systems can be classified as entities too. Entities are the essential objects of a system and should not be confused with the system elements of structure, process, function, and purpose. Entities are commonly depicted as triads composed of three essential characteristics: (a) the *thing* or object, (b) its location in time and space, and (c) its associated properties or characteristics (Antony, 2016, pp. 17-42).

An entity, like a system, is identifiable, discoverable, and measurable. For example, in the natural world, matter is an entity composed of mass (i.e., measurable), occupies space (i.e., discoverable), and has distinguishing properties (i.e., identifiable) such as its current state of being in relation to time. In other words, all systems and entities exhibit or emit spatiotemporal (a) properties or attributes, (b) it's entity state or activity, and (c) its likely relationship to other entities. The significance of entities is that hazards, activators, threats, and events are entities that can be systematically collected and analyzed. To be sure, relationships are intangible entities that are identifiable, detectable, and measurable. Whether they are of STE or ACTN origin, entities are subject to reductional, relational, and evaluative analysis.

Socio-technological-environmental (STE) systems in the HSOE. The types of STE systems in the HSOE are identified throughout the publications and documents of chapter II's literature review. Social systems are comprised of people, communities, businesses, infrastructure, government, and institutions that are both private and public. Accordingly, social and technological systems are derived from multidisciplinary human ingenuity, innovation, and creativity. This means social systems are products of the sciences as much as humanity. Engineers, economist, politicians, and many more people from all academic and practitioner-based career fields comprise the STE systems. And, environmental systems originate from the natural world of mineral resources, plants, animals, and natural phenomenon like earthquakes and storms.

Mnemonics, or memory aids, are useful tools for maintaining organized information and thinking in complex information environments. Two memory aids can help researchers and analysts categorize and recall the common types of STE systems:

PIE and S3E. The first is PIE: population, infrastructure and institutions, economy and environment. The second is S3E: social, engineered, economic, environmental. Another tool for organizing the types of hazards, threats, and crises that originate from STE systems is ACTN or ACTioN (pronounced *action*). ACTN hazards, threats, and their consequential crisis events come from STE systems. Both STE and ACTN systems will be discussed in more detail later in this chapter. Clearly, researchers and analysts can create or choose their own mnemonics, but I will use these three memory aids in my discussion about the human, technological, and natural worlds.

The human world. The human world is, as the term implies, human-centric meaning its population strives to survive and thrive for its own sake just like all other species. However, from a human-centric security perspective, emphasis is placed on the dignified humanity of the individual person and the humane treatment of all people. This means institutional safety and security efforts are intended to protect a person’s right to live in a humanitarian environment, safeguard their natural civil liberties and rights, and guarantee their legal rights through an impartial social justice system (Hampson, 2013, p. 281; Haynes, Hough, Malik, & Pettiford, 2011, p. 552). This human security viewpoint has had a significant influence on the policy formulation and practical application of homeland security and intelligence activities in the United States. For example, U.S. governmental PCRCL guarantees, judicial oversight, and departmental compliance assessments are rooted in these concepts of protecting fundamental freedoms, inalienable rights, constitutional rights, and the right to life and liberty. Compliance with these human security based PCRCL safeguards will better assure the national population that it can live in freedom from want and fear (Malik, 2015, p. 70). On the other hand, when the homeland security and intelligence domains do not comply with PCRCL guarantees, public discontent can manifest as robust demonstrations—a Constitutionally protected activity.

Human security and safety. The human-centric FSLTT homeland security domain relies upon a federal government that creates and maintains "political, social, environmental, economic, military, and cultural systems that together give people the building blocks of survival" (Hampson, 2013, p. 282). Certainly, human security directly links an individual's sense of security to the larger whole-community security apparatus found at the municipal, state, and national levels. To accomplish this task, DHS must balance human-centric and state-centric policy and practitioner requirements through the routine and deliberative administration of intelligence analysis, risk management, and operational tasks within the parameters of PCRCL compliance. Human-centric safety and security planning, policy formulation, and practice considers the types of adversarial threats that originate from the human domain as well as the equally relevant technology-centric and eco-centric concerns that influence the human domain.

The spectrum of threats to human social systems includes a broad range of potential crises originating from economic collapse, food scarcity, environmental resource depletion, political breakdown, demographic tension, criminal proliferation, natural phenomenon, violence, war, or genocide (Malik, 2015, p. 65). Planning for crises, formulating preparedness policies, and resourcing emergency practitioners must be balanced by the competitive safety and security needs that come out human and environmental domains. As indicated by the broad range of threats in the above-mentioned list, human-centric threats in the HSOE are categorized into four groupings for intelligence analysis and operational focus and clarity. Again, the four categories of hazards, threats, and crisis events are adversarial, cyber, technological, and natural (ACTN).

Adversarial hazards, threats, and crisis events. The hazards and threats that originate from the human domain are adversarial by nature. This is because people are purposeful systems driven by goals and intent (Ackoff & Emery, 2017). Therefore, criminals, terrorist, and their crimes are adversarial and threatening to the national population's right to live, to enjoy their civil liberties, and exercise their legal rights. For example, crimes such as burglary, murder, tax evasion, discrimination, and mass shootings, despite their violent and non-violent differences, can deprive victims of their lives, their income, opportunities, and their freedom from living in fear. Certainly, this is not a comprehensive list of all adversarial hazards, threats, and criminally initiated crisis events (e.g., disorderly conduct and arson) that can be found in state or federal jurisdictional penal codes. The significance of adversarial hazards to an HSIE all-hazards analyst is that analysis of criminals, terrorist, and crimes—all-crimes analysis—must also include compliance with PCRCL policies and legal statutory mandates. DHS and the U.S. Department of Justice (DOJ) all-crimes intelligence activities, law enforcement operations, and social justice verdicts within the HSOE, must be PCRCL compliant (PCRCL for Fusion Centers, 2018).

Social systems. Social systems and human systems (i.e., animate systems) are purposeful systems that interact with their natural and technological environments as well as with other social systems. They must interact with their environment to survive (ACASA, 2018). Human systems such as neighborhoods, cities, and businesses rely on social and technological inflows and outflows such as municipal services and financial transactions. Also, they rely on rainfall, sunshine, and clean air as part of their basic needs for survival. Other social systems, also called social assets, include emergency services, utility companies, health care facilities, schools, public administration, jails, online support groups, and volunteer organizations (Pine, 2015, pp. 2-44). This is not a comprehensive list because the scope of human social systems is quite extensive.

The technological world. Technological innovation is the result of human creativity when it is coupled with human problem-solving abilities. Undoubtedly, not all technology is created with a problem in mind. For example, video games are imaginative and technically advanced forms of entertainment that were not intentionally created to solve problems other than boredom. Arguably, decades later, these forms of entertainment are financially lucrative and form an estimated $78 billion economic base as of 2017 (WePC, 2018) thus contributing to solving economic security and human security problems. On the other hand, video game piracy and other cybersecurity concerns illustrate the extent of technological proliferation throughout the human-world. Many more examples of technological integration into society are available for discussion: automobiles, nuclear power generation, global positioning systems (GPS) to name a few. Simply said, people and technological systems are so extensively entwined that nearly all aspects of modern life depend upon their interaction (Ericson, 2016, p. 1).

Physical security and technological safety. The Department of Energy (DOE) and DHS both deliver safety, security, and resilience planning, policy making, and practical application efforts for the national population. The DOE's security programs include nuclear nonproliferation, security of the U.S. nuclear weapons stockpile, management of the strategic petroleum reserve, cybersecurity, critical infrastructure security, worker health and safety, and emergency preparedness training (Department of Energy, 2018). The DHS also is engaged in safety and security efforts alongside other FSLTT departments and agencies like DOE through its National Protection and Programs Directorate, Science and Technology Directorate, and Countering Weapons of Mass Destruction Office. These directorates and offices are supported by other DHS operational and intelligence offices in their efforts to protect critical infrastructure, technological research and development, and countering nuclear proliferation and attack (Operational and Support Components, 2018). Physical and virtual security measures are implemented by DHS in the prevention and protection from technological hazards and threats as well as the mitigation of technological crises.

Physical security and systems safety measures are designed to prevent and protect the nation's population of technological accidents, mishaps, and failures through preemptive forensic engineering (e.g., anticipating potential mishaps and causal factors) (Ericson, 2016, p. 2) and the implementation of physical security standards and resources (Interagency Security Committee, 2015). An example of a physical security approach to public and private institutions is Crime Prevention Through Environmental Design (CPTED). The CPTED approach to physical security emphasizes the relationship between human behavior and design of the physical environment (Fennelly, 2017, pp. 1-21). This is a multidisciplinary approach to physical security including expert studies and expertise from law enforcement personnel, crime analysis, environmental engineering, structural engineering, and behavioral science to better design physical sites and security measures. CPTED's interdisciplinary approach considers police and community relations, urban problems, geography, neighborhood crime problems, business practices, and public administration in its physical and environmental engineering designs.

Systems safety measures are based on hazard risk analysis conducted from a system engineering perspective. Technological systems contain inherent hazards that are statistically predictable thus preventable. “Systems safety… is a form of preemptive forensic engineering, whereby potential mishaps are identified, evaluated, and controlled before they occur” (Ericson, 2016, p. 2). Across the FSLTT technological systems safety field, MIL-STD-882, *System Safety Standard Practice*, is considered the doctrinal guide for implementing systems safety engineering and hazards risk analysis with the primary objective to “identify, eliminate or control, and document system hazards” (Ericson, 2016, p. 3).

Thus far, the adversaries and technology discussions have recognized two of four categories of hazards, threats, and crises within the HSOE. DHS’s *CPG 201: Threat and Hazard Identification and Risk Assessment Guide—Second Edition* groups hazards and threats into three categories: (a) natural, (b) technological, and (c) human-caused (2013, p. 6). However, a third, cyber, is a technology derivative that is of such significance to modern life that I have elevated it to a category of its own.

Cybersecurity. Just as the HSOE is the habitat of a broad range of hazards and threats, security institutions, safety engineers, and analysts, cyberspace is the home a diverse hybrid culture of people and machines. Cyberspace also has a niche culture consisting of hazards, threats, virtual and real institutions, computer science engineers, and digital forensics analysts. “Cyberspace is the realm of computer networks (and the users behind them) in which information is stored, shared, and communicated online”

(Singer & Friedman, 2014, p. 13). It is important to recognize that this information environment is not only virtual; it also is physical and human. Cyberspace truly is a hybrid environment of hardline internet cables, submarine fiber-optic cables, desktop computers, wireless routers, virtual chatrooms, and social media applications, as well as the people who distribute information, currency, and ideology in it. Accordingly, cyberspace has physical, digital, and cognitive characteristics that are both benevolent and malevolent in their nature.

Cybercrime consist of four deviant, criminal, and terrorist behaviors using cyber-technology: (a) cyber-trespass, (b) cyber-deception and theft, (c) cyber-porn and obscenity, and (d) cyber-violence (Holt, Bossler, & Seigfried-Spellar, 2018, p. 23). Within these four categories are a variety of undesirable cyber-behaviors ranging from malicious hacking, privacy violations, digital piracy, fraud, exploitation, harassment, and terrorist recruitment. The U.S. Computer Emergency Readiness Team's (US-CERT) definition of a cyber incident reveals how a cybercriminal exploits cyber-vulnerabilities. A cyber incident is a computer network event that jeopardizes the confidentiality, integrity, or availability of computers, information, communications systems, networks, or infrastructure (National Cyber Incident Response Plan, 2016, p. 8). The CIA triad (e.g., confidentiality, integrity, and availability) are the security goals in an information environment from cyber-threats (Singer & Friedman, 2014, p. 35)

The CIA triad is grounded in ensuring data and user privacy (i.e., confidentiality), unaltered data (i.e., integrity), and system availability. To counter cyber-threats and respond to cyber-incidents that reside in or occur within the HSOE's cyber-domain, the DHS takes on a whole-of-nation approach to planning, policy, and practice approach that includes private and public partnerships. This is a shared responsibility between the private sector and government agencies that own, operate, and protect national critical infrastructure, safeguard and implement PCRCL compliance measures, and synchronize their cybersecurity capacities (National Cyber Incident Response Plan, 2016, p. 7).

Information security. Private and public sector departments and agencies counter cyber-incidents through risk-informed information security programs. Information security programs add a measure of analysis and applied intelligence to the cybersecurity efforts of critical infrastructure protection and network security by following the risk management and risk assessment models of identifying assets, threats, vulnerabilities and cyber-risks. A typical risk-informed cyber-incident process would consist of six phases: (1) preparation, (2) detection and analysis, (3) containment, (4) eradication, (5) recovery, (6) post incident activity (Andress, 2014, p. 16). Also, an information security defensive strategy and analytic approach would consider five zones based on the physical, digital, and cognitive characteristics of cyberspace: (a) data, (b) application, (c) host, (d) internal network, (e) external network (Andress, 2014, p. 19). Together, the risk-informed cybersecurity process and the identification of basic cyber analytic-zones combine into a baseline cyber-analysis process and analytic point-of-entry approach to understanding cybersecurity problems. I will discuss this analytic approach in more detail in chapter V.

Technological hazards, threats, and crisis events. Technological and cyber hazards, threats, and crisis events clearly have a direct relationship with the people who either created, caused, or are affected by them. In the physical world, technological systems safety is focused on the management principles and engineering design of machinery, transportation, or computers with a low or acceptable probability of failure that can cause harm during its life cycle (e.g., system safety, system safety engineering, and system safety management) (Ericson, 2016, p. 5). Examples of technological crises of concern in the HSOE are bridge collapse due to aging infrastructure and outdated design practices, aircraft engine failure due to stress fractures, and industrial toxic chemical release due to accidental safety precaution failures. Technological threats, including cyber-threats, are both safety and security threats because the primary effects and follow-on secondary consequences could impact critical infrastructure and key resources as well as the at-risk communities. Prolonged power outages, economic distress, poor sanitation, and disease related health risk are a few examples of secondary consequences.

Technological systems. The technological systems (i.e., mechanistic and cyber systems) do not have purposes of their own because they did not create themselves. These types of systems were created by people to serve the purposes or needs of people (ACASA, 2018). Examples are homes, watches, cellular phones, satellites, refineries, dams, and water purification facilities designed to protect the environment for the needs of people. Like social systems, technological systems are extensive and too numerous to itemize.

The natural world. The natural world and the human world share similarities that, when taken into consideration, makes the natural environment's hazards, threats, and disasters easier to comprehend. Humans, like other species, are inherently connected to their natural environment for the basic resources to fulfil their physical needs of air, water, food, and shelter (Burton, 2018). Indeed, technological advancements in chemical engineering and the production of synthetic materials in agriculture and building materials are derived from natural resources such as crude oil, animals, and plants. Earth, like people, creates as well as destroys.

Natural processes “concentrate energy and then release it, killing life and causing destruction” (Abbott, 2017, p. 1). As an active planet, energy flows from the earth’s interior, the sun, gravity, and impacts from asteroids and comets. This flow of energy, whether it is internal or external, is the source for environmental hazards, threats to society, and natural disasters. In fact, the constructal theory of flow that I discussed in chapter I is grounded in the understanding of energy flows through all forms of matter and even ideology. This constant flow of energy is responsible for natural disaster sources such as earthquakes, tornadoes, hurricanes, erosion, and drought. This is the process of construction and destruction that create landmasses in the form of volcanic rock and then slowly weathers it to gravel and sand. Also noted in chapter I, panarchy is the understanding of the adaptive cycle of the natural and human world that follows a pattern of growth, conservation, destruction, and renewal. The natural world—our natural environment—is in a constant state of change caused by the flow of energy.

The DHS agency central to responding to and helping others recover from natural disasters is FEMA. Although FEMA is resourced and prepared to respond to all types of disasters, man-made and natural, it is the DHS agency that leads the response to federally declared disasters in accordance with the statutory authorities outlined in the Stafford Act (i.e., Robert T. Stafford Disaster Relief and Emergency Assistance Act—Public Law 93-288). FEMA relies on the whole-community approach to implement national planning frameworks, the national preparedness goal, and to provide disaster assistance when SLTT governmental agencies are overwhelmed.

Environmental security. Environmental problems that originate from the natural world and human world are holistic, long term, and political challenges (Hough, 2014, p. 33). The systemic characteristic of the natural environment, evident by the continuous inflows and outflows of energy and its transformative process of creation and destruction, is an interdisciplinary problem that requires the expertise of the natural sciences, humanities, mathematics, and civil engineering to name a few. A coordinated holistic problem-solving approach by practitioners of varying expertise in law enforcement, biology, architecture, geography, or meteorology is required for environmental security issues that arise suddenly and can last for many years. Plainly, public administration and policy formulation in environmental security requires determined political support. The whole-community approach to environmental security cannot rest solely on local communities because political will is needed to ensure the national population lives in a safe, secure, and resilient environment.

The HSOE includes environmental security concerns as much as it does human security. Human innovation, population growth, and industrial expansion throughout the world has proliferated technology, quickly uses natural resources, and has dramatically changed human and physical geography (Dalby, 2013, p. 312). Human actions are changing the earth’s lithosphere, biosphere, hydrosphere, atmosphere, and even outer space. These human-caused environmental alterations contribute to significant environmental hazards and threats to society. For example, the construction of dams to create water reservoirs and hydroelectric power also destroys river ecosystems and disrupts the flow of water to outlying communities. Resilient populations and infrastructure require adaptive political mindsets, departmental programs, and practical environmental security models. It is in the climate and environmental change scenario that mitigation measures gain prominence among the prevent, protect, respond, and recover preparedness missions carried out by FSLTT governmental agencies and non-governmental organizations.

Natural hazards, threats, and crisis events. Natural hazards are generally grouped into three categories that are based on the physical world: (a) geological, (b) metrological, and (c) hydrological (Hough, 2014, pp. 119-125). This grouping, however, does not address non-human caused biological hazards such as micro-organisms, viruses, and toxins. An expanded grouping of natural hazard sources can be found in the physical zones of the natural world that originate from the earth's core to outer space: (a) lithosphere, (b) biosphere, (c) hydrosphere, and the (d) atmosphere. Adding the human domain of the anthroposphere offers at least five analytic points-of-entry (APOE) for natural and human caused crises.

The lithosphere zone is the realm of seismic activity and produces hazards and threats such as earthquakes that are non-human caused (e.g., natural faultline quakes compared to nuclear detonation caused). Other threats and disasters occur in the lithosphere zone but may have causal factors other than seismic (e.g., subsidence, soil erosion, wildfires, or mass wasting). The biosphere zone is the habitat of natural pathogens, viruses, animal venom, and disease to name a few. The hydrosphere zone is the domain of water borne disease, tsunamis, floods, coastal hazards, and hurricanes. The atmosphere is the origin of metrological and climatic hazards and threats severe storms and tornadoes (Keller & DeVecchio, 2016). Naturally, some natural hazards and threats are hybrid phenomenon like a hurricane that originates in both the hydrosphere and atmosphere. For clarity, I will group natural hazards by the four abovementioned zones and add the anthroposphere (i.e., the human sphere) as a fifth primary analytic zone. Nevertheless, there are at least 45 analytic subzones (i.e., APOEs) within the five primary physical world analytic zones and this tally does not consider outer space beyond the earth's atmosphere (Hassenzahl, Hager, & Berg, 2011).

Environmental systems. Natural environment systems unavoidably include social and technological systems because of the widespread proliferation of people and machines in the natural world (ACASA, 2018). In their purest form, environmental systems are weather phenomenon, the ocean's circulation system, the climate change cycle, and wildlife ecosystems (Hassenzahl et al., 2011). Consequently, the unavoidable convergence of STE systems has shaped the human-centric and eco-centric mindset of society and decision-makers. Human security and environmental security convergence also has shaped sustainable development discussions and disputes about planning and policy decisions by local communities and federal government entities.

At the planning and policy formulation level of government that includes DHS influence as a homeland security practitioner, are three factors: (a) environmentally focused decisions about environment and natural resources; (b) socially focused decisions about the needs of society; and (c) economic decisions about near- and long-term cost of environmental and social policies (Hassenzahl et al., 2011, p. 28). The significance of these factors to the homeland security practitioner are likely to be found in prioritization of homeland security, safety, and resilience resources and their application in the tasks of providing security for lives, property, and the environment. These are public safety and security concerns stemming from the convergence of STE and ACTN systems within the HSOE.

The United States Department of Homeland Security (DHS). "The United States has massive, overlapping homeland security and intelligence enterprises" (Steiner, 2015, p. 12). These security and intelligence domains work together to provide the nation with the capabilities and capacity to achieve the National Preparedness Goal "to prevent, protect against, mitigate, respond to, and recover from threats and hazards that pose the greatest risk" (National Preparedness Goal, 2015, p. 1). Across the national homeland, including its territories, maritime zones, and airspace, DHS carries out various operational missions and intelligence activities in support of the National Preparedness Goal.

Homeland security is an all-encompassing task for DHS. As the third-largest department of the federal government, it must coordinate with and establish cooperative agreements with at least 22 other federal departments and agencies (Mature and Strengthen the Homeland Security Enterprise, 2018); state and local governments; private sector industry; nongovernmental organizations; and the national population to maintain a prosperous way of life. The DHS missions are goal-oriented and functional because they are integrated into the five preparedness missions as well as the department's organizational structure.

Departmental missions. The missions of DHS and their preparedness goals specifically address ACTN hazards and threats ranging from terrorist attacks; chemical, biological, radiological, and nuclear (CBRN) materials; organized crime, unlawful immigration, and cyber. Although not specified in the DHS mission statements, implied

ACTN hazards and threats are all-hazards risks; air, land, and sea-borne adversaries; and illegal trade and travel (Steiner, 2015, pp. 17-18). The six DHS missions are: (a) enforce and administer immigration laws, (b) ensure resilience to disasters, (c) prevent terrorism and enhance security, (d) safeguard and secure cyberspace, (e) secure and manage the nation's borders, and (f) mature and strengthen the homeland security enterprise (Our Mission, 2018). These intelligence enterprise supported missions are conducted daily by DHS personnel in coordination with federal, state, local, tribal, territorial, and private organizations in a complex multijurisdictional, widely distributed, and diverse (Steiner, 2015, p. 21) operational environment.

National preparedness missions. The homeland security enterprise of FSLTT and private sector organizations are viewed by DHS as an "all-of-Nation approach (National Preparedness Goal, 2015, p. 1)" to capacity generation and core capability sustainment in support of the five preparedness missions. Building the resources, capabilities, and trained workforce to, for example, carry out intelligence and information sharing, threats and hazards identification, mass care services, or economic recovery capabilities is the responsibility of the whole national community. Both public and private sector practitioners are involved with the planning and operational coordination activities of the National Preparedness System (NPS), the DHS missions, and the five national preparedness missions (5PM). Preventing terrorism; protecting the national population, property, and natural resources; mitigating the loss of life and property; responding to save lives and meet basic needs; and recovering the economy, infrastructure, health, and environmental systems after a crisis event are the 5PMs (National Preparedness System, 2011, p. 1).

The NPS enables the all-of-Nation homeland security approach to "support decision-making, resource allocation, and measure progress toward these outcomes" (National Preparedness System, 2011, p. 1). In other words, the NPS is a system-of-systems involving intelligence activities, interagency operational planning, resource building, and logistics. The NPS's components are meant to build, sustain, and deliver the 5PM's core capabilities to achieve the NPG (National Preparedness System, 2011, p. 6). The six NPS components follow the meaning-making, decision-making, and problem-solving continuum: (1) identifying and assessing risk, (2) estimating capability requirements, (3) building and sustain capabilities, (4) planning to deliver capabilities, (5) validating capabilities, and (6) reviewing and updating.

There is no way to eliminate every type of hazard or threat to the nation. Adversaries are cunning, technology is imperfect, and the natural cycle of creating and destroying is eternal. It is through understanding this context and by pragmatic acceptance of this fact that risk-informed applied intelligence gains significance. While the NPS strives to generate and allocate limited resources and the 5PMs guide homeland security operational planning, policy, and practice, the HSIE must be cognizant of the importance of providing timely and relevant risk-informed intelligence products to DHS leadership and its operational and support components.

Departmental organizations. The current organizational and support components of DHS have missions that are directly linked to the department's six missions. This is a hierarchical nesting of operational, intelligence, research and development, and managerial missions among the department's subordinate offices, directorates, and agencies. The U.S. Citizenship and Immigration Services (USCIS) enforces and administers immigration laws; the United States Customs and Border Protection (CBP) component secures and manages the nation’s borders; the United States Coast Guard (USCG) secures and manages maritime borders, saves lives during disasters, and prevents terrorism and enhances security; the Federal Emergency Management Agency (FEMA) ensures resilience to disasters; the United States Immigration and Customs Enforcement (ICE) enforces and administers immigration laws; the Transportation Security Administration (TSA) prevents terrorism and enhances security; and the United States Secret Service (USSS) prevents terrorism and enhances security and safeguards financial infrastructure.

Other components support DHS missions in the areas of weapons of mass destruction (WMD) counterproliferation (e.g., Countering Weapons of Mass Destruction Office); conduct research and development (e.g., Science and Technology Directorate); and conducts intelligence analysis and information sharing (e.g., Office of Intelligence Analysis) (Operational and Support Components, 2018). The organization of DHS components not only coordinate with other federal departments and agencies, they also coordinate and conduct research, intelligence, and operations with SLTT and private industry through the Office of Public-Private Partnerships (P3), fusion centers (FC), critical infrastructure Information and Analysis Centers (ISAC), and other HSOE and HSIE initiatives like the Information Sharing Environment (ISE) (Lahneman, Homeland Security Intelligence, 2018; Steiner, 2015, pp. 21-27). More specifically and relevant to the development of the AH-ISM are the intelligence activities of the HSIE and the competencies of the intelligence analysts who work there.

Integrating the Homeland Security Intelligence Enterprise

The HSOE assuredly encompasses all-hazards in all-regions and jurisdictions of the homeland security enterprise. The HSIE is empowered to make sense of it for FSLTT decision-makers. This next section will integrate the HSIE into this HSOE domain of meaning-making, decision-making, and problem-solving.

HSIE communities-of-interest and communities-of-practice. HSIE is the umbrella term for all FSLTT and private organizations that provide risk-informed applied intelligence to the leadership, customers, and components of the homeland security domain. Although there are differing views about which organizations should be included in the HSIE (i.e., the entire IC and other national security stakeholders [Lahneman, Homeland Security Intelligence, 2018]), I have selected a more narrow viewpoint that limits the HSIE to DHS components, their component intelligence programs (CIP), and its intelligence clients, customers, and consumers in the public and private sectors. This view recognizes that the HSIE is a component of the larger federal intelligence enterprise (Richelson, 2016, p. xv) and the homeland security enterprise that operates within the HSOE.

The HSIE is not defined by statute; however, it is referenced in DHS policy and practice. DHS identifies the HSIE as the intelligence offices and CIPs of the Office of Intelligence and Analysis, CBP, ICE, USCIS, USCG, TSA, USSS, and FEMA. Furthermore, CIPs are defined as any organization within DHS's components that conducts the complete intelligence cycle (Homeland Security Committee, 2016, p. 11). This viewpoint of the HSIE couples its intelligence and operations components with that of the broader homeland security enterprise leads to an acknowledgement that homeland security is characterized as a multijurisdictional, multiagency, and multidisciplinary domain.

The stakeholders (e.g., clients, customers, and consumers) of homeland security intelligence include the nation's leadership at all levels of government, owners and operators of critical infrastructure and key resources in the private sectors, the nation's population, and their economic base. All of which are necessary for the nation to survive and thrive. This community of stakeholders is the community-of-interest in the homeland security domain because each member of the whole community has a vital interest in the competency of the HSIE's analytical community-of-practice.

The HSIE's community-of-practice is disperesed across the nation at intelligence and operations centers located in each state, region, municipality, tribe, and territory to include private organizations such as volunteer groups. A simple thought trigger is to group a community-of-interest as the recipients and beneficiaries of the active intelligence participants in the community-of-practice. This simple explanation does not account for interagency and organizational flow of information between the groups; however, it does simplify understanding of them.

There are three characterizations of intelligence stakeholders to define before proceeding. For the purpose of clarity in my research, I have grouped the recipients of intelligence products as clients, customers, and consumers. Clients are actively involved with articulating their intelligence requirements and the overall intelligence synthesis process. They have a vested interest in ensuring intelligence products meet their needs in a timely manner; therefore, they are active participants. On the other hand, consumers are not actively involved with the requirements, analysis, and production of the intelligence products that they utilize. Consumers take what is readily available and determine if it is relevant to their operational and intelligence needs after it is posted or disseminated on information sharing networks. Customers are between the two because they do not specify the timeliness nor the specificity of the products. However, they are recognized by analysts as having a direct and relevant interest in the product's topic. They will be included in the distribution of the product once it is completed. This clarification of clients, customers, and consumers is based on my own experiences and observation in the intelligence domain.

HSIE pluralistic intelligence. Researchers and analysts of ACTN hazards and STE systems come from many scientific and technical disciplines to study the components, characteristics, and interactions of society and disasters. This interdisciplinary approach offers policy makers and other decision-makers, like on-scene incident commanders, a broader context of understanding about how people react and cope with a crisis, and what to expect from secondary and tertiary hazards and threats. Not only must the immediate STE vulnerabilities get attention but also the likely long-term consequences. Although a multidisciplinary approach includes various disciplines of study, an interdisciplinary—or transdisciplinary—approach takes a holistic and unified look at the homeland security problem (McEntire, 2006, p. 1). This is the pluralistic synthesis approach to homeland security.

Pluralistic intelligence is the synthesis of multiple disciplines from the sciences and humanities to generate knowledge about all-hazards and all-crimes by utilizing all-sources of information. It also is applicable in all-jurisdictions of the HSOE. Following the meaning-making, decision-making, and problem-solving continuum, pluralistic intelligence gains two other characteristics that are found in risk management and applied research: probability and practicality. Thus, pluralistic intelligence, in a homeland security domain context, is defined as an interdisciplinary approach to generating all-hazards knowledge and providing risk-informed applied intelligence products to homeland security enterprise leadership and practitioners in support of the National Preparedness Goal.

This definition of pluralistic homeland security intelligence touches upon the STE interdisciplinary, multijurisdictional, all-hazards, and all-crimes (i.e., ACTN) aspects of the HSOE and the HSIE's core requirements of conducting analysis, generating knowledge, assessing risk, and managing information (i.e., intelligence and information sharing) with homeland security enterprise communities-of-practice to achieve the 5PM missions that are carried out in overlapping phases from pre to post incident. This pluralistic intelligence aspect of the HSIE is best represented in the DHS sponsored, state and regionally operated fusion centers (FC).

There are 78 FC's across the nation comprising what is called the National Network of Fusion Centers. These FC's are in disparate climatic zones and geographic regions including rural and densely populated cities. Some are terrorism-centric while others take on an all-crimes analysis and operations approach. Others are all-hazards focused—approximately 48 of the 78 are all-hazards, all-crimes, and counterterrorism focused. They are functionally comprised of representative organizations and personnel from DHS components, state and local law enforcement, corrections, emergency management, the National Guard, and Privacy / Civil Rights and Civil Liberties officers with subject matter expert (SME) skills ranging from management, to analysis, to maritime security (2016 national network of fusion centers final report, 2016, pp. 2-9). Fusion centers illustrate the interdisciplinary environment necessary for pluralistic intelligence to thrive.

Interdisciplinary understanding of hazards and threats in the HSOE. The interdisciplinary aspects of the HSOE and HSIE's STE systems and ACTN hazards and threats are shown by similarities in several of the disciplines that contribute to the interdisciplinary characteristics of the homeland security and intelligence domains. Law enforcement is an established security discipline with proven methodologies for analyzing and investigating crimes and criminals; systems safety engineering has highly technical and methodical procedures for investigating technological mishaps; epidemiology uses a clinical reasoning and testing method for diagnosing diseases and examining epidemics. I will present three triadic models from each discipline to illustrate their similarities in identifying hazards and threats: first is the law enforcement triad; second is the technological hazard triad, and third is the epidemiologic triad.

Law enforcement. The law enforcement problem analysis triangle, or crime triangle, actually is two triads that are merged together. The first depicts the routine activities that "must converge in time and space for crime to occur (Walker & Drawve, 2018, p. 42)": (a) the offender, (b) the victim, and (c) the place. The second depicts the *controllers* that can "prevent a crime from occurring (Walker & Drawve, 2018, p. 42)": (a) the offender's handler, (b) the victim's guardian, and (c) the manager of the place where the crime is committed. This crime triad illustrates the essential interaction and relationships among the elements of a crime event. First is the adversarial threat; second is the social system target (e.g., a person); third, is the time and location nexus of the crime event. The application of handler, guardian, and manager layers illustrates the potential and need for prevention, protection, and mitigation of potential crime events. Handlers can prevent the offender from committing a crime. Alternately, a handler can encourage the commission of a crime too. Guardians can protect victims by their presence or other preventative means. Lastly, managers can apply prevention, protection, and mitigation measures at places they control (e.g., physical barriers, lighting, or employment of guardians). The crime triad implies that offenders take advantage of a victim's or place's vulnerability while committing the crime (see figure 2).

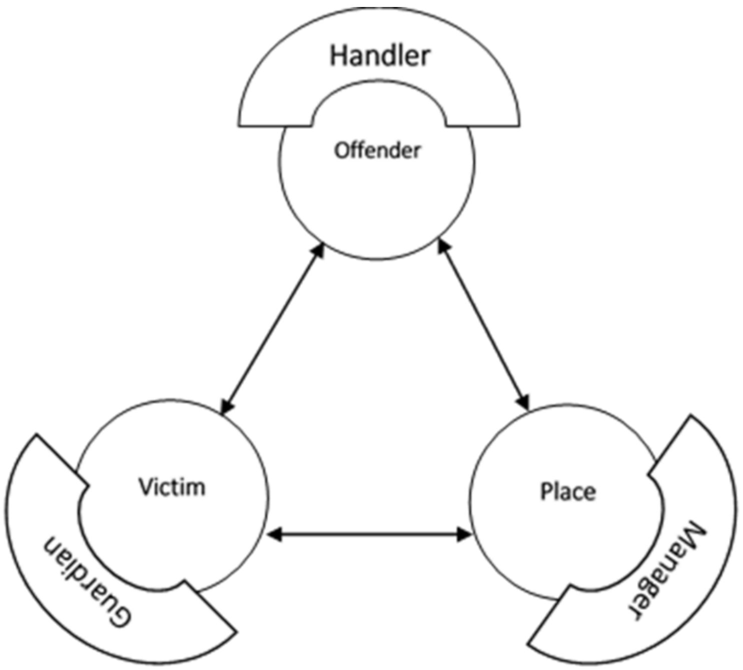

Figure 2. The Law Enforcement Crime Triad. The crime triad is two converging triads in time and space consisting of (a) the offender and handler, (b) the victim and guardian, (c) the place and its manager. The triad illustrates the potential for prevention, protection, and mitigation of a crime event. Handlers can prevent offenders from committing a crime. Guardians can protect victims from the offender. And, managers can mitigate the opportunity and effects of likely crime events. This figure is adapted from descriptions in *Law Enforcement Intelligence* by David L. Carter (2009), *Intelligence analysis for problem solvers* by John E. Eck and Ronald V. Clark (2018), *Out of bounds: innovation and change in law enforcement intelligence analysis* by Deborah Osborne (2006), *Intelligence-led policing* by Jerry H. Ratcliffe (2016), and *Foundations of crime analysis* by Jeffery T. Walker and G. R. Drawve (2018).

Systems safety engineering. A technological hazard has three components that also must converge in time and space for a mishap or accident to occur: (a) a hazard source, (b) an initiating mechanism, and (c) the target and threat outcome. The hazard source (HS) is the hazardous resource of energy in the technological system and it is the component that produces danger. The initiating mechanism (IM) causes the hazard to transform from a dormant state to an active state to cause a mishap. The target and threat outcome (TTO) are assets or targets that are vulnerable and the consequences of the mishap (Ericson, 2016, p. 34). The interactive relationship among the three hazard triad components converge in time and space (see figure 3).

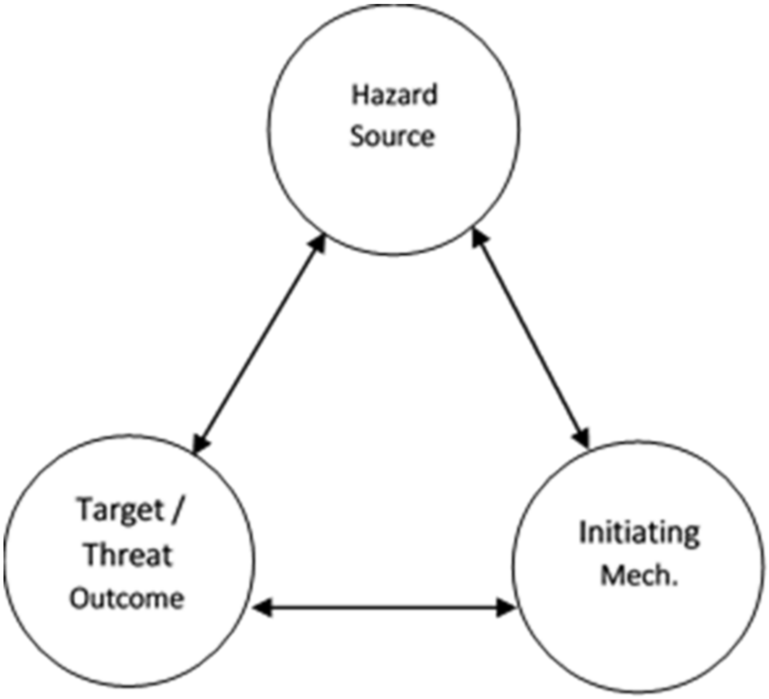

Figure 3. The Technological Hazard Triad. The convergence in time and space of a hazard source, initiating mechanism, and the target transforms a hazard into a technological mishap with a threat outcome (i.e. consequences). Systems safety engineers use this triadic model as their entry point to analyze and investigate technological hazards, threats, and accidents. This figure is adapted from *Hazard analysis techniques for system safety* by Clifton A. Ericson (2016).

Epidemiology. Disease is the result of interacting genetic and environmental factors and is easily illustrated through communicable disease in the form of an epidemiologic triad consisting of: (a) the host (e.g., a person), (b) the agent (e.g., bacterium), and (c) the environment (e.g., contaminated water) (Gordis, 2014, p. 19). People are susceptible (i.e., vulnerable) to disease through their own bodies and the environment by way of transmission vector that delivers the disease. This epidemiologic triadic convergence occurs in time and space like the crime and hazard triads. Similarly, this triad acknowledges that a person's vulnerability to the disease increases their likelihood of contracting it (see figure 4).

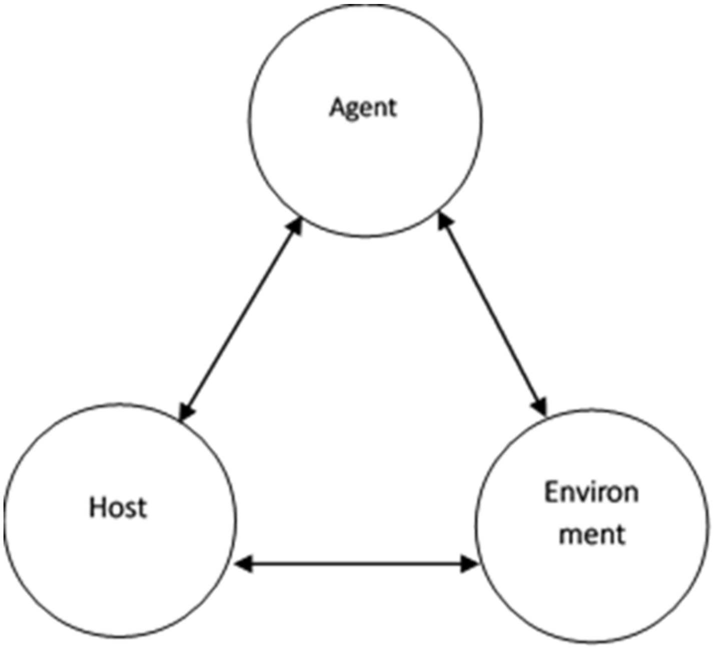

Figure 4. The Epidemiologic Triad. Communicable disease is illustrated by the epidemiologic triad comprised of a host, an agent, and their environment. The disease is transmitted via a vector and it exploits a vulnerability within the host to thrive. The convergence of a person with a disease and a favorable environment for infection takes place in at a specific time and space. This figure is adapted from descriptions in *Epidemiology* by Leon Gordis (2014).

Interdisciplinary synthesis. These three triadic models from law enforcement, systems safety engineering, and epidemiology illustrate the similarities among the various disciplines in the homeland security and intelligence domains. By reducing an event into its most basic interactive components, an intelligence analyst or investigator is better able to establish the relationships among the entities as they converge in time and place. Moreover, they can identify vulnerabilities, likelihood, and preparedness measures. Along with an understanding of systems components, these triadic models are interdisciplinary and useful for conducting risk-informed applied intelligence assessments in the all-hazards and all-crimes security environment.

The interdisciplinary all-hazards crisis event predicate. By synthesizing these triadic models, and the criminal predicate model, one can create an interdisciplinary all-hazards crisis event predicate model. The criminal predicate model, like the crime triad, illustrates the convergence of three necessary components in time and space to create a reasonable suspicion that a crime is or is about to be committed (Carter, 2009, p. 63). The three converging components are: (a) people or organizations, (b) the elements of a crime per the penal code, and (c) the time and place. This convergence also is called the criminal nexus and its usefulness in understanding crime events underscores its interdisciplinary applicability in understanding the nexus of society, threats, and vulnerabilities in time and space (see figure 5).

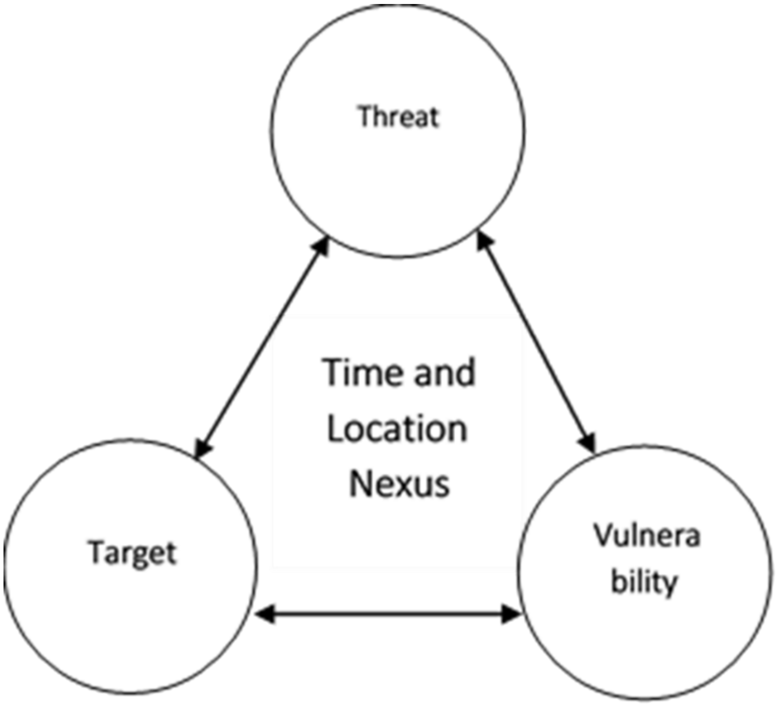

Figure 5. Interdisciplinary All-Hazards Crisis Event Predicate. A crisis event predicate is the convergence of an ACTN threat with a STE target's vulnerability in time and space. The crisis event is the result of a systems-based transformation process from a dormant hazard to an active threat to a realized crisis event. All crisis events emerge from the interactive relationships among these three components and activators (i.e., initiating mechanisms). The homeland security domain's interdisciplinary FSLTT and private partnership plans, policies, and practitioners serve as administrative and practical *handlers*, *guardians*, and *managers* to implement the 5PMs of prevent, protect, mitigate, respond, and recover. This figure is the result of research synthesis from previously cited sources.

Analytic approaches and points-of-entry. The interdisciplinary convergence of identifying systems components, their functional components, and their characteristics with the crisis event predicate marks the beginning steps of establishing a unifying interdisciplinary analysis methodology. Along with systems theory's emphasis on connectivity and relationships, flow theory's emphasis on the natural tendency of energy and ideas to flow among systems, and transformational state changes that occur within systems, an all-hazards analyst can identify initial APOEs to begin analysis of a phenomenon. For example, an analyst who is studying the potential crisis event in a region can choose an APOE from a list of STE assets (e.g., a neighborhood), from the ACTN hazard sources (e.g., river basin), from ACTN threats (e.g., flooding), or from a known crisis event (e.g., hurricane landfall). Additionally, APOE's can be established by geographic or atmospheric zones. Rather than an APOE based on *who* or *what* questions, an all-hazards analyst also can begin with *where* and *when* questions.

An interdisciplinary method for choosing an APOE also can be found in the natural and human world's geographic and atmospheric zones. Beginning at the earth's core and through the atmosphere's layers to outer space, an analyst can select APOE zones to study what types of STE and ACTN systems reside there and when are they present. For example, an oil and gas platform in the Gulf of Mexico extends upward from ocean surface into the lower atmospheric zone and below into the ocean's underwater zones on into the earth's crust. In this example, there are at least six APOE zones affected by an oil and gas platform: the lithosphere, the three oceanic life zones (e.g., the hydrosphere), the biosphere, and the troposphere. Moreover, the potential for a technological disaster on an oil and gas platform could extend the affected zones and APOEs higher into the atmosphere by wind, out across the ocean's surface by currents, and into the depths of, and onto, coastal zones and the wide-ranging human zone called the anthroposphere. Further analysis of this oil rig disaster would reveal the potential for secondary and tertiary STE and ACTN crisis events in affected soil zones, biomes, and trophic levels. Figure 6 depicts some of the APOEs available to all-hazards analysts.

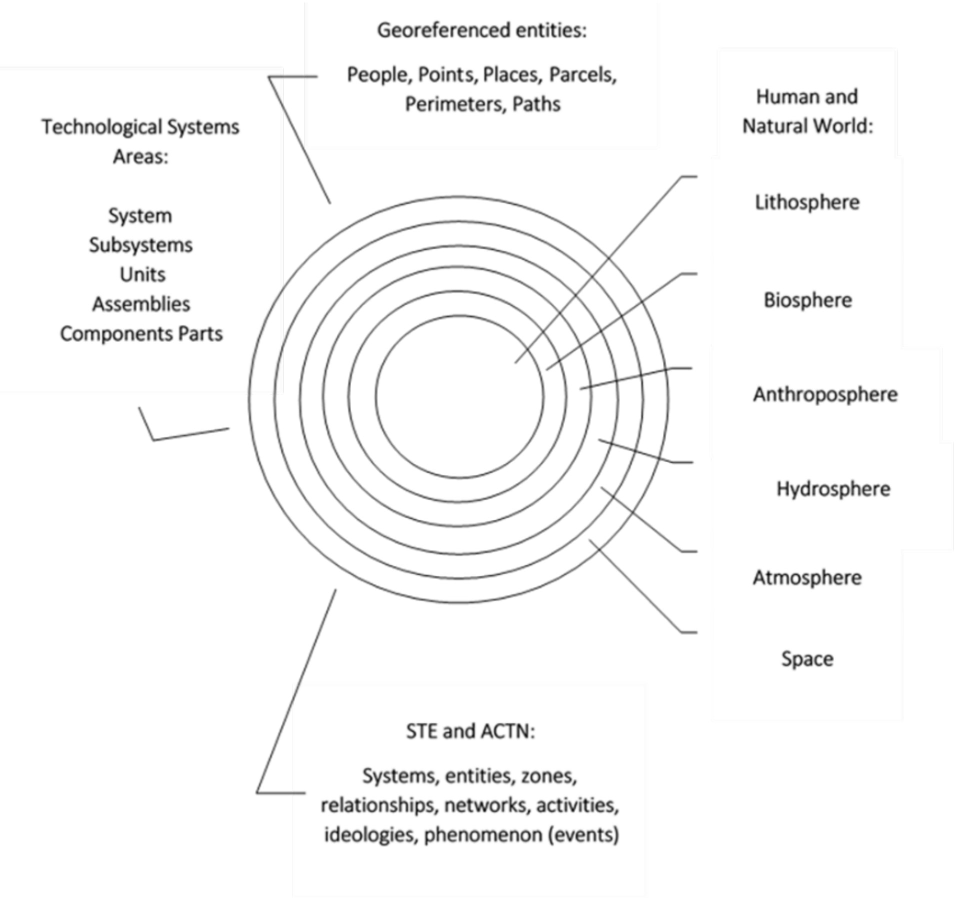
Georeferenced entities:
People, Points, Places, Parcels, Perimeters, Paths
Technological Systems Areas:
System
Subsystems
Units
Assemblies
Components Parts
Human and Natural World:
Lithosphere
Biosphere
Anthroposphere
Hydrosphere
Atmosphere
Space
STE and ACTN:
Systems, entities, zones, relationships, networks, activities, ideologies, phenomenon (events)

Figure 6. Analytic Points of Entry (APOE) Examples. STE and ACTN systems are found in nearly every zone of the earth and atmosphere. This figure represents only a few that can be used as APOE zones for all-hazards analysts. A more comprehensive list of the natural and human world's APOE zones identifies at least 45 in the various biomes, trophic levels, freshwater, ground water, coastal, oceanic, earth, atmospheric, and anthroposphere zones. This figure is the result of research synthesis from previously cited sources.

An all-hazards analyst has at least three security and interdisciplinary analytic approaches in addition to the APOEs. An analyst can approach an intelligence problem from a target-centric (Clark, 2017), activity-based (Biltgen & Ryan, 2016), or risk-informed STE analysis perspective. In other words, an all-hazards analysts can analyze the ACTN phenomenon as a known entity or system (e.g., the hazard or threat target-centric analysis); the activities occurring within a zone that may reveal unknown entities or systems (e.g., patterns of life and activities-based analysis); or the STE system, its vulnerabilities, and probability of experiencing a crisis event (e.g., risk-informed analysis). Recall that systems and entities are identifiable, detectable, and measurable; and, events can be predictable and preventable. Also note that not all intelligence must be risk-based and anticipatory because intelligence may be produced for its own sake without applying the fundamentals of risk assessment and risk management. These approaches help the all-hazards analyst to establish an analytic approach or perspective that is either centrally focused on the ACTN threat, the STE asset, or the various activities that may identify or detect an ACTN or STE system in a zone.

The HARTE crisis event model. Given the flow principle, transformational state changes, and the holistic significance of relationships among interconnected entities, another foundational conceptual model about all-hazards crisis events can be constructed. In this model, ACTN hazards can become threats to STE systems and on to become crisis events. Like the initiating mechanisms in the technological hazards triad, activators initiate the transformation of a dormant hazard into an active threat to STE systems. And, the interaction of active threats with unsecure STE systems cause crisis events. This is the hazard-activator-relationship-threat-event (HARTE) crisis event model. This triadic model is an ACTN and STE system continuum of hazard to threat to crisis event that has a spatiotemporal nexus with activators and relationships. Incidentally, this transitional concept as described by Dr. Bruce Newsome in his book *Security and Risk Management* (2014) was my point-of-entry-text (POET) for the AH-ISM. Although the mnemonic HARTE is my creation, I would like to give credit to the POET of my research because it is the original text that my research findings are layered and constructed over (Kincheloe & Berry, 2004, p. 109). The HARTE model is depicted in figure 7.

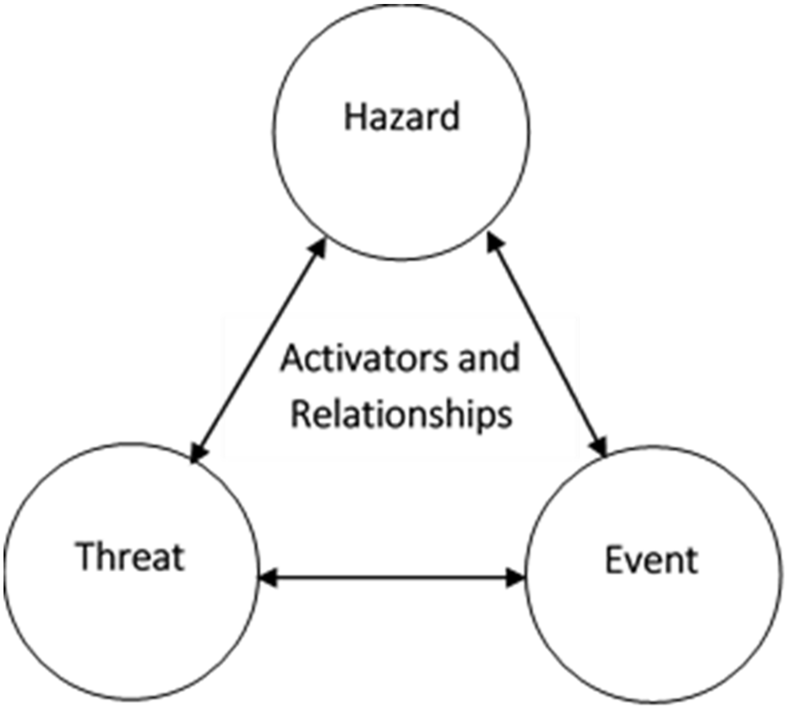

Figure 7. The HARTE Crisis Event Model. In this interdisciplinary all-hazards model, dormant hazard sources interact with activators to become threats; then, relationships among ACTN hazards and activators create active threats to STE systems; lastly, active threats interact with unsecure STE system vulnerabilities to come crisis events like disasters. This figure is the result of research synthesis from previously cited sources.

The HARTE interdisciplinary crisis event model examples. Two interdisciplinary examples from the natural sciences and medical sciences help illustrate the transdisciplinary application of the HARTE crisis event model. The first (see figure 8) depicts the hazard-threat-crisis event continuum as an earthquake along with examples of how seismologist and municipal handlers, guardians, and managers may coordinate and cooperate in pre and post-event ways. The second (see figure 9) depicts the hazard-threat-crisis event continuum as an epidemic with examples of how medical and municipal handlers, guardians, and managers may coordinate and cooperate in pre and post-event ways. In both models, multidisciplinary and multijurisdictional information sharing from data collection (e.g., data identification, detection, and measurement) by sensors and instruments as well as interdisciplinary and interagency coordination and cooperation for policy formulation, emergency planning, and practical application based upon risk-informed all-hazards intelligence is evident.

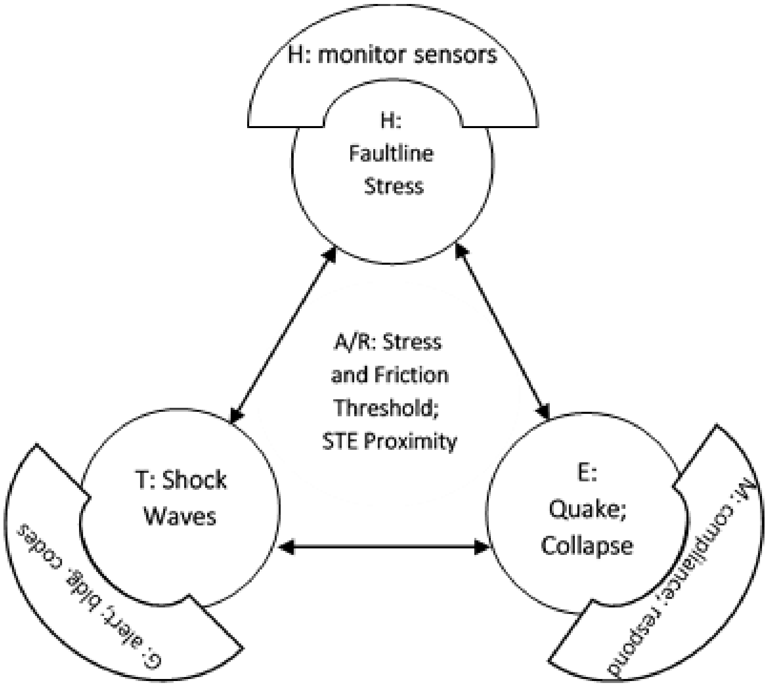

Figure 8. Interdisciplinary Crisis Event Triad Example: Earthquake (not human caused). Natural earthquakes are the result of stress overcoming friction thresholds along a geological fault possibly near STE communities (Abbott, 2017; Federal Emergency Management Agency, 1997; Keller & DeVecchio, Natural hazards, 2016; Mileti, 1999). As illustrated in this figure, (1) a faultline stress hazard source is identified and measured by geologist *handlers* using seismic sensors and instruments; (2) active threat shock wave are emitted and they are detected and measured for seismic event alerts as well as useful data for municipal *guardians* who make construction safety policies and building codes; (3) municipal *managers* comply with construction codes as a prevention, protection, and mitigation effort and respond during realized crisis events. This figure is the result of research synthesis from previously cited sources.

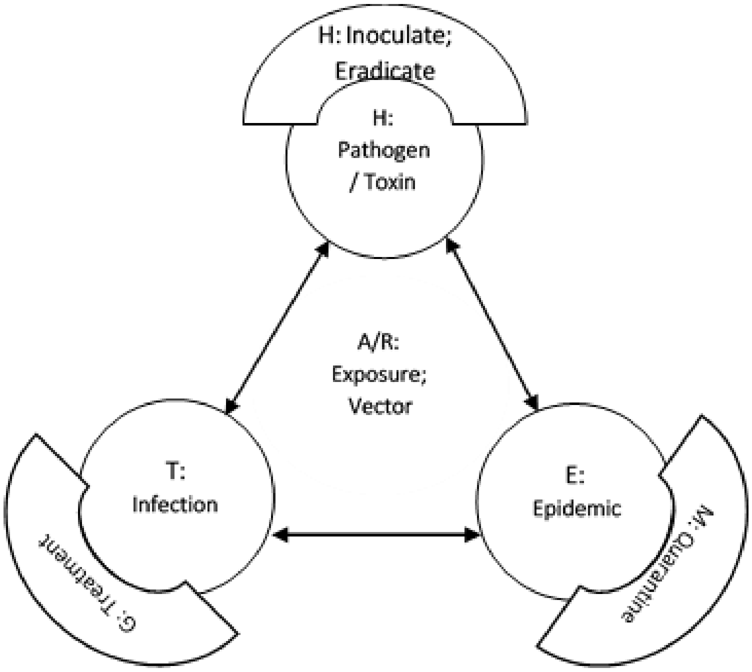

Figure 9. Interdisciplinary Crisis Event Triad Example: Disease / Contamination Outbreak. Disease (or a hazardous material contamination) is the result of a pathogen or toxin infecting a host to become an epidemiological hazard source (Gordis, 2014; Stern, Cifu, & Altkorn, 2015). As illustrated in this figure, (1) potential pathogen agents (i.e., hazard source) are identified and measured by epidemiologist *handlers* using medical sensors and instruments; (2) active threat host (e.g., human or animal) are exposed, infected, exhibit symptoms, and are then tested, diagnosed, and treated by medical *guardians*; (3) additional host and vectors are detected and measured for community epidemic alerts as well as collecting useful data for medical and security *guardians* who make health care policy and plans; (4) municipal *managers* comply with epidemic emergency policies and plans as prevention, protection, and mitigation efforts and respond during realized epidemic crisis events. This figure is the result of research synthesis from previously cited sources.

In summary, pluralistic intelligence in the homeland security domain is innately interdisciplinary. These brief explanations about analytic approaches, APOEs, and the HARTE crisis event model help illustrate the interdisciplinary nature of ACTN crises and STE systems. Thus far, my discussion about pluralistic intelligence has not been comprehensive and only serves as an introduction about the multidisciplinary, multiagency, multijurisdictional, and multidomain characteristics of STE systems and their potential crisis events caused by ACTN threats. By adopting a systems view and an interdisciplinary perspective in my analysis, I created three fundamental concept models for analysts to reference and use: the systems components model in figure 1, the all-hazards crisis event predicate model in figure 5, and the HARTE crisis event model in figure 7. Along with selecting a systemic analytic approach and APOE entity or zone, an HSIE analyst is better situated to conduct intelligence analysis, academic research, or investigations into all-hazards analysis problems.

The HSIE intelligence synthesis system components. The HSIE is an intelligence system-of-systems. It is an enterprise of networked people, knowledge, information systems, and institutions distributed across the nation and with global connections. Like the petroleum industry's core function and purpose to produce petroleum-based products from oil and gas resources for the national population's consumption, the HSIE's function and purpose is to generate risk-informed applied intelligence products from raw data for the national leadership and stakeholder's consumption. These intelligence activities are purposeful by supporting the NPG to ensure national safety, security, and resilience and are functional by adhering to systemic core competencies and processes. Four institutional core competencies are necessary for risk-informed applied intelligence production: (a) knowledge management, (b) information management, (c) risk management, and (d) intelligence analysis.

These four core programs and processes establish the cornerstone of meaning-making and are directly linked to the system components of structure, process, function, and purpose. Without information management and information technology networks, there would be no data collection and information sharing structure to the HSIE. Without knowledge management, there would be no knowledge generation process or intelligence production function. Without intelligence analysis and risk management, there would be no purposeful products for application in the decision-making and problem-solving processes. These core competencies will be discussed in more detail in following sections, but for now I will explain the HSIE's system components. The link among meaning-making core competencies and decision-making is summarized by author Richard Antony:

> Regardless of the application, decision-making tasks of practical interest generally require evidence gathering, analysis, and various forms of evaluation / assessment. Given the complexity of many applications, from situational awareness to predicting the weather, decision-making frequently requires exploitation of a variety of relevant information sources, application of appropriate a priori knowledge, as well as intelligent combination of the evidence (Antony, 2016, p. 1).

Intelligence purpose. Intelligence is state of being, a process, and a product. Intelligent people, animals, or machines are said to have *intelligence* like it is a descriptive characteristic of their state of being. Intelligence also is a process that flows from the collection of data to the final production of an intelligence product for a customer. Accordingly, intelligence also is the product. It is the manifestation of data, information, and knowledge into a form that is useful—actionable and applicable. It is the "information that meets the stated or understood needs of policy makers and has been collected, processed, and narrowed to meet those needs" (Lowenthal, 2015, p. 2). Following this definition, intelligence is attained, created, and produced for a purpose. It fulfills the needs of meaning-making to support decision-making.

Intelligence activities. To do this, intelligence is derived from data sources by human and technical means. The information management process of collecting, analyzing, and sharing intelligence begins with identifying the sources of data and the means to get it. There are five means (i.e., disciplines) that also translate into sources: (a) open source intelligence (OSINT), (b) human intelligence (HUMINT), (c) signals intelligence (SIGINT), (d) geospatial intelligence (GEOINT), and (e) measurement and signature intelligence (MASINT) (Lowenthal & Clark, 2016, p. 1). Altogether, these are the primary groupings of intelligence disciplines, sensor types, and all-source data that will eventually become actionable and applied intelligence after a process of intelligence analysis and synthesis—they are called the 5-INTs. In its entirety, the processes and programs that are maintained and executed by the intelligence community (IC) are referred to as intelligence activities. Another way of understanding data sources is by the MODES (e.g., media, observation, documents, experts, and secondary sources) method that I discussed in chapter I and will discuss again in chapter V. At this point, I will focus on the IC's use of the 5-INTs.

The HSIE's intelligence management system. Intelligence activities are managed by the IC and HSIE in a systemic method through institutional policies, programs, and processes. The intelligence management system, like any other system, has the components of process, function, purpose, and structure with identifiable inflows and outflows of data and information. Surely, what happens to the inflow of raw data before it becomes an outflow of intelligence is a transformation process called synthesis because it merges and analyzes data from multiple sources.

Intelligence management process. Managing the 5-INTs is easily explained by the TCPED process of tasking, collecting, processing, exploiting, and disseminating intelligence products (Lowenthal & Clark, 2016, p. 1). The TCPED process requires IC and HSIE leadership, management, and analysts working with clients and customers to establish collection requirements, conduct collection tasking and management, process raw data into an understandable format (e.g., digital data into readable text), exploit the data into usable information for analysis, and finally to disseminate or share the final product with clients, customers, and general IC consumers. Experienced managers are required in each TCPED intelligence activity phase to ensure timeliness, quality, and reliability of the finished intelligence product. To simplify this process and present it in an interdisciplinary format for academic researchers, students, and practitioners in other fields like emergency management, I will use the CASA mnemonic: collect, analyze, synthesize, and apply. These are the four core competencies of the intelligence process as it relates to an all-hazards risk-informed applied intelligence model.

Intelligence management function. The intelligence function of transforming raw data into useable information, knowledge, and actionable intelligence requires both human reasoning and machine aided applications. This is the knowledge generation aspect of the knowledge management core competency. Managing the intelligence function requires a hybrid of technology and goal-oriented humans. The 5-INTs produce more data than a team of analysts can analyze; the challenge is access to too much data, rather than not enough, and the ability to analyze it. Another challenge is that analysts need to understand the 5-INT collection process to better apply the knowledge generation function.

Knowledge generation follows a continuum that flows from the input of raw data from sensors into analysis applications like the U.S. Army's Distributed Common Ground System-Army (DCGS-A) that is a system for managing large amounts of data from collection to production (U.S. Army Acquisition Support Center, 2018). Information management technology systems like this help the analysts in critical reasoning and analysis of raw data to transform it into useful information. Then, that information is further analyzed along with current and historical context to generate knowledge. At this point, the knowledge gained through this functional process becomes applied intelligence when it is integrated into the purposeful processes of decision-making and problem-solving. Thus, data is synthesized into intelligence in a functional and purposeful manner. This is the DIKI knowledge generation continuum (Ratcliffe, 2016, pp. 71-74).

Intelligence management purpose. The purpose of CASA and DIKI process and function is to produce risk-informed applied intelligence. As previously stated, this is meaning-making in support of decision-making and problem-solving that is an intelligence management purpose. The final intelligence products are intended to alert (i.e., early warning), assess, advise, anticipate, and to be applied by intelligence and security practitioners in at least three ways: (a) a deliberate planning process, (b) policy formulation, and (c) practical application. These are the 3Ps of integrated and applied intelligence products. As stated, analysts can influence the 3Ps by providing alerts, assessments, anticipatory estimates, or advice (4As) if desired by their clients, customers, or according to their institution's normal practice. The mnemonics CASA, DIKI, 4As, and 3Ps will be integrated into the AH-ISM discussion in chapter V.

Intelligence management structure. The intelligence enterprise is comprised of networked analysts, intellectual capacity, knowledge repositories, information technology systems, and institutional infrastructure, and institutional organization hierarchies. The structure of the IC and subcomponent intelligence entities is physical and virtual. It is comprised of cables, radio frequencies, sensors, instruments, operators, maintainers, analysts, facilities, information sharing communities-of-interest, human spies, and overhead satellites in space. Undoubtedly, the intelligence management structure is as complex as the intelligence system-of-systems. Along with the processes, functions, and purposes that I have described, intelligence structure, supported by information management policy and programs, is a required component of the overall system. Specifically, the intelligence management structure that I will discuss in more detail is structured communication because without it, applied intelligence assessments and products cannot be understood nor disseminated to those who need it. A breakdown in structured communication means a breakdown in the entire intelligence synthesis system.

Intelligence activities are complex technical and human systems with distinct institutional structures, internal processes, technical functions, and goal-oriented purposes. Each system component requires intensive intelligence management oversight to synchronize and synthesize. To summarize, the CASA process populates the DIKI function that drives the structured communication and deliberate application of intelligence in the 3Ps to meet the client's requirements. Next, I will give a more detailed explanation of how the intelligence synthesis system's four core competencies are integrated into risk-informed applied intelligence process.

The HSIE intelligence synthesis system's core competencies. Intelligence activities and intelligence management's systems components (e.g., intelligence process, function purpose, and structure) relies upon four fundamental institutional programs and processes to generate, organize, retain, safeguard, and disseminate intelligence. The principles of these four core competency programs establish the foundation and bring together the people, tools, and systems needed for intelligence synthesis. Altogether, knowledge management, information management, risk management, and intelligence analysis form the core components of the intelligence synthesis system and, together, they assure the diligent production of risk-informed applied intelligence within the HSIE.

Knowledge management core competency. Knowledge management is "doing what is needed to get the most out of knowledge resources" (Becerra-Fernandez & Sabherwal, 2015, p. 4). This means intelligence management must leverage the human capital, organizational capital, and social capital within the HSIE. The employees and practitioners of the HSIE are the human resources of intellectual capital gained from their knowledge, technical and interpersonal skills, and productive capabilities. Additionally, the HSIE's institutional knowledge resides in its databases, doctrinal manuals, organizational culture, and systems components. Lastly, the HSIE's social capital is found in the relationships, formal and informal, and information sharing interactions among its communities-of-interest and practice (Becerra-Fernandez & Sabherwal, 2015, p. 5). The knowledge capital and the intelligence generation capacity of the HSIE's personnel, organizations, and social groups contribute to its ability to ensure long-term institutional knowledge continuity.

Knowledge management foundations. The problem-solving task of the homeland security and intelligence domains is directly connected to the three foundations of knowledge management (KM): (a) KM infrastructure, (b) KM mechanisms, and (c) KM technologies. These three foundational tenets of KM make available the technical and organizational infrastructure that is needed to produce and share knowledge. An overlap exists between KM foundations and information management in the use of information technology (IT) to support their processes; however, KM is generally focused on establishing enduring IT and organizational structures for long-term continuity and retention of knowledge resources. In other words, KM is in the business of building knowledge capital and capacity and IM is in the business of enabling KM to accomplish those goals.

Knowledge management solutions. The foundations of KM capital and capacity generation (i.e., meaning-making) exist to support KM solutions (i.e., decision-making and problem-solving). KM solutions are the processes of gathering data, information, and knowledge and then retaining, sharing, and applying it by using integrated KM systems and technologies. The four primary tasks that are conducted through the application of KM foundational principles, creating, organizing, transferring, and applying knowledge (Department of the Army, 2014, pp. 3-6), directly contribute to the KM solution principle. Again, an information management overlap occurs here; but, it's important to note that KM is a broader program dedicated to the getting the most out of knowledge resources to achieve organizational goals as well as long-term knowledge continuity (Becerra-Fernandez & Sabherwal, 2015, pp. 41-43). This line of thought is similar to creating institutional “deep*”* knowledge that will be passed along from one generation to the next.

Knowledge management and intelligence synthesis discussion. The constructal theory about the natural flow of energy and ideas among entities is captured in knowledge management’s foundations and application. KM aids the natural flow of knowledge to enhance shared understanding among people and organizations, individual and institutional learning, and decision-making (Department of the Army, 2014, pp. 3-2). Knowledge generation (i.e., the DIKI functional continuum) also is a key principle in KM and is often presented as DIK or DIKU: data, information, knowledge, and understanding (Becerra-Fernandez & Sabherwal, 2015, p. 20; Department of the Army, 2014, pp. 3-1).

The DIKI intelligence creation continuum is the primary functional component of purposeful intelligence synthesis. Moreover, the KM tasks of knowledge generation, organization, sharing, and application are equated to the four core competencies of analysis (e.g., critical reasoning, knowing the subject matter, communicating, and then applying the knowledge). These core competencies will be discussed in a coming section in this chapter.

Information management core competency. Closely related and having overlapping processes with KM is the second core competency: information management (IM). This managerial process is narrower in focus than the broader KM focus to generate knowledge capital, capacity, and continuity. IM is the “science of using procedures and information systems to collect, process, store, display, disseminate, and protect data, information, and knowledge products” (Department of the Army, 2014, pp. 3-6). IM enables KM by providing IT systems, security measures, and technically trained personnel to support intelligence activities, operational missions, managerial decisions, and applied solutions to problems. IM helps intelligence analysts create accurate, timely, useable, complete, precise, and secure (Department of the Army, 2014, pp. 3-7) intelligence for the customer.

Information systems and technology. Knowledge and intelligence are the cognitive aspects of KM and IM. IT is the physical and virtual dimension comprised of collection sensors, measurement instruments, data processors, databases, display consoles, and information sharing networks. Without IT, knowledge generation would be limited only to the human mind with limited ability to process terabytes of metadata, create digital situational awareness graphics, multiecheloned anticipatory and probabilistic threat assessments, and share them across the national and global IC network. IT systems enhance the human capacity to collect, analyze, synthesize, and communicate information.

The intelligence cycle and the 5-INT disciplines are heavily reliant upon IT. The CASA process of collecting, analyzing, synthesizing, and applying intelligence depends on technical collection platforms and instruments to collect and measure data on earthquakes, terrorist, and cyber criminals. Academic researchers also rely on IT to collect data from the media, direct observation, documents, expert interviews, and other secondary sources (i.e., MODES). The DIKI function, structured communication, and the integration of intelligence into the 3Ps of plans, policies, and practice, also rely on a robust IT infrastructure.

Information management and intelligence synthesis discussion. Systems and entities are identifiable, detectable, and measurable because they emit information about their identifying characteristic like location, size, shape, or color. These signatures are emitted in many ways that are detectable by highly sensitive sensors that are calibrated to detect and measure what is identifiable about a system or its components. For example, electromagnetic waves are emitted or reflected from on object on earth that is detectable from airborne collection platforms like unmanned aerial vehicles (Clark, 2011, pp. 1-35). Also, acoustic and chemical signatures are detectable and measurable by instruments positioned on the earth's surface, in cities, or in the atmosphere. Some of the 5-INTs collection platforms are satellites, aircraft, unmanned aerial vehicles, aerostats, ships, submarines, ground sites, and people (Clark, 2011, pp. 37-56).

Sensors and instruments are IT systems used in the collection of data by intelligence professionals and academic researchers to better understand STE systems and all-hazards, threats, and crises. I have included sensors and instruments (S/I) with the MODES mnemonic to become MODES-S/I because of their extensive use in research and development and the science and technology fields. MODES-S/I and the 5-INTs are two methods to carry out the IM data collection process. They are both data sources and collection methods and they are directly linked to the all-hazards intelligence analyst's analytic approach (e.g., target-centric, activity-based, and risk-informed) and the selected APOE. The type of 5-INT or MODES-S/I method that will be used to collect data is determined by the client's requirements and the analyst's chosen analytic approach and APOE. This statement infers periodic analyst and client negotiation sessions about requirements, approach, and APOE throughout CASA process and its DIKI function convergence.

Intelligence analysis core competency. The third core competency program of HSIE intelligence synthesis is intelligence analysis. Technically, analysis is an IM task like collection and dissemination; however, because of its importance in the meaning-making process, it is considered a stand-alone process equal to KM, IM, and RM. Without the critical reasoning skills of all-hazards analysts—people—there would be no intelligence in the intelligence domain. Although machine-learning and artificial intelligence is a possibility, it has not replaced the deliberate and purposeful systems of humans and critical reasoning.

Intelligence Analysis approaches and methods. Intelligence analysis is inherently a cognitive process within the mind. It is a deliberative process of understanding something (e.g., a system, entity, or phenomenon) and to give it meaning within the context of our environment to solve a problem. Thus, analysis is critical reasoning. Within the interdisciplinary HSIE and IC there is no "baseline standard analytic method (Clark, 2017, p. 6)" for analysts to follow. However, there are many methods and approaches to conducting analysis. For example, the target-centric, activity-based, and risk-informed analytic approaches that were discussed previously; and, narrower structured analytic techniques. Intelligence analysis is many things at once: it is short-term, mid-term, and long-term focused; it is tailored to the tactical, operational, and strategic levels; it decomposes a problem; it looks for relationships and patterns; it studies facts, assertions, presumptions, and assumptions; and it is vulnerable to human fallacy and biases. Most importantly, analysis is critical reasoning with a defined purpose.

Analysis should follow a prescribed process to measure progress, identity information gaps, and for quality assurance (Carter, 2009; Clark, 2017; Eck, Clarke, &

Petrossian, 2018; Pherson & Pherson, 2017). In a time-restricted environment, an established process helps with productivity and timeliness. Also, an agreed upon analytic process is helpful in a multijurisdictional and interdisciplinary setting by providing a common approach for the participants.

Intelligence analysis synthesis discussion. The process of analysis follows four phases that are meant to ensure its quality, applicability, and timeliness. An intelligence product that is of poor quality, not applicable to the problem, and late is irrelevant. The four phases are: (1) reductional analysis, (2) relational analysis, (3) evaluative analysis, and (4) integrative analysis. These phases (RREI) of analysis, that I have derived and summarized from my research, will be discussed in detail along with synthesis in chapter V. Like IM that has a narrower focus than KM, analysis is more narrowly focused than synthesis. Synthesis includes not only the results of all-source analysis, it also includes interdisciplinary perspectives, operational context, the multijurisdictional needs of customers, and the political constraints placed on clients. Analysts who conduct intelligence synthesis in the HSIE should be conscientious of the *all* in all-hazards, all-crimes, all-sources, all-agencies, all-disciplines, and all-jurisdictions.

Risk management core competency. Risk management (i.e. assessing risk probability) is the fourth core competency program of the HSIE's intelligence synthesis. Although quality intelligence assessments do not always require the assessment of risk (e.g., vulnerabilities, likelihood, and consequences) and can be produced as informative products only, the benefits of risk-informed intelligence products for decision-makers in the security domain are numerous. Risk-informed intelligence improves "security strategy, resource allocation, planning, communications and transparency, and thereby confidence" (Newsome B. , 2014, p. 7) in the intelligence product.

Risk management and intelligence synthesis discussion. Analysts who can advise and participate in the decision-making process with the client are better positioned to move beyond the alert and inform tasks. Advising is a more proactive risk-informed management approach that improves the quality of intelligence assessments and anticipatory intelligence assessments. Its noteworthy that risk-informed anticipatory assessments are not predictive because no one can predict the future. Statistical analysis increases the estimates of likelihood and probability of a future scenario's occurrence, but it does not definitively predict that it will occur. Risk assessments and risk management programs are the fourth cornerstone of the HSIE's risk-informed applied intelligence synthesis system.

Core competencies and intelligence synthesis discussion. Thus far, I have described the HSOE and the HSIE as components of the larger homeland security and intelligence domains. I have recognized that the HSOE is comprised of STE systems and ACTN hazards, threats, and crisis events. I have discussed how the HSIE's pluralistic intelligence system provides risk-informed applied intelligence to support the NPG and its five preparedness missions (5PM) of prevent, protect, mitigate, respond, and recover.

Furthermore, I have demonstrated that the HSIE is an intelligence synthesis system of intelligence management structures, processes, functions, and a purpose that are derived from the four core institutional and programmatic competencies of knowledge management (KM), information management (IM), risk management (RM), and intelligence analysis. All of which are essential enablers of the HSIE's practitioners, policy makers, and institutional capacity to build knowledge capital, capacity, and continuity. Next, I will discuss a positive constraint that is placed on HSIE intelligence activities and operational missions by the United States Constitution and legal statutes: privacy, civil rights, and civil liberties compliance.

Privacy, civil rights, and civil liberties compliance in the HSIE. Since its establishment in 2002, DHS and the homeland security domain has dealt with privacy, civil rights, and civil liberties (PCRCL) issues as new federal institution (e.g., the PATRIOT Act of 2001 controversies). However, PCRCL controversies have been the subject of numerous statutory laws, official and unofficial governmental policy, and judicial rulings since the founding of the United States and the Constitution. The PATRIOT Act is one of the modern era PCRCL challenges to the federal government's power and authority over enhanced surveillance capabilities of U.S. and foreign citizens by law enforcement agencies and expanded spy programs by the National Security Agency (NSA) for example (Geary, 2014, pp. 275-278).

The DHS Privacy Office is statutorily mandated to evaluate departmental PCRCL programs, conduct compliance oversight, promote best practices, operate departmental PCRCL incident response, and train departmental personnel on PCRCL laws, policy, and compliance measures (Privacy Overview, 2018). To better understand the importance of PCRCL compliance within the HSIE, the definitions and differences between privacy, civil rights, and civil liberties are needed. Privacy is a person's "interests in preventing the inappropriate collection, use, and release of" personally identifiable information (PII) such as personal characteristics, social security number, address, medical records, or GIS locations (Global Advisory Committee, 2012, p. 40). Privacy rights are derived from judicial rulings rather than explicit declarations within the U.S. Constitution (Carter, 2009, p. 133).

Civil rights are the "obligations imposed on government to promote equality" such as "equal protection under the law and equal opportunity to exercise the privileges of citizenship regardless of race, religion, sex, or other characteristics unrelated to the worth of the individual (Carter, 2009, p. 133) ." Civil liberties, on the other hand, are the unalienable rights of people that are written into and derived from the U.S. Constitution, the Bill of Rights, and its amendments. Civil liberties "offer protection to individuals from improper government action and arbitrary governmental interference" (Carter, 2009, p. 133).

Together, privacy rights, civil rights, and civil liberties are positive constraints placed on HSIE policy makers and practitioners who collect, access, analyze, and share information about U.S. persons (i.e., EO 12333 defined persons as U.S. citizens and permanent resident aliens [Global Advisory Committee, 2012, p. 40]). More specifically, PCRCL must be handled by HSIE personnel, including SLTT Fusion Centers, in accordance with "applicable law, including but not limited to the First, Fourth, Fifth, and Fourteenth Amendments of the Constitution; the Privacy Act of 1974; 28 C.F.R. Part 23; Executive Order (EO) 12333; and the Department's Guidance on the Use of Race in Law Enforcement Activities" (Civil Rights / Civil Liberties Impact Assessment: DHS Support to the National Network of Fusion Centers, 2013, p. 2).

The enforcement of PCRCL compliance within the HSIE does not, nor can it, guarantee the absence of violations. However, the preventive and protective measures are in place to ensure at least minimum legal institutional and individual compliance is conducted in a systemic and deliberate manner. Thus, the HSIE's analytic goal is to provide risk-informed applied intelligence that is PCRCL compliant to homeland security decision-makers (see figure 10). This institutional goal is carried out by the all-hazards analysts that it employs and is illustrated alongside the meaning-making to decision-making to problem-solving continuum as an intelligence synthesis continuum in figure 11.

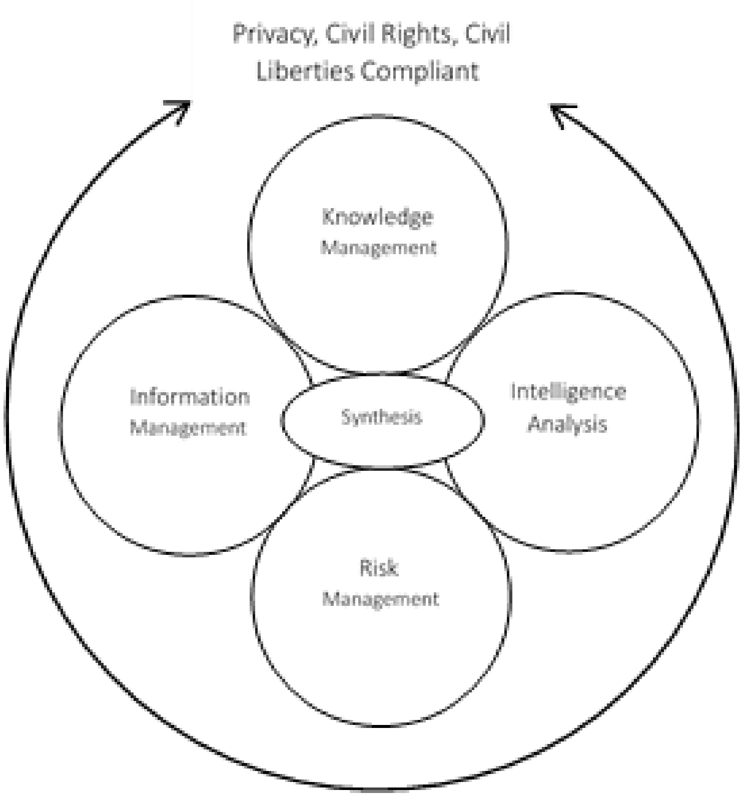

Figure 10. Intelligence Synthesis Core Competencies. The knowledge, information, and risk management programs as well as the intelligence analysis process are the four core competencies of privacy, civil rights, and civil liberties compliant intelligence synthesis within the HSIE. This figure is the result of research synthesis from previously cited sources.

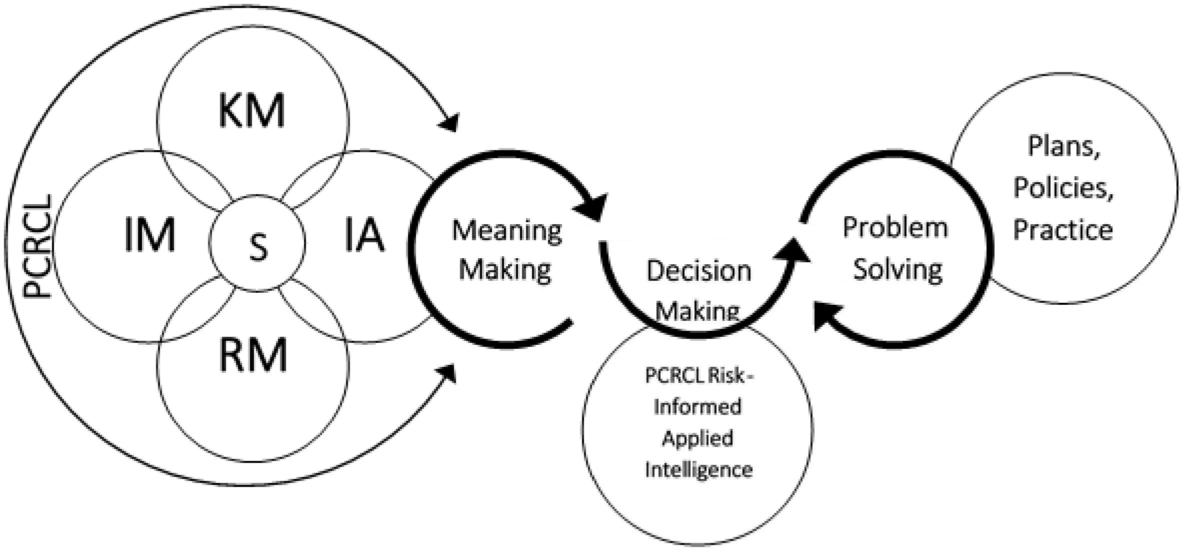
KM
IM
S
IA
RM
PCRCL
Meaning Making
Decision Making
Problem Solving
Plans, Policies, Practice
PCRCL Risk-Informed Applied Intelligence

Figure 11. The Intelligence Synthesis Continuum. The meaning-making to decision-making to problem-solving continuum is supported by privacy, civil rights, and civil liberties (PCRCL) compliant knowledge (KM), information (IM), and risk management (RM) programs as well as the intelligence analysis (IA) and synthesis (S) processes within the HSIE. Decision-making is based upon PCRCL compliant risk-informed applied intelligence and problem-solving is enabled by effective plans, policies, and practical application. This figure is the result of research synthesis from previously cited sources.

Defining The All-Hazards Intelligence Analyst

HSIE intelligence professionals. Analysts, U.S. Office of Personnel Management job series 0132, are grouped in the intelligence series of professional positions concerned with "work in the collection, analysis, evaluation, interpretation, and dissemination (Office of Personnel Management, 2009, p. 26)" of information and intelligence. Within the HSIE, the 0132 series of intelligence professionals perform national and departmental intelligence functions in DHS component intelligence programs (CIP) (Homeland Security Committee, 2016, p. 11). Although not specifically titled as all-hazards intelligence professionals, their all-hazards and all-crimes duties are evident by the missions of the FCs, ISACS, and other CIPs where they are employed in the HSIE.

An all-hazards approach by 0132 series intelligence professionals is further emphasized in the *Crosswalk of Target Capabilities to Core Capabilities* FEMA document. In it, the former Target Capabilities List (TCL), published by DHS in 2007, is compared with updated NPG capabilities that recognize the variety of ACTN threats and the core preparedness responsibilities that includes intelligence and information sharing to provide anticipatory intelligence regarding emerging or imminent threats to the United States, its people, property, or interest through the intelligence cycle (Federal Emergency Management Agency, 2011, pp. 7-8).

To produce all-hazards risk-informed applied intelligence products that are PCRCL compliant, 0132 series intelligence professionals must abide by the institutional policies and programs that establish the foundation of the HSIE's pluralistic intelligence approach. Again, PCRCL compliant KM, IM, and RM programs and intelligence analysis process are the four core competencies of the enterprise's intelligence synthesis system. This means, all-hazards analysts in the HSIE must be proficient in their knowledge about intelligence generation (i.e., DIKI), the intelligence process and reasoning (i.e., CASA and RREI), sharing and communicating intelligence assessments (i.e., SC), and integrating and applying intelligence into the client's requirements or purpose (i.e., 4As and 3Ps). In other words, all-hazards analysts must have content knowledge of *know how* and *know what* (Schleicher, 2018, p. 235)—know how the intelligence process, intelligence generation, and intelligence communication is conducted and know what is in the STE and ACTN subject matter.

Applied knowledge foundations. A person's knowledge content is based on four separate but converging areas adapted from the pedagogical knowledge content model: (a) knowledge of the learning process, (b) knowledge of the subject matter, (c) knowledge of the contexts of the environment, and (d) knowledge of the audience, student, or customer (Whitman & Kelleher, 2016, p. 159). In relation to HSIE all-hazards analysts, this means having knowledge in the CASA intelligence process; knowledge in the STE and ACTN systems; knowledge the HSOE and the operational context; and knowledge about the client, customers, and their requirements. Additionally, two other knowledge content models are useful for understanding the all-hazards analysts' position within the HSIE: the 3i model and the instructional core model to be explained in the next section.

Knowledge of content areas. An analyst's knowledge content areas about the process, subject matter and its context, and the client are illustrated in two other models. First, the 3i model depicts the union of intelligence analysts and their interpretation of the criminal environment; then it depicts the decision-maker's impact on the criminal environment; and lastly, it depicts the influential relationship between the decision-maker and the intelligence analysts (Eck, Clarke, & Petrossian, 2018, p. 19). This triadic knowledge content model of the analyst, the subject matter, and the client adds the relationship types that are typically exercised between participating people and the subject: how the analyst interprets (i.e., understands) the subject matter; how the analyst and client influence each other during the intelligence analysis process (i.e., establish trust) ; and what impact the subject matter and the client have on each other (i.e., intelligence product acceptance). Another similar knowledge content model is the instructional core.

The instructional core model is triadic with a teacher, the student, and the subject matter content. Similarly, this model emphasizes the interactive relationships between them: how well the teacher understands the curriculum and the subject matter content; how well the student understands the subject matter content (i.e., the impact of cognitive engagement); and the teacher's influence on the student's understanding and cognitive engagement. Like the 3i model, the instructional core depicts the two participants and the subject matter as well as their types of relationships (Whitman & Kelleher, 2016, p. 153).

These knowledge content and instructional core models underscore the knowledge creation, intellectual capital, and intelligence generation capacity of the analyst and client relationship with the subject matter. This synergistic relationship is bounded by the four core intelligence synthesis competencies of KM, IM, RM and intelligence analysis. To better illustrate this concept, I have created the applied intelligence core model that shows interactive relationships among the all-hazards analyst, intelligence customer, and STE and ACTN content (see figure 12).

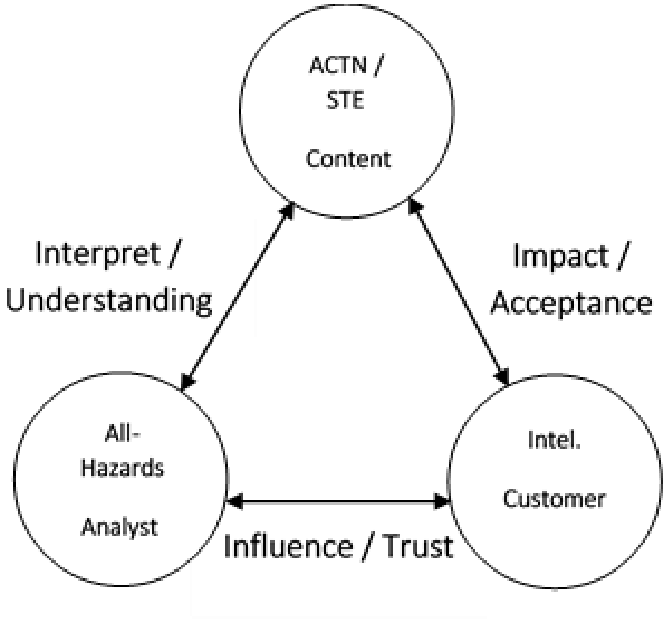

Figure 12. The Applied Intelligence Core Model. The relationships among three knowledge content areas of the subject matter (i.e., content), the analyst, and the customer are depicted in this figure. Analysts must interpret and understand the content to build an influential and trusting relationship with the intelligence customer, so the customer will accept the intelligence product and understand its impact on the decision-making process. This figure is the result of research synthesis from previously cited sources.

Knowledge of core competencies. Analysts have been called "knowledge workers*"* (Lowenthal, 2015, p. 158) because of their intimate involvement with its maturation process from raw data to intelligence. Researcher and author Andreas Schleicher states:

> The more knowledge that technology allows us to search and access, the more important becomes deep understanding and the capacity to make sense out of content. Understanding involves knowledge and information, concepts and ideas, practical skills and intuitions. But fundamentally, it involves bringing them together, integrating and applying them, in ways that are appropriate to the learner's context (World class: how to build a 21st-century school system, 2018, pp. 238-239).

The correlation between this explanation about the essentials of creating and applying knowledge by educators is relevant to intelligence analysts who must use technology to gather and analyze extensive amounts of data and information; synthesize it with context, conceptual frameworks, and customer requirements; and then integrate and apply it into a problem-solving setting.

All-hazards analysts, like educators or business consultants, must know the content of their subject and profession well enough to go beyond just offering an assessment and take time to teach it to their clients—clearly, within the bounds of professional discretion. From this understanding of the HSIE's four institutional core competencies, its pluralistic intelligence context, and the applied intelligence core model, I have identified four core competencies of all-hazards analysts: (a) critical reasoning abilities (i.e., think), (b) knowledge and synthesis capacity (i.e., know), (c) communication skills (i.e., speak), and (d) applied intelligence abilities (i.e., act) that I will discuss next.

Critical reasoning abilities. This is the analysts' ability to combine a deliberate critical reasoning process (e.g., critical thinking steps) with creative *out-of-the-box* thinking. This is the combination of structured and unstructured thinking that is both systematic and unbounded thus allowing elaborative understanding of problems. Elaborative thinking connects new knowledge to familiar knowledge so analysts can think divergently and creatively about the problem and its solutions (Schleicher, 2018, p. 232). An analyst's critical reasoning abilities are simply stated as *think* and represents their ability to interpret the subject matter content.

Knowledge and synthesis capacity. This is the analysts' capacity to integrate technology (e.g., sensors, instruments, and software applications) into the critical reasoning process to synthesize large amounts of data and information from multiple sources, disciplines, and jurisdictional perspectives. Although all-hazards analysts cannot be a subject matter experts (SME) in all scientific disciplines, they must be able to comprehend the relevant baseline data points, recognize relationships, reveal patterns, and organize it into useful information that will become relevant knowledge and applied intelligence. This is the synthesis process and it is stated as *know*; it represents the analysts' capacity to understand the subject matter content.

Communication skills. An analyst must have effective written and oral communication skills to convey the results of their work to their clients. An organized process and format for presenting intelligence alerts, assessments, and advice that is based on clearly stated facts, claims, presumptions, and assumptions, is structured communication. Structured communication is stated as *speak* and it represents the analysts' ability to positively influence the client's trust in their analytic ability and acceptance of the intelligence product.

Applied intelligence ability. Finally, an analyst must know how to apply their knowledge and intelligence products in a productive manner. Recall, analysts assert the 4As of alert, assess, anticipate, or advise to inform decision-makers. The applied intelligence ability of analysts is referred to as *act* and it represents their ability to influence clients and customers during planning, policy formulation, and practical application (3Ps) of their intelligence products. It is noteworthy at this point of the analysis discussion to point out that actionable intelligence and applied intelligence differ slightly. Actionable intelligence implies that decision-makers and practitioners will use the intelligence to act quickly, or in the near-term, in an operational context. Applied intelligence implies that they will use it for other purposes such as operational or emergency planning and policy formulation.

All-hazards analysts' core competencies synthesis. The four competencies of an all-hazards analyst that are derived from the institutional core competencies and pluralistic intelligence frameworks, are used to form the foundation of the AH-ISM and are illustrated in figure 13. The applied intelligence core model of the analyst, customer, and content relationships is indirectly evident in the structure of the baseline ISM. Moreover, the DIKI maturation of raw data into intelligence is evident in the left to right flow of knowledge generation function and ending with the applied intelligence purpose.

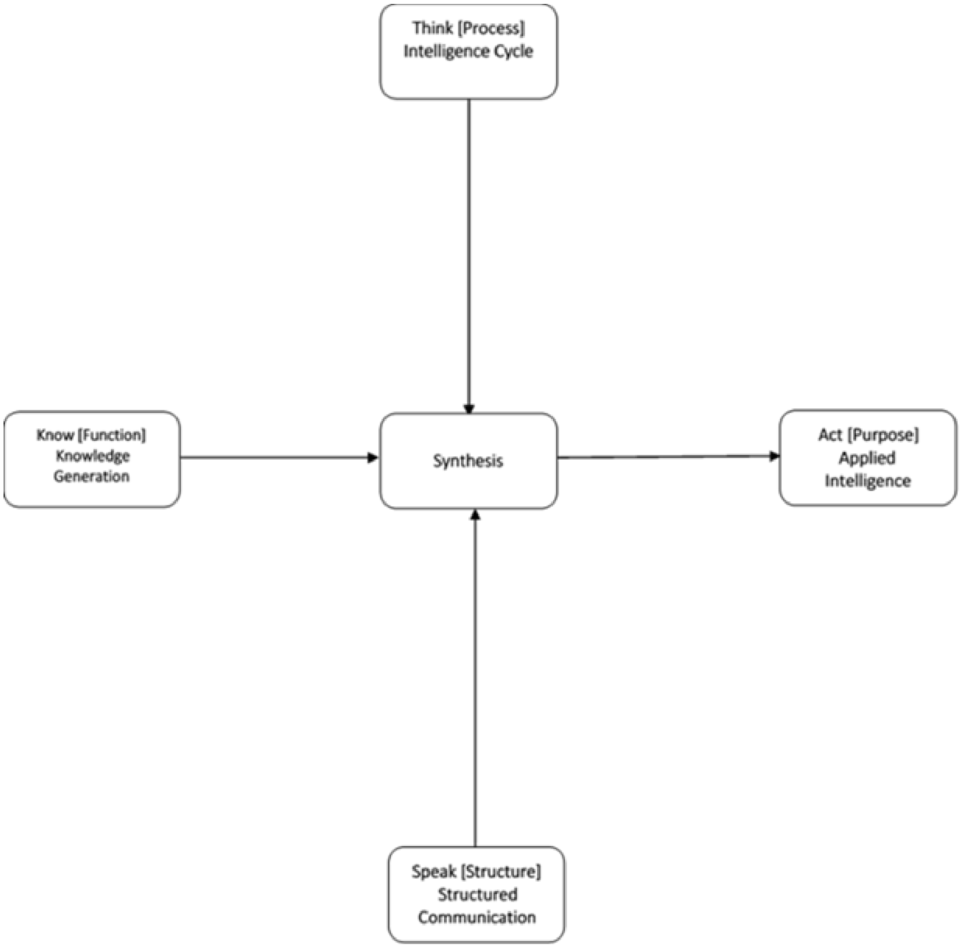

Figure 13. The Baseline Intelligence Synthesis Model (ISM). This model represents the intelligence synthesis capacity created from a systems component model (e.g., process, function, structure, and purpose) that is aligned with the four core competencies of an analyst (e.g., think, know, speak, and act). In this model, the critical reasoning process and intelligence cycle, the knowledge generation function, and the structured communication skills are inputs into the synthesis process that produces applied (i.e., actionable) intelligence. This baseline model is the conceptual foundation of the All-Hazards Intelligence Synthesis Model (AH-ISM). This figure is the result of research synthesis from previously cited sources.

Professional development. The all-hazards analysts' core competencies are education based meaning they can be taught so they are within the institutional purview of professional development. Analysts, like any other practitioner in other career fields, enhance their content knowledge through a professional development process consisting of the three domains of learning: (a) institutional education, (b) operational "on-the-job" training, and (c) experience-based self-development (Department of the Army, 2012, pp. 1-2). An HSIE analyst's minimum required academic education is at the secondary education level, with additional operational or research experience if possible, and preferably have a four-year degree from a higher-level education institution (The Global Advisory Committee, 2015, p. 4).

Additional education, training, and self-development are acquired through HSIE intuitional programs like the network of Federal Law Enforcement Training Centers (Federal Law Enforcement Training Centers, 2018) and FEMA Emergency Management Institute online training courses (Federal Emergency Management Agency, 2018). Altogether, these formal and informal training resources, even though they include interdisciplinary, interagency, and multijurisdictional topics, are primarily law enforcement-centric and lack a true all-hazards approach to analysis training (Global Justice Information Sharing Initiative, 2007, 2010; The Global Advisory Committee, 2015).

Intelligence analysts' mindset. The combination of intuition, formal and informal education, training, and experiences congeal as the analysts' mindset. A mindset is like a world view because it forms the conceptual framework of how an analyst approaches and frames an analytical problem. The think-know-speak-act applied intelligence mindset, is an elaborative analytic embarkation point for the all-hazards analyst. It helps them to establish the analysis approach to the subject-matter, the initial APOE, and operational boundaries within spatial, temporal, and contextual parameters. Additionally, it helps them establish rapport with their client and earn their trust. The HSIE all-hazards analyst must be proficient in the institutional core competencies of KM, IM, RM, intelligence analysis; PCRCL compliance; and, their professional competencies of critical reasoning, communication, and intelligence synthesis and application (see figure 14). Thus, the think-know-speak-act mindset serves as a good start point for any analyst. The ISM model completes the analysis phase of my thesis and it will be the start point for chapter V's discussion on building the AH-ISM.

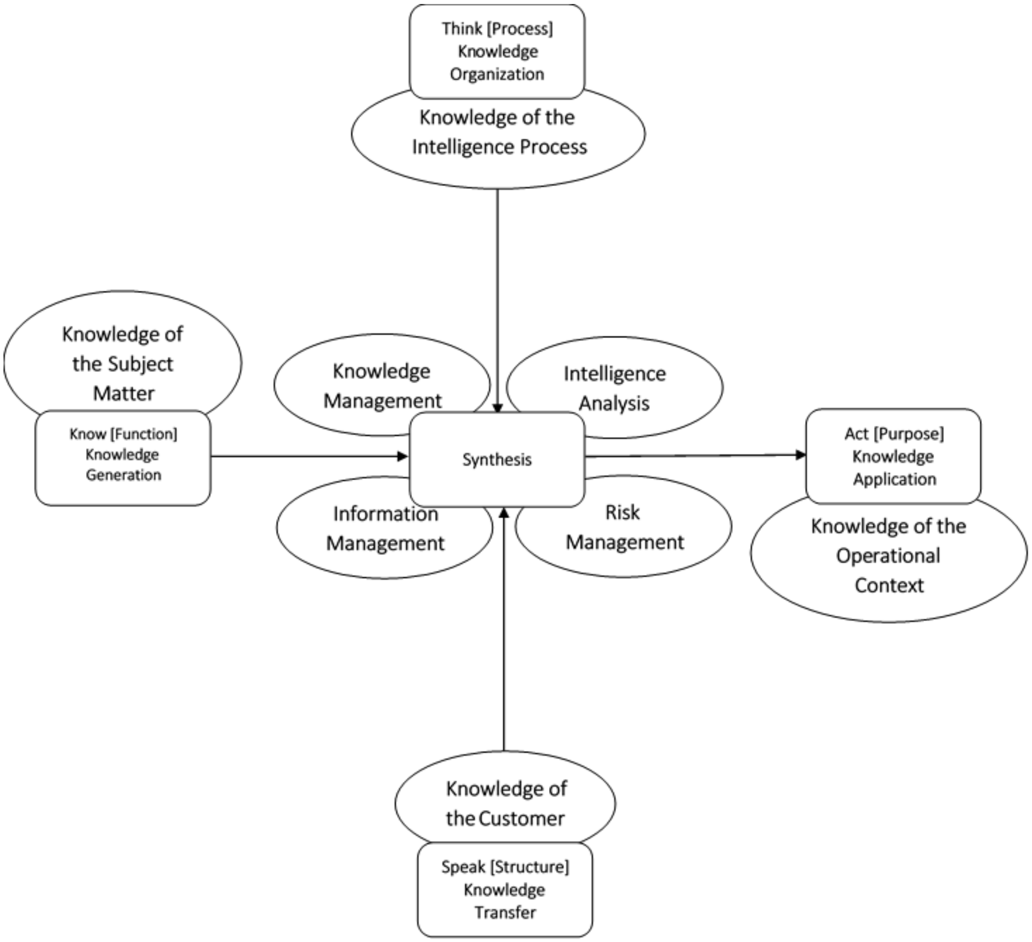

Figure 14. The Baseline Intelligence Synthesis Model (ISM) including Knowledge Content Areas and Knowledge Management Tasks. The merging of the institutional core competencies (e.g., KM, IM, RM, and intelligence analysis), the knowledge content areas (e.g., knowledge of process, subject matter, the customer, and context) and the analysts' professional competencies (i.e., think-know-speak-act) are illustrated in this figure of the baseline intelligence synthesis model. This model represents the systemic production of risk-informed applied intelligence that is privacy, civil rights, and civil liberties compliant. This figure is the result of research synthesis from previously cited sources.

In conclusion, my analysis of the United States' homeland security and intelligence domains offered a reductional analysis of the homeland security operational environment (HSOE) and the homeland security intelligence enterprise (HSIE) to identify their essential systems components and entities. Then, by a relational analysis and an interdisciplinary approach, I presented the transrelational similarities among several all-hazards disciplines within the HSIE. Lastly, I integrated these interdisciplinary findings into the HSIE, as well as the HSOE, and created a baseline ISM to illustrate the institutional and professional core competencies of IC and HSIE intelligence analysts. Although not specifically addressed in this chapter, I evaluated the relevance and usefulness of my analytic efforts throughout my analysis phase of research thus utilizing the RREI method (e.g., reduce, relate, evaluate, integrate). My evaluative analysis will be discussed at the end of chapter V by using the CORE reflexivity method.

The ISM is the starting point for the creation of an all-hazards version of the model to help analysts understand the processes, functions, structures, and purpose for generating all-hazards risk-informed applied intelligence that is privacy, civil rights, and civil liberties compliant. In chapter V, I will build upon the baseline ISM to create the AH-ISM for use by HSIE practitioners in support of the National Preparedness Goal. Furthermore, I will present interdisciplinary examples of the AH-ISM to illustrate its applicability in a multidisciplinary, multiagency, and multijurisdictional intelligence and operating environment.

CHAPTER V

Discussion

My research findings are depicted in two conceptual models about common intelligence synthesis core competencies that are unique to the HSIE, the intelligence synthesis model (ISM) and the all-hazards intelligence synthesis model (AH-ISM). Both models are systems-based and constructed from institutional and professional core competency traits of the intelligence and analysis career fields. The ISM's systems components of process, function, structure, and purpose are based on the integration of the intelligence analysis process, the knowledge management (KM), information management (IM), and risk management (RM) institutional programs and the critical reasoning, knowledge synthesis, communication, and applied intelligence professional competencies of intelligence analysts. Also, the U.S. Constitutional guarantee of privacy, civil rights, and civil liberties (PCRCL) compliance is integrated into the baseline ISM and the AH-ISM. The shorthand memory aid for the analysts' professional competencies that form the visual structure of both models is think-know-speak-act.

The systems components of the ISM are formed by (a) the CASA intelligence process (e.g., collect, analyze, synthesize, and apply); (b) the DIKI knowledge generation function (e.g., data, information, knowledge, intelligence); (c) CEWB structured communication (e.g., claim, evidence, warrant, backing) to be discussed in this chapter; and, (d) the 3Ps and 5PM applied intelligence purposes (e.g., policy, plans, practice; prevent, protect, mitigate, respond, recover). The ISM is the baseline model for producing risk-informed applied intelligence that is privacy, civil rights, and civil liberties compliant for intelligence clients, customers, and consumers. Moreover, it is the conceptual framework for meaning-making in support of the decision-making process and problem-solving results.

In this chapter, I will discuss the AH-ISM and give examples of its transdisciplinary application within the HSIE. By adding the HARTE crisis event continuum alongside the DIKI knowledge generation continuum, the ISM acquires an all-hazards functional focus. The combined system components of the DIKI and HARTE functions represents the infusion of all-source, all-crimes, all-agencies, all-jurisdictions, and all-disciplinary information to generate intelligence products for all-hazards intelligence clients. This description presents all-hazards synthesis as a robust systemic process as well as an analytical mindset. Thus, the AH-ISM is an all-hazards model with applications in emergency management, critical infrastructure protection, systems safety engineering, and any other homeland security component intelligence program (CIP) that relies upon risk-informed applied intelligence products for operational safety and security success.

The All-Hazards Intelligence Synthesis Model

The all-hazards HSOE is an intelligence challenge for HSIE analysts. This pluralistic operational environment is full of all types of ACTN hazard sources and active threats to numerous STE systems like neighborhoods, public infrastructure, and private businesses requires a pluralistic analytical mindset to comprehend. However, the HSIE's intelligence analysis training standards for its 0132 series analysts are primarily based on crime analysis standards (Department of Justice, 2007, 2008, 2012). To improve this institutional training deficit, a common all-hazards analytical framework is needed. Such a universal intelligence analysis and synthesis model would offer a shared touchstone for the HSIE's community-of-practice in their coordination and collaborative efforts at fusion centers, ISACs, and FSLTT operational centers across the nation. The AH-ISM would help unify intelligence analysts who work in and with law-enforcement agencies, incident commands, emergency management, risk management, the natural sciences, health sciences, and systems safety engineering disciplines.

The AH-ISM is a systems-based model, so it is inherently transdisciplinary and applicable in all disciplines that contribute to or conduct ACTN and STE intelligence synthesis and research. It's graphic representation of intelligence synthesis makes it an appealing interdisciplinary model that is easily shared and referenced by analysts. Referring to figure 13 once again, the model visually depicts its functional system component as a combined DIKI and HARTE continuum moving towards the applied intelligence purpose from left to right corresponding with the think-knowledge generation to act-knowledge application competencies (flowing through the synthesis center point). It depicts the process system component of the CASA continuum connecting into the DIKI and HARTE continuum (at the synthesis center point) flowing from the top corresponding with the think-knowledge organization competencies. The AH-ISM depicts the structure system component and the CEWB structured communication continuum connecting into the DIKI and HARTE continuum (at the synthesis center point) flowing from the bottom corresponding with the speak-knowledge transfer competencies shown.

The informational flow of the ISM and AH-ISM is through and towards the intelligence synthesis transformational function and then on to its applied intelligence purpose. The model's structure creates a visual and functional quad-chart with four counterclockwise-following areas beginning in the upper-left, to lower-left, to lower-right, and to the upper-right. The functional significance of these four zones are represented by the four RREI analysis activities of reduce, relate, evaluate, and integrate respectively. These four RREI analysis phases are subphases of the analysis step in the CASA process. The AH-ISM is depicted in figure 14 which is presented after the following discussion about the think-CASA and RREI processes.

The *think* all-hazards intelligence synthesis processes. The *think* process of the AH-ISM is built upon research, discovery, and problem-solving methods such as the intelligence cycle, the scientific research method, critical-thinking strategies, and business analysis methods (Pherson & Pherson, 2017, p. 48). The *think* process is an organized method of gathering, analyzing, assessing, evaluating, and integrating data, information, and intelligence into a final intelligence assessment or anticipatory estimate product. For example, critical-reasoning strategies, like the medical field's clinical-reasoning process (Stern, Cifu, & Altkorn, 2015), begins with questions and ends with drawing conclusions and presenting findings. Similarly, the scientific method begins with defining the problem and ends with presenting conclusions (Pherson & Pherson, 2017, p. 48). And, the intelligence cycle that is used by the IC, DOD, and law enforcement, has up to six steps: (a) planning, (b) requirements, (c) collection, (d) processing and exploitation, (e) analysis, and (f) dissemination (Lowenthal, 2015).

For conceptual simplicity, I will use a generic and easy to remember four-step intelligence process in the AH-ISM: (a) collect, (b) analyze, (c) synthesize, and (d) apply (CASA). Each step of the CASA intelligence process has substeps that will be explained in the following sections. Discernibly, CASA is the general intelligence process and

RREI is the narrower analysis process and both flow into the central intelligence synthesis function along with the DIKI and HARTE functions and CEWB structured communication.

Collect: gathering all-hazards data and information. The first phase of the AH-ISM's CASA knowledge organization and intelligence process is the collection of raw data, information, knowledge, and available intelligence products for the follow-on intelligence analysis phase. Previously, I discussed how the analytic approach (AA) and APOE influences the intelligence synthesis process by determining the targets, activities, and assets to be researched and analyzed. Analysts and clients determine if analysis will focus on a specific known threat targets (i.e., target-centric analysis), the activities of unknown targets (i.e., activity-based analysis), or specific STE assets and their vulnerabilities (i.e., risk-informed analysis). Furthermore, the AA helps determine the APOE selection like a geographic zone, an entity, a whole system, or one of its system components (e.g., a process, infrastructure, or functional components).

The AA and APOE influence the collection process as much as the client's requirements and the types of systems data to be collected. Also, the three systems characteristics of identifiable, detectable, and measurable (IDM) determine the collection sources, methods, and sensor types. Recall, identifiable characteristics are generally descriptive and can be positional. This means an entity's identity can be determined as well as its location. Detectable characteristics are the identifying characteristics (i.e., signatures) that are emitted, reflected, or otherwise discoverable by people and the 5INTs technical collection sensors. Likewise, detection means spatiotemporal characteristics of an entity are discoverable. Measurable characteristics are the signatures that reveal an entities identifying characteristics shape, size, color, chemical composition, or any other characteristic that an instrument can qualify or quantify for analysis. Discovery of IDM is accomplished by the 5INTs as well as MODES-S/I as discussed in chapter IV. Thus, collection, in the AH-ISM's CASA process, is influenced by the client's requirements, IDM, AA, and APOE; and, it is accomplished by the 5INTs and MODES-S/I sources and means.

Analyze: understanding all-hazards and the meaning-making process. Analysis is the second phase of the AH-ISM's CASA knowledge organization and intelligence process. Analysis is the central process of the all-hazards and all-source intelligence synthesis system. It encompasses the reduction of collected data, information, knowledge, and prior intelligence into relevant baseline data points, discovering their relationships, evaluating their veracity, and integrating them into a finished intelligence product. Indeed, analysis is the heart of the HARTE all-hazards intelligence synthesis process. The AH-ISM's RREI analysis process steps are: (1) reduce, (2) relate, (3) evaluate, and (4) integrate.

Reduce: the reductional analysis quadrant. Reduce is the first step of the analysis phase and it is primarily concerned with categorizing and coding the collected data. It is conceptually and functionally placed in the upper left-hand quadrant of the model between the CASA intelligence process and the DIKI function. This location indicates that reductional analysis begins when raw data is collected and then transferred to analysts, so it may be broken down into its constituent systems, system components, or basic entities (i.e., baseline data points) before it enters the DIKI function. After raw data is processed in the relate step, it is ready to move into the DIKI function and the next step of relational analysis.

Reductional analysis of collected ACTN and STE datum is conducted in this quadrant to identify basic attributes, characteristics, variables, and any other pertinent entity components. This is done, for example, by entity analysis, coding, and categorizing of specific hazard sources, activators, preliminary relationships, active threats, crisis phenomenon, and STE assets. Although the analytic approach (e.g., target-centric, activity-based, or risk-informed) and the APOE will have an influence, the reductional analysis primary targets are ACTN hazards and threats, the 6Is activators, and the S3E / PIE STE systems or assets.

Relate: the relational analysis quadrant. Relate is the second step of the analysis phase and it is concerned with connecting and combining the reduced baseline data points. It is conceptually and functionally placed in the lower left-hand quadrant of the model between the DIKI and HARTE function and CEWB structured communication. This location indicates that relational analysis begins when baseline data points are linked together to discover links, nodes, networks, and the types of relationships among them. At this point, relational analysis starts the transformational process of raw data into useful information and establishing an evidentiary base for structured communication.

Relational analysis of ACTN and STE baseline data points is conducted in this quadrant to discover sequences, patterns, relationships, anomalies, and meanings among dormant hazards, active threats, and crisis events as well as STE systems components. Preliminary content, comparative, spatial, temporal, and association analysis are some of the analytic methodologies done in this step before useful information becomes content knowledge about the subject matter. Moreover, at the end of the relational analysis step, evidence and preliminary claims are established and included in structured communication formats. The relational analysis primary targets are ACTN hazards and threats, the 6Is activators, ATN relationships (e.g., activities, transactions, and networks) and the S3E / PIE STE systems or assets.

Evaluate; the evaluative analysis quadrant. Evaluate is the third step of the analysis phase and it is concerned with refining useful information and acquired knowledge into a structured intelligence product. Evaluative analysis collates the refined information so its cumulative intelligence value (CIV), to be explained later, is substantiated as verifiable content knowledge to be integrated into the client's intelligence assessment. It is conceptually and functionally placed in the lower right-hand quadrant of the model between CEWB structured communication and the final stages of DIKI and HARTE knowledge content's maturation into applied intelligence. Evaluate is the meaning-making confirmation step of RREI.

During the evaluative analysis step, the intelligence product is tailored for the client based on the analyst's understanding of the client's requirements as well as evaluation of its claims, evidence, supporting facts, presumptions, and assumptions. This is the phase of the RREI process when analysts reassess their professional competencies of think, know, and speak before they *act* by integrating their content knowledge into intelligence alerts, assessments, anticipatory estimates, and offering advice to decision-makers. Evaluative analysis of intelligence is conducted in this quadrant to objectively scrutinize the relevance of patterns, themes, anomalies, concepts, and context about

ACTN hazards and threats, STE systems, as well as the client's intelligence product needs.

Integrate: the integrative analysis quadrant. Integrate is the fourth step of the analysis phase and it is concerned with the final production of intelligence products that are tailored to the client's requirements. Integrative analysis, as the term indicates, integrates content knowledge of the subject matter and the customer into a product that is fit for issuing alerts (i.e., early warning) and actionable intelligence, providing intelligence assessments (i.e., situational awareness), offering anticipatory intelligence estimates (i.e., risk-informed future scenarios), and decision-making advice if requested by the client. It is conceptually and functionally placed in the upper right-hand quadrant of the model between DIKI and HARTE intelligence generation and the CASA intelligence process indicating the cyclic nature of intelligence analysis. Client and customer feedback, after-action reviews, and the need to build upon previous knowledge means CASA and RREI are recurring process.

The integrative analysis step is an interdisciplinary collaborative effort to ensure the intelligence product meets the all-hazards needs of the HSIE client who is charged with supporting or carrying out the 5PMs of the NPG (e.g., prevent, protect, mitigate, respond, and recover). During integration, HSIE analysts and clients must consider the influence and impact of the 5PMs and the 3Ps (e.g., planning, policies, and practice) on the CIV of the intelligence product. By the way, the integrate step is the last opportunity for analysts to mitigate any unrealistic or unobtainable high expectations of their clients who may not understand the capabilities and limits of technical intelligence collection systems or the overall intelligence process. The integrative analysis primary targets are the 5PMs, the 3Ps, and the client's requirements. Figure 15 depicts the RREI analysis process integrated with the AH-ISM.

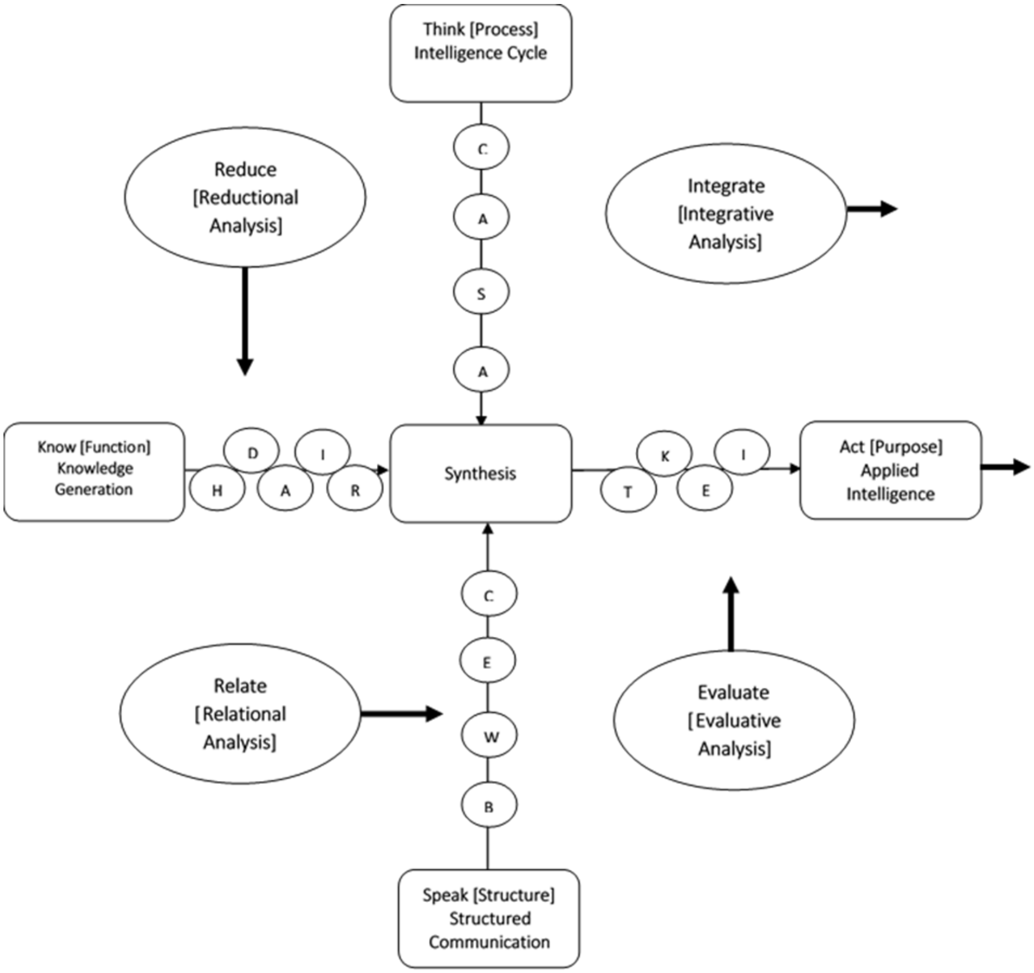

Figure 15. The All-Hazards Intelligence Synthesis Model Including the RREI Analytic Process. The AH-ISM combines the DIKI and HARTE continuums to show the parallel transformative processes of knowledge generation and crisis events. Both continuums converge in the intelligence synthesis process as well as the applied intelligence purpose of the HSIE. The RREI analysis process flow is depicted in the four quadrants of the AH-ISM beginning with (a) the collection of raw data from the CASA process (i.e., intelligence cycle), (b) through the data to information function (i.e., knowledge generation), (c) into structured communication as knowledge, then (d) through the knowledge to intelligence purpose (i.e., applied intelligence). The applied intelligence purpose continues along the continuum from the AH-ISM's meaning-making purpose on to decision-making and problem solving. Although not fully depicted in this figure but indicated by the right pointing arrows, applied intelligence products also follow a similar time continuum from alerts to actionable intelligence to situational awareness assessments to anticipatory estimates of future scenarios. This figure is the result of research synthesis from previously cited sources.

Synthesize: interdisciplinary and multijurisdictional all-hazards intelligence integration. Synthesis is the third phase of the AH-ISM's CASA knowledge organization and intelligence process. Considering the RREI analysis phase is the heart of the intelligence synthesis process and it is focused on the production of the integrated and tailored intelligence product for the client, synthesis should be considered in a broader multidisciplinary, multiagency, and multijurisdictional context. Although RREI is an all-source all-discipline analytic process, synthesis considers the AH-ISM's multiplicity in the context of its communities-of-practice and interest. Synthesis evaluates and integrates the variety of products, participants, and perspectives of the HSIE, HSOE, and IC. Another perspective of synthesis is to consider the RREI analysis process as the means for generating intelligence capital, or hard-currency intelligence products, within the AH-ISM; and, synthesis is the means for generating intelligence capacity from the AH-ISM. Along these lines, synthesis is an investment by and into the intelligence community-of-practice.

Generating intelligence capital. Intelligence capital is the cumulative intelligence value (CIV) currency of the AH-ISM's applied intelligence products. Following the applied intelligence core model of figure 11, the CIV of an intelligence product is its estimated low or high value to the client based on three criteria: (a) analyst-content understanding and interpretation, (b) analyst-customer influence and trust, and (c) customer-content impact and acceptance. As depicted in figure 16, high level estimates of these three criteria push the intelligence products CIV to a higher level. Clearly, a high CIV is a vote of confidence in the analyst's ability to generate intelligence capital.

The more intelligence capital within the HSIE, the more intelligence capacity it will acquire.

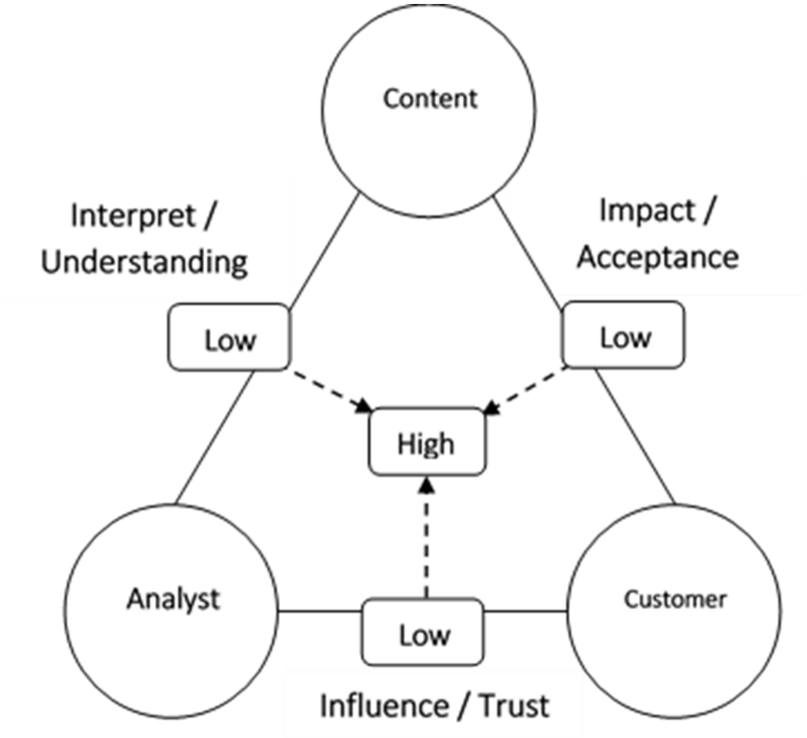

Figure 16. Building Intelligence Synthesis Capital: The Cumulative Intelligence Value (CIV) Estimate. A high level CIV is like the hard-currency intelligence products of the HSIE. The better an analyst interprets and understands the content, the more likely a customer will accept the product and its impact on the decision-making process. Likewise, the analyst's influence will increase as well as the customer's trust level. Altogether, this is the intelligence capital and CIV of the AH-ISM. This figure is the result of research synthesis from previously cited sources.

Generating intelligence capacity. Intelligence capacity is primarily tacit and elicit knowledge resource-centric whereas intelligence capital and the CIV are product driven. Like the National Preparedness System that creates preparedness capacity for the nation, the AH-ISM's synthesis process, centrally located in the model, generates intelligence synthesis capacity for the HSIE. The input sources of intelligence synthesis are clearly depicted in the ISM and AH-ISM as institutional and professional core competencies (see figure 13). Additionally, the RREI analysis process inputs intelligence capital to the multidisciplinary, multisource, multiagency, multijurisdictional, and multiechelon synthesis resources. Intelligence synthesis capacity value (ISCV) estimation is closely related to the evaluate step of the RREI process; however, it is more broadly focused beyond the intelligence product and on the overall intelligence system's capacity to meet the needs of the homeland security and intelligence domains.

ISCV estimation is closely related to the evaluate step of the RREI process; however, it is more broadly focused beyond the intelligence product and on the overall intelligence system. Inputs from PCRCL policies and law, FSLTT agencies at fusion centers, private critical infrastructure intelligence from ISACs, and a host of other IC and DHS CIPs are examples of the many public and private jurisdictions, governmental echelons, disciplines, and sources of intelligence. This is both the input and outputs of synthesis that are depicted in the AH-ISM. Like the CIV, ISCV estimates of low to high value are desired to attain the highest possible confidence levels of intelligence synthesis capacity. Figure 17 illustrates the ISCV inputs from the RREI steps into the intelligence synthesis capacity of the AH-ISM. Accordingly, synthesis is the product of CIV and ISCV estimates.

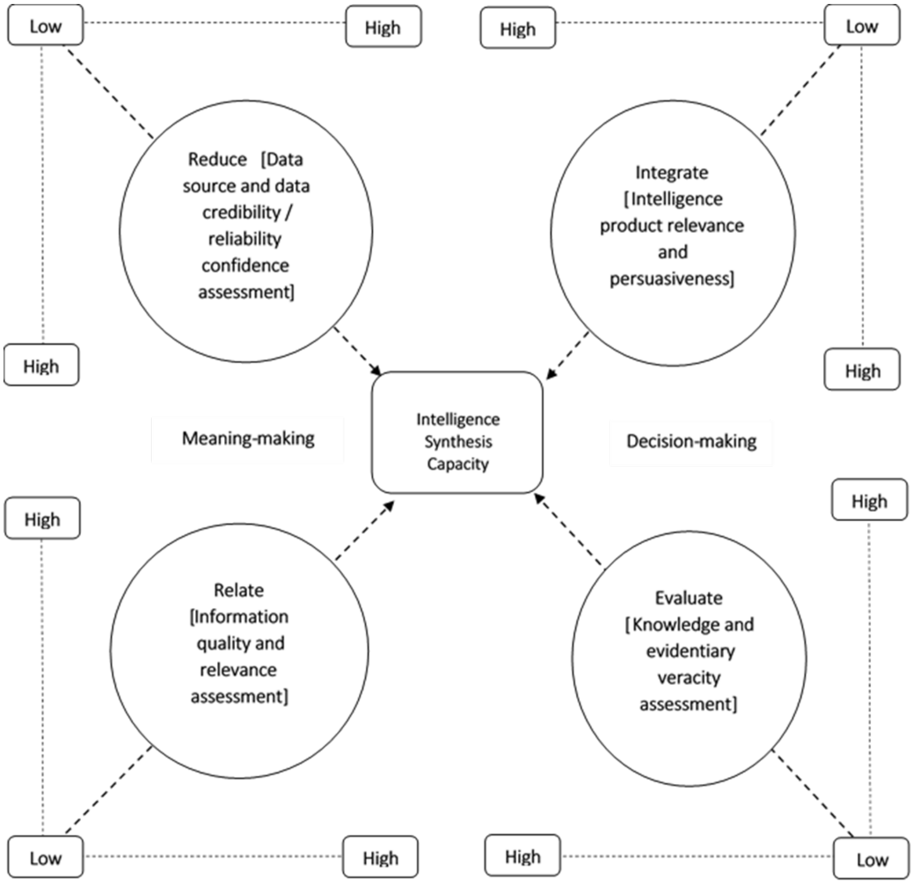
Low
High
High
Low
Reduce [Data source and data credibility / reliability confidence assessment]
Integrate [Intelligence product relevance and persuasiveness]
High
High
Meaning-making
Intelligence Synthesis Capacity
Decision-making
High
High
Relate [Information quality and relevance assessment]
Evaluate [Knowledge and evidentiary veracity assessment]
Low
High
High
Low

Figure 17. Building Intelligence Synthesis Capacity: The RREI Analysis Inputs. Analysts and customers can estimate the overall intelligence synthesis capacity value (ISCV) by estimating the value levels of the RREI analysis inputs as well as the process, function, structure, and purpose system components of the AH-ISM. Importantly, privacy, civil rights, and civil liberties considerations are included in the synthesis process. This figure depicts the ISCV of the AH-ISM from the RREI values ranging from low to high: (1) estimate the data and data sources credibility, reliability from reductional analysis; (2) estimate the information quality and relevance from relational analysis; (3) estimate the knowledge and evidentiary veracity from estimative analysis; (4) estimate the intelligence product relevance and persuasiveness from integrative analysis. The CIV and ISCV are closely related; however, the CIV is generally RREI product-centric whereas the ISCV is AH-ISM capacity-centric. This figure is the result of research synthesis from previously cited sources.

Apply: integration of risk-informed applied intelligence into the decision-making process. Apply is the fourth and last phase of the AH-ISM's CASA knowledge organization and intelligence process. After collection, analysis, and synthesis resulting in a finished intelligence product with a CIV that satisfies the client's requirements as well as an ISCV that contributes to the HSIE's communities-of-practice and interest, all-hazards analysts must take the next step of applying their knowledge and integrating the intelligence product into the decision-making process. This final step is dependent upon the quality of work that was gained by applying their professional competencies alongside the institutional competencies. To effectively alert, assess, anticipate, and advise (4As) HSIE clients, customers, and consumers, all-hazards analysts must fully utilize their knowledge of the intelligence process, the subject matter, the customer, and the operational context (i.e., think-know-speak-act). Additionally, they must combine knowledge management, information management, risk management, intelligence analysis principles, and PCRCL compliance into the apply phase of the AH-ISM.

The *know* all-hazards intelligence synthesis functions. The know function of the AH-ISM is grounded in the maturation of raw data into refined intelligence. Although this is not a truly linear process with a well-defined beginning and end, it is more easily depicted as such in the left to right function to purpose arrow as seen in figure 14. It is a continuum that begins with the collection of raw data, useable information, previously generated knowledge, and published intelligence products and continues to be refined and updated as new data and information is acquired. Knowing is continuous and analysts are knowledge workers—this is a fundamental concept of the AH-ISM that applies to the parallel HARTE crises event continuum based in the transformation of dormant hazards into realized crisis events.

The dual flow of DIKI and HARTE is fed by the CASA processes and throughout the RREI analysis process. This knowledge generation function ultimately produces synthesized all-hazards intelligence products that are integrated into a homeland security operational plan, an institutional policy, or a departmental mission directive in support of the NPG. Notably, the DIKI and HARTE function also supports the body of knowledge of practitioners and academic researchers.

The HARTE model's hazard to threat transformation. The AH-ISM's functional continuum depicts the infusion of data and information into the hazard transformation process. The basic concept of this transformational continuum begins with a dormant hazard source that interacts with an activator to become an active threat. Then, the active threat is directed towards a STE asset thereby threatening its potentially exposed and unsecured vulnerabilities. This interaction between and active ACTN threat and a STE system develops into a realized crisis event such as an incident, disaster, or catastrophe when its exposed and unsecured vulnerabilities are overwhelmed.

The HARTE model's activators and relationships. This HARTE transformational flow is more simply stated as hazard to threat to crisis event. However, it also consists of interactive activators and the relationships among the ACTN and STE system's components and entities. Although they are not specifically addressed in a single citable publication, I have tentatively placed activators and initiating mechanism into six types (the 6Is) that I will use for simplicity in my research discussion: (a) initiators, (b) influencers, (c) instigators, (d) inciters, (e) ignitors, or (f) inhibitors. Certainly, relationships are central to the HARTE all-hazards crisis event model because they determine how hazard sources interact with activators and how threats interact with STE systems. This crisis generation process is aligned with the state change process and flow theory which applies not only to natural energy process but also to the flow of ideas and ideology.

Relationships among systems and entities can be placed into three general categories based on their associations through (a) activities, (b) transactions, and (c) networks (ATN) (Antony, 2016, pp. 17-42; Biltgen & Ryan, 2016, pp. 55-67). Physical and non-physical things (i.e., entities), can be associated or related together by what they do. For example, motorcycles are modes of transportation as well as planes, trains, and automobiles and what they do, their functional purpose, is transport people. This type of activity association also contributes to their utility as proxies for people. This means if a vehicle (i.e., a proxy entity) can be located, then its associated owner, operator, or passenger (i.e., the target entity) also can be located.

Transactional associations or relationships means something is given or received between two entities like money, sustenance, data, or information. Although the activities of the entities may not be the same or even remotely similar, they still can be linked by a transaction. For example, a legitimate bank can be linked to an organized crime syndicate by a financial transaction. Networks also may link entities together through online social media networks or virtual communities. Another example is natural trophic levels that are essentially nourishment networks (i.e., ecosystems) consisting of different types of animals, plants, and people that are directly and indirectly related. The association of entities by ATN relationships is a way of considering how the HARTE crisis event continuum functions.

The HARTE model's crisis events. The National Response Framework (NRF) and the National Incident Management System (NIMS) discuss the incident command system (ICS) and the Stafford Act Emergency or Major Disaster Declaration (Department of Homeland Security, 2013, 2016, p. 28). Within these publications the types and levels of disasters are discussed and range from small in scale and scope single incidents to emergency declarations to disaster declarations to large scale catastrophes. For the purposes of simplicity in my research discussions, I will refer to the typed of crisis events as incidents and emergencies, disasters, and catastrophes as IDC. This acronym will represent the scale and scope of incidents that require implementation of ICS under the NIMS as well as Stafford Act disaster declarations and large-scale catastrophes across multiple jurisdictions or regions.

To summarize the *know* all-hazards intelligence synthesis functions, consider the mnemonics and acronyms that I have introduced thus far. Hazard sources and threats are adversarial, cyber, technological, natural (ACTN) and affect social, technological, and environmental (STE) systems such as populations, infrastructure and institutions, the economy and environment (PIE) or, said in another way, social, engineered, economic, and environmental (S3E) systems. ACTN hazard sources are generally activated by initiators, influencers, instigators, inciters, ignitors, or inhibitors (6Is). Relationships among ACTN, STE, and the 6Is are either activity-based, transactional, or through shared networks (ATN). And, lastly, realized crisis events resulting from the interactions among dormant hazards, activators, relationships, and active threats are either incidents, disasters, or catastrophes (IDC).

The all-hazard crisis event predicate model establishes that ACTN threats, STE targets, and their potentially exposed and unsecured vulnerabilities converge in a time and location nexus. Like the interdisciplinary event triad depicting handlers of offenders (i.e., threats), guardians of victims (i.e., STE assets), and managers of STE and vulnerabilities, the integration of the HARTE crisis event model and the all-hazards crisis event predicate illustrates the nexus of ACTN, 6Is, STE, IDM, time, location, the 3Ps, and the 5PMs (see figure 18). This is an interactive conceptual model meaning it should trigger analytic thinking about the significance of FSLTT and private sector analysts and decision-makers in their roles as ACTN and STE handlers, guardians, and managers to prevent, protect, mitigate, respond, and recover from all-hazards crisis events.

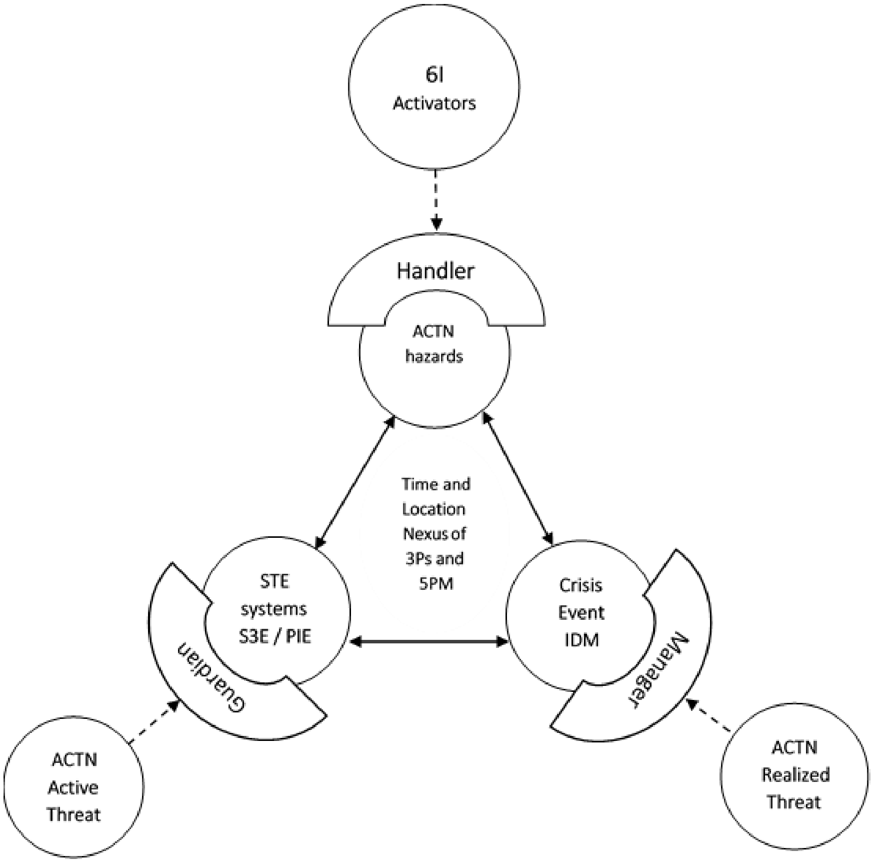

Figure 18. The Integrated HARTE Crisis Event Model and All-Hazards Crisis Event Predicate. This model illustrates the interactive coordination and cooperation roles of homeland security intelligence and operations practitioners who serve as ACTN and STE handlers, guardians, and managers. The nexus of the crisis event (i.e., the HARTE model) in time and location (i.e., the crisis event predicate) with public and private sector handlers, guardians, and managers underscores the significance of effective planning, policy formulation, and practical application of missions to accomplish the five preparedness missions. This figure is the result of research synthesis from previously cited sources.

The *speak* all-hazards structured communication structure. Intelligence synthesis system structure is exemplified in several ways: it is the institutional vertical and horizontal hierarchy structure like the HSIE's operational components, their CIPs, and their institutional missions affiliation with the IC; it is the formal and informal information sharing structures of HSIE and HSOE communities-of-interest and practice networks; and it is the information technology structure that facilitates the HSIE's collection requirements and intelligence generation purpose. The AH-ISM's structural focus stems from knowledge management's knowledge transfer task and from the analysts' knowledge-of-the-customer competency. Together, they emphasize the importance of the all-hazards analysts' effective communication skills in the form of structured communication (i.e., speak).

***Integrating Toulmin's argumentation model into the AH-ISM*.** Structured communication in the AH-ISM is based on Stephen Toulmin's structured argumentation method (Clark, 2017; Inch & Warnick, 2010; Onwuegbuzie & Frels, 2016). Structured argumentation is "a framework to make assumptions, reasoning, rationale, and evidence explicit and transparent" (Clark, 2017, p. 125). It structures evidentiary data, information, assumptions, presumptions, terms, concepts, hypotheses, and claims—that are derived from the intelligence process and data transformation function—into an organized (i.e., structured) format. Hence, the term structured communication rather than argumentation because analysts are primarily required to transfer knowledge and intelligence products to their clients rather than argue about it. The Toulmin model of organizing claims, evidence, warrant, and backing (CEWB) is easily integrated into a final intelligence synthesis product.

CEWB in structured communication. Toulmin's model of argumentation is based on the premise that a claim (i.e., an analytical conclusion) is derived from evidence (i.e., data and information), the warrant (i.e., the linking reasoning) that connects the claim and data, and the backing of more facts or accepted presumptions (Inch & Warnick, 2010, p. 43). For example, the claim-conclusion that illegal narcotics are being distributed by a local gang is based on police surveillance and testimonial evidence-data. Furthermore, the claim and the evidence are linked by the warrant-reasoning that police presence is absent in the community and the backing that research has proven the absence of a guardian increases the opportunity for crime in a location. This CEWB method forms the analytic basis for structured communication in the AH-ISM.

Analytic claims can also be called conclusions or assertions because they are intended to put forward a claimed proposition that is data or evidentiary derived. Additionally, analytic claims place the burden-of-proof on the analysts who make the claim because it is their responsibility to justify their conclusion with evidence, the warrant, and relevant backing. This evidentiary burden severs to strengthen their own content knowledge as well as that of the client (Walton, 2014, p. 116). Ultimately, it also builds trust between analysts and clients (see figure 11).

Assertions, presumptions, and assumptions in structured communication. At this point, it is important to note the differences between assertion (i.e., analytical claims), assumptions, and presumptions that are likely to be included in intelligence products. As previously stated, assertions are evidence-based claims that carry the burden of justification. Assumptions, on the other hand, do not require evidentiary backing and have no burden of justification. Indeed, assumptions can be lies. Presumptions are tentatively accepted as unproven claims; however, a presumption must be proven or justified when challenged (Walton, 2014, pp. 116-117). Often, intelligence products contain presumptions along with assertions that are based on explanatory, testimonial, circumstantial, corroborative, and factual evidence, data, and information (Clark, 2017, pp. 125-126).

This CEWB structure of presenting, or communicating, analytical claims, conclusions, and assessments based on organized supporting evidence is necessary for gaining the trust and confidence of an intelligence client. Clearly, the CIV—the intelligence capital—of an intelligence product is higher when CEWB veracity is high. Likewise, the ISCV—the intelligence capacity—of the intelligence synthesis system is higher when CEWB and CIV are consistently valued as high by intelligence clients and customers.

Analytic structured communications are based on the Toulmin model and institutionally prescribed formats that guide analysts in their core competencies of knowledge organization, generation, transfer, and application. An analytical product's format must have "a structure—discrete parts, some superior or subordinate to others" (Newsome, 2016, p. 288). For example, structure is provided by academic publications and standards that are adopted by the scientific or intelligence communities like the *Publication Manual of the American Psychological Association*, the U.S. Army's operations order format (e.g., situation, mission, execution, sustainment, command and signal), and the U.S. Army's intelligence estimate tabs (e.g., terrain, weather, civil considerations, intelligence preparation of the battlefield products) (Department of the Army, 2014, pp. C-2 - C-17). The information and intelligence that an analyst communicates to the client in each of these examples should be derived from the CEWB model. An all-hazards analyst cannot effectively apply the 4As without a structured communication method based on CEWB analytic reasoning and product presentation.

The *act* all-hazards applied intelligence synthesis purpose. The last systems component of the AH-ISM is its ultimate purpose to produce risk-informed applied intelligence that is privacy, civil rights, and civil liberties compliant. At the analytical level of the all-hazards analyst, this purpose is summed up as *act*. In other words, analysts have the responsibility to act within the scope of their duties to apply the 4As in support of their intelligence clients and customers. At the intelligence synthesis level of the AH-ISM, this purpose is the integration of applied all-hazards intelligence into the HSIE and HSOE domains.

The act competency and applied intelligence purpose completes the intelligence synthesis system. Together with think, know, and speak, as well as the other systems components of function, structure, and process, the ISM can be depicted as an open system with its functional components of input, transformation, and output. Figure 19 illustrates the ISM as an open system that combines knowledge organization, generation, transfer, and application inputs, transformation, and outputs.

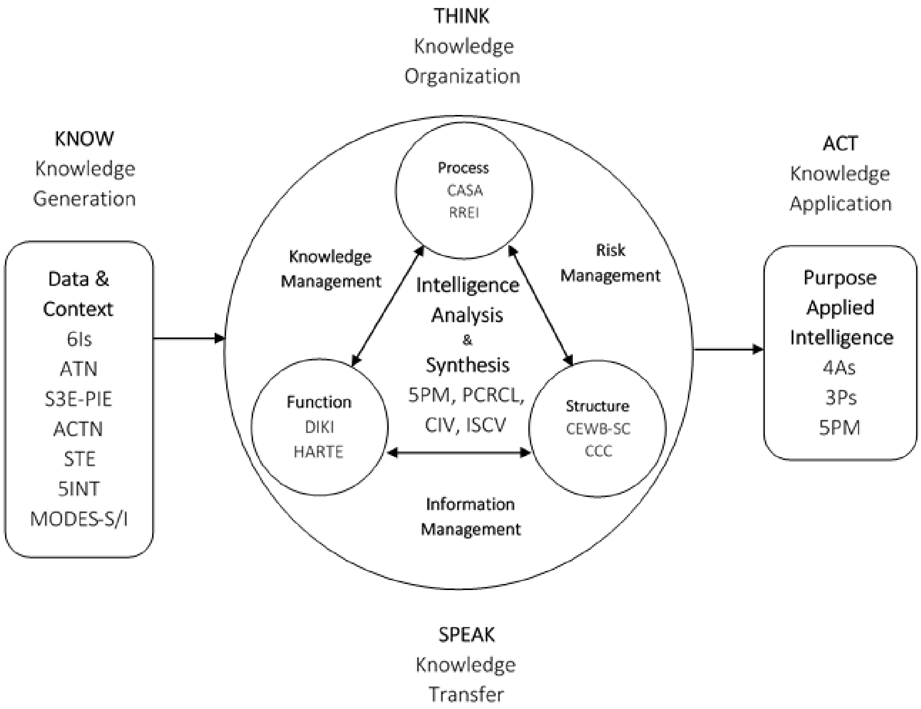

Figure 19. Intelligence Synthesis as a System. The ISM and AH-ISM models are based on an open system model. This figure depicts the systems components and core competencies that were used to create the ISM and AH-ISM. It sequentially depicts (1) the data and contextual inputs, (2) the analysis and synthesis transformational processes, functions, and structures, and (3) the purposeful outputs of the intelligence synthesis system. This figure also aligns think-know-speak-do professional competencies with the KM, IM, RM, and IA institutional competencies that are included in the model. This figure is the result of research synthesis from previously cited sources.

I have introduced no fewer than 34 acronyms that are AH-ISM specific in the analysis and discussion chapters about building the ISM. These acronyms are systems based and derived from the institutional and analyst's professional knowledge core competencies as well as the mission directives and legal requirements placed on the HSIE. An acronym-only illustration of the AH-ISM may help with organizing and visualizing it from a different perspective by placing these acronyms in their appropriate position within the model (see figure 20).

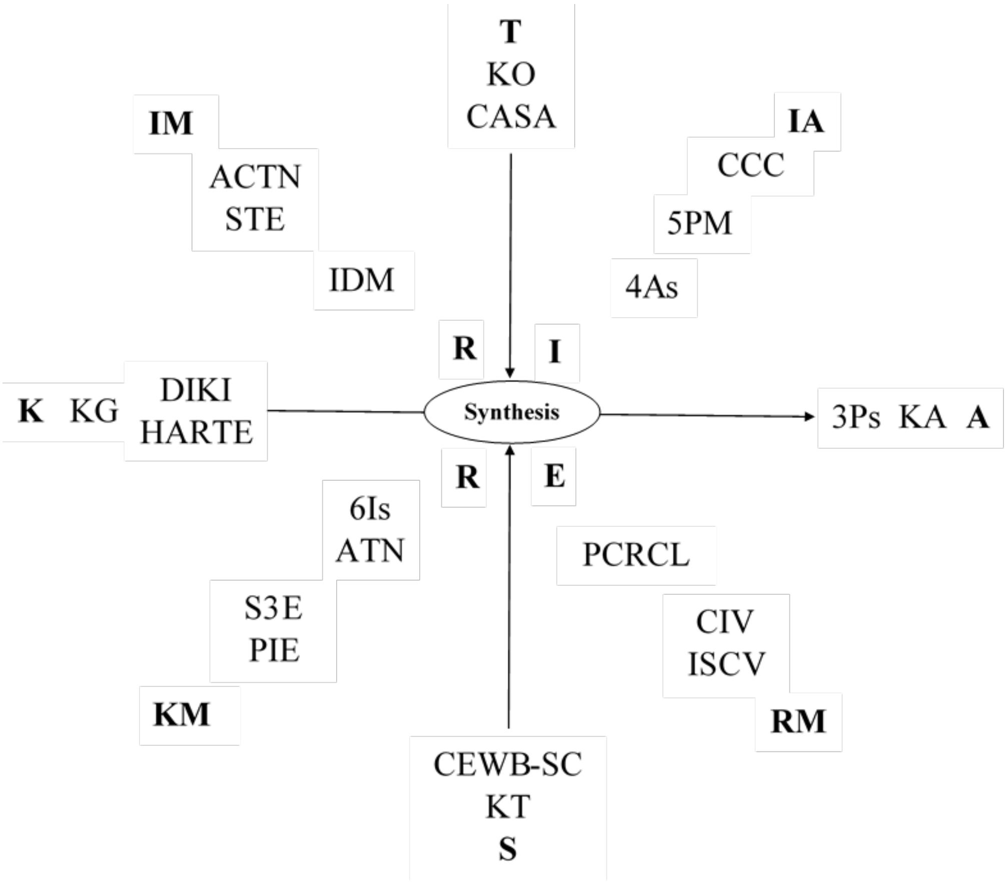

Figure 20. AH-ISM Acronym Only Illustration. This figure represents each acronym that is relevant to building the AH-ISM in their appropriate position to help with organizing and visualizing the model. T is think, K is know, S is speak, and A is act. KO is knowledge organization, KG is knowledge generation, KT is knowledge transfer, and KA is knowledge application. IM is information management, KM is knowledge management, RM is risk management, and IA is intelligence analysis. CASA is collect, analyze, synthesize, apply. DIKI is data, information, knowledge, and intelligence. HARTE is hazards, activators, relationships, threats, and crisis events. CEWB-SC is claim, evidence, warrant, backing and structured communication. 3Ps is policy, plans, and practice. ACTN is adversarial, cyber, technological, and natural. STE is socio-technological-environmental systems. IDM is identify, detect, and measure. S3E is social, engineered, economic, and environmental. PIE is population, infrastructure and institutions, economy and environment. 6Is is initiators, influencers, instigators, inciters, ignitors, or inhibitors. ATN is activities, transactions, and networks. CIV is cumulative intelligence value. ISCV is intelligence synthesis capacity value. PCRCL is privacy, civil rights, and civil liberties. CCC is clients, customers, and consumers. 5PM is prevent, protect, mitigate, respond, and recover preparedness missions. 4As is alert, assess, anticipate, and advise. RREI is reduce, relate, evaluate, and integrate.

Altogether, analyst, all-hazards intelligence products, and their intelligence clients are parts of the whole homeland security domain's problem-solving system. Through meaning-making intelligence assessments and anticipatory estimates, analyst support the decision-making process of emergency and operational planning, policy formulation, and the practical application of those plans and policies. In turn, they contribute to the NPG's missions of prevention, protection, mitigation, recovery, and response as well as the overall safety, security, and resilience of the nation's population and resources. However, decisions alone do not solve homeland security problems—action is required for practical application of plans and policies.

Interdisciplinary Examples of AH-ISM Function Models

The AH-ISM is easily adapted to include many other multidisciplinary functional and purposeful continuums that support all-hazards intelligence synthesis. For example, law enforcement and the judicial systems applications include the evidentiary burden-of-proof continuum ranging from mere suspicion to reasonable suspicion to probable cause to beyond-a-reasonable-doubt to complete certainty (Carter, 2009, p. 63; Walton, 2014, pp. 52-54). Privacy, civil rights, and civil liberty (PCRCL) application includes the first amendment activity protection continuum ranging from routine to expressive to precursory to conclusive activity (Global Advisory Committee, 2012; Department of Homeland Security, 2013, 2018). Another PCRCL application is behavioral and ideologic centric and ranges from non-traditional or diverse to controversial to extreme to criminal. And lastly, another example would be health services test-treatment continuum ranging from pretest, test, treatment, post-treatment (Stern et al., 2015, pp. 5-6).

Like the HARTE crisis event continuum, these multidisciplinary functional and purposeful continuums require inputs from system components that are similar to the CASA and RREI processes, the DIKI knowledge generation function, and CEWB structured communication to be applied, thus becoming actionable, by decision-makers in their respective homeland security contributing disciplines. To be sure, these pluralistic intelligence examples of ACTN hazards, evidentiary, and procedural continuums depicted in figures 18 – 25 are applicable to the AH-ISM as well as the broader all-hazards HSIE and HSOE. Although these figures only depict functional and purposeful continuums, each associated discipline has unique processes and structural system components that contribute relevant data, information, and knowledge into its intelligence synthesis system. Complete selected AH-ISM examples will be presented in the subsequent section of this chapter.

Law enforcement and justice disciplines function examples. Law enforcement and related judicial training is the common program of instruction for DHS intelligence analysts. Consequently, they are primarily trained in the all-crimes analysis aspects of the HSOE with an understanding of how the DIKI knowledge generation process builds upon the functions and purposes of burden-of-proof, evidence, evidential persuasiveness, PCRCL protected activities, behaviors, ideologies, and in PCRCL compliance by institutions and individuals. Additionally, the health care, systems safety engineering, and cybersecurity professionals also understand how the DIKI knowledge generation process builds upon the functions and purposes of epidemiologic and diagnostic clinical reasoning, cyberattacks, and technological accidents and mishaps. Each career field is a contributing discipline to the homeland security operations and intelligence domains committed to safety, security, and resilience.

Burden-of-proof. Burden-of-proof is a legal standard "for what is to be considered a proof in evidential reasoning in law" (Walton, 2014, p. 1). It is used in a court of law, so a judicial decision can be made in a case even though all the facts are not known. Burden-of-proof standards contribute to the law enforcement and judicial continuum of figure 21.

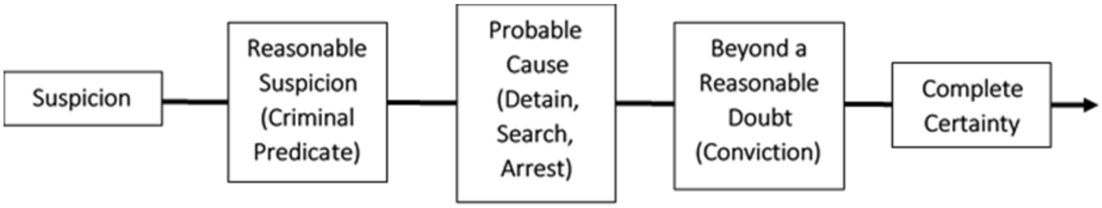
Suspicion
Reasonable Suspicion (Criminal Predicate)
Probable Cause (Detain, Search, Arrest)
Beyond a Reasonable Doubt (Conviction)
Complete Certainty

Figure 21. The Burden-of-proof Continuum. Burden-of-proof and evidentiary reasoning ranges from an inconclusive state to a conclusive state. It begins with mere suspicion of a crime without evidence to reasonable suspicion based on the criminal predicate. From the criminal predicate nexus, it moves to probable cause that allows for legal detention, search, and arrest of the offender to criminal conviction based on judicial reasoning that is beyond-a-reasonable-doubt. It concludes with complete certainty that also is evidentiary based. Not all facts must be known throughout the burden-of-proof continuum because assertions can be based on accepted presumptions. This figure is derived from descriptions and explanations in *Burden-of-proof, Presumption and Argumentation* by Douglas Walton (2014) and *Law Enforcement Intelligence* by David L. Carter (2009).

Evidence and persuasiveness. Evidential reasoning in law, like burden-of-proof, is coupled with persuasiveness to help a law enforcement officer, jury, judge, or intelligence analyst "move forward to a conclusion under conditions of uncertainty, lack of knowledge and even inconsistency" (Walton, 2014, p. 1). Figure 22 depicts evidential reasoning and persuasiveness coupled together in a single continuum. Alongside the burden-of-proof continuum, it helps move forward the analytic reasoning process.

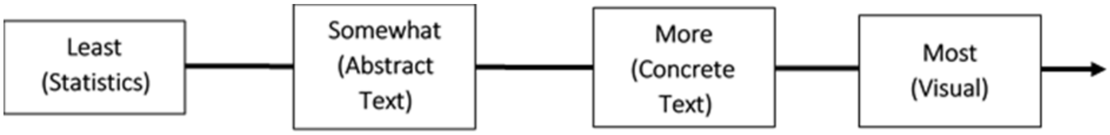

Figure 22. The Integrated Evidence and Persuasiveness Continuum. The evidential persuasiveness continuums range from the lowest level of persuasiveness and the type of evidence to the highest level of persuasiveness and its type. The least persuasive type of evidence to most intelligence clients is statistical, followed by abstract textual, then concrete textual, on to the most persuasive form of visual evidence. This figure is derived from descriptions and explanations in *Intelligence Analysis: A Target-centric Approach* by Robert M. Clark (2017) and *Burden-of-proof, Presumption and Argumentation* by Douglas Walton (2014).

Behavior and ideology. Although some behaviors and ideologies are considered offensive, controversial, and extreme by some people in society, they are not inherently or legally criminal. Behavior and ideology are PCRCL protected until they meet the criminal predicate test of convergent people or organizations, the codified elements of crime, in time and place. The criminal predicate standard must be met before PCRCL protected behaviors and their associated ideology become criminal thus justifying law enforcement intervention or intelligence activities focus (see figure 23).

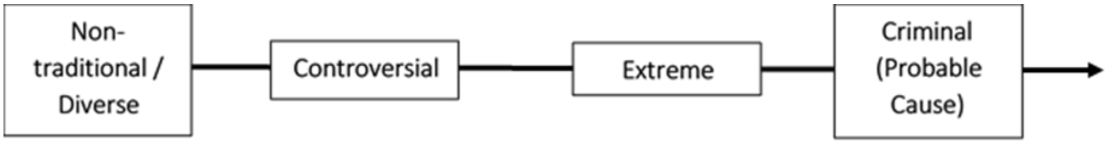

Figure 23. The Behavior and Ideology Continuum. PCRCL protected behavior and ideology converges with criminal behavior in the criminal predicate when probable cause is established that a crime is or will be committed. The range of behavior and ideology begins with PCRCL protected non-traditional or diverse to controversial to extreme. Extreme behavior that exhibits criminal intent (e.g., ideological terrorism) as established by the criminal predicate is probable cause for law enforcement intervention. This figure is derived from descriptions and explanations in *Law Enforcement Intelligence* by David L. Carter (2009).

Activities. Like PCRCL protected behavior and ideology, protected activities, even though some may consider them offensive, controversial, or extreme, are not criminal until the criminal predicate nexus occurs (see figure 24).

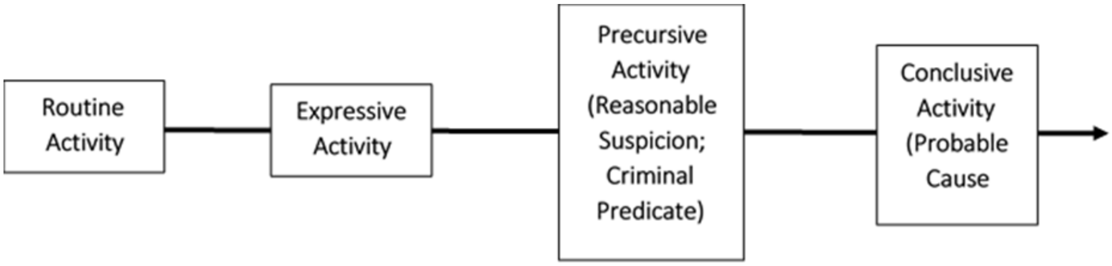
Routine Activity
Expressive Activity
Precursive Activity (Reasonable Suspicion; Criminal Predicate)
Conclusive Activity (Probable Cause

Figure 24. The Activities Continuum. PCRCL protected activities (i.e., protest and demonstrations) converge with criminal activities, like ideologically motivated behavior, in the criminal predicate when probable cause is established that a crime is or will be committed. The range of activities begins with PCRCL protected routine activity to expressive activity to precursive activity (i.e., potentially demonstrative of a criminal predicate). It concludes with conclusive activity that is demonstrative of a criminal predicate. This figure is derived from descriptions and explanations in *Law Enforcement Intelligence* by David L. Carter (2009).

PCRCL compliance. DHS, hence the HSIE, is required by law to conduct its CIPs and operational components in a manner that complies with the minimum legal standards of PCRCL protections for U.S. persons. DHS policy design and practice are intended to go beyond minimum legal compliance and enhance individual liberty “when there is no countervailing harm to the Department’s homeland security mission” (Civil Rights / Civil Liberties Impact Assessment: DHS Support to the National Network of Fusion Centers, 2013, p. ii). Figure 25 depicts the PCRCL compliance continuum.

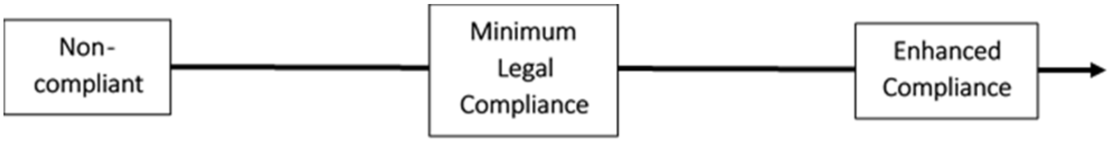

Figure 25. The Privacy, Civil Rights, and Civil Liberties Compliance Continuum. Institutional and individual compliance with PCRCL laws and policies range from non-compliant to enhanced compliance with minimum legal compliance between the two

extremes. DHS strives for enhanced PCRCL compliance by implementing extra institutional policy-based provisions. This figure is derived from descriptions and explanations in *Law Enforcement Intelligence* by David L. Carter (2009) and *Civil Rights / Civil Liberties Impact Assessment: DHS Support to the National Network of Fusion Centers* published by DHS (2013).

Health care disciplines function example. Health care professional must determine when testing and treatment of a patient is necessary. This clinical reasoning process is called the test-treatment threshold (Stern et al., 2015) and it is easily integrated into the natural history or progression of disease continuum beginning with exposure and ending with the preferred outcomes of cure or containment and the undesirable outcomes of disability or death (Gordis, 2014). Figure 26 depicts this integrated continuum that is supported by the clinical reasoning process.

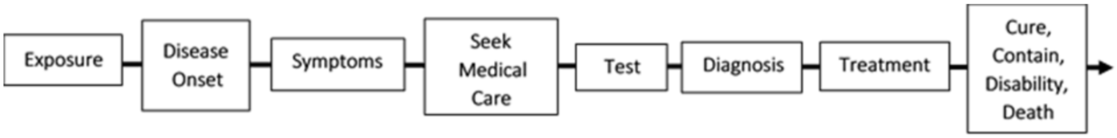

Figure 26. The Integrated Epidemiological and Diagnosis Test-Treatment Continuum. The epidemiologic natural history of disease and the clinical reasoning diagnostic test-treatment thresholds combine to form this figure depicting the hazard to crisis event continuum in the health care fields. It begins with exposure to a disease hazard source to the optimal treatment end state of cure or containment or the undesirable results of disability or death. This figure is adapted from *Epidemiology* by Leon Gordis (2014) and *Symptoms to Diagnosis* by Scott C. Stern, Adam S. Cifu, and Diane Altkorn (2015).

Cybersecurity function example. Cybersecurity and cyber-law enforcement must comply with PCRCL protections as well as the burden-of-proof and evidential reasoning standards. Figure 27 depicts the actions of both cybersecurity practitioners and cyber-criminals in the conduct of their respective activities.

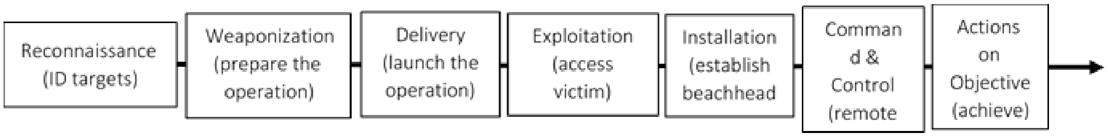
Reconnaissance (ID targets)
Weaponization (prepare the operation)
Delivery (launch the operation)
Exploitation (access victim)
Installation (establish beachhead
Comman d & Control (remote
Actions on Objective (achieve)

Figure 27. The Cyber Kill Chain Continuum. Cybersecurity response actions and the weaponization of cyber tools are depicted in this figure ranging from cyber-reconnaissance of the cyber system or person to the cybersecurity response or the cyber-criminal's achievements. The criminal and crisis event predicate is exemplified in this cyber kill chain continuum (e.g., target / victim, offender / threat, cyber place / vulnerabilities, and the intent to commit a cyber-crime). This figure is adapted from *Gaining the Advantage: Applying Cyber Kill Chain Methodology to Network Defense* published by Lockheed Martin (2015).

Technological systems safety function example. Technological accident and mishap investigations are not necessarily criminally focused unless evidence of a criminal predicate is discovered by systems safety engineers or investigators. Until then, accident and mishap investigations are focused on the technical and technological causal factors rather than adversarial or criminal causal factors (see figure 28).

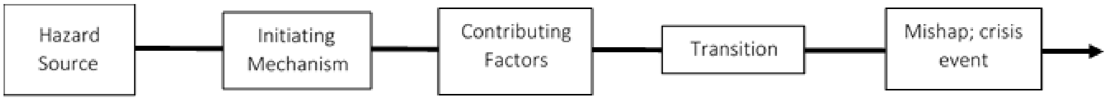

Figure 28. The System Mishap Continuum. Systems safety is focused on the hazard source to crisis event continuum depicted in this figure resulting in a technological mishap or accident. The transitional HARTE crisis event continuum, that includes activators (i.e., initiating mechanisms) and relationships (i.e., contributing factors), are evident in this technological continuum. This figure is derived from Hazard Analysis Techniques for System Safety by Clifton A. Ericson II (2016).

Interdisciplinary Examples of the AH-ISM

Five interdisciplinary examples of completed AH-ISMs are presented in this section to illustrate that the model is replicable and scalable across disciplines and in its scope. The AH-ISM can be reproduced in law enforcement, cybersecurity, systems engineering, health care, and the natural science to name a few. It can be adjusted in its scale and scope to reflect the myriad of processes, functions, and communication structures resident in intelligence and security fields. The purpose of the AH-ISM, however, remains the same regardless of the disciplinary field that replicates it: to provide synthesized applied intelligence.

The adversarial and law enforcement AH-ISM. A competed AH-ISM portrays the parts and whole of the intelligence syntheses system. Each of the four systems component of the AH-ISM are represented as the think-know-speak-act competencies and each of the DIKI and HARTE dual functions and purposes form the centerline of the model. The CASA processes and CEWB structure feed into the knowledge generation and applied intelligence production purpose of the model. The law enforcement CASA-think process is depicted by two complementary processes that promote the critical reasoning and knowledge organization core competencies: the SARA and NCISP intelligence processes (Carter, 2009; Eck et al., 2018; Ratcliffe, 2016). Both of these crime analysis models emphasize the systemic collection, analysis, synthesis, and application of relevant data about crime and criminals.

The DIKI and HARTE-know functions are depicted by the burden-of-proof function model that emphasizes the necessity of processing raw data (i.e., suspicion) into useable information (i.e., criminal predicate); then, into knowledge and intelligence (i.e., probable cause and beyond-a-reasonable-doubt). The CEWB structured communication is depicted by the various law enforcement relevant products of crime statistics, investigative reports, crime maps, and testimony and emphasizes the knowledge transfer and communication skills core competencies. Finally, applied crime intelligence is depicted as integrated law enforcement policies and programs like Intelligence-Led Policing, training, or even judicial conviction based on the complete certainty of persuasive evidence derived from intelligence synthesis—the AH-ISM (see figure 29).

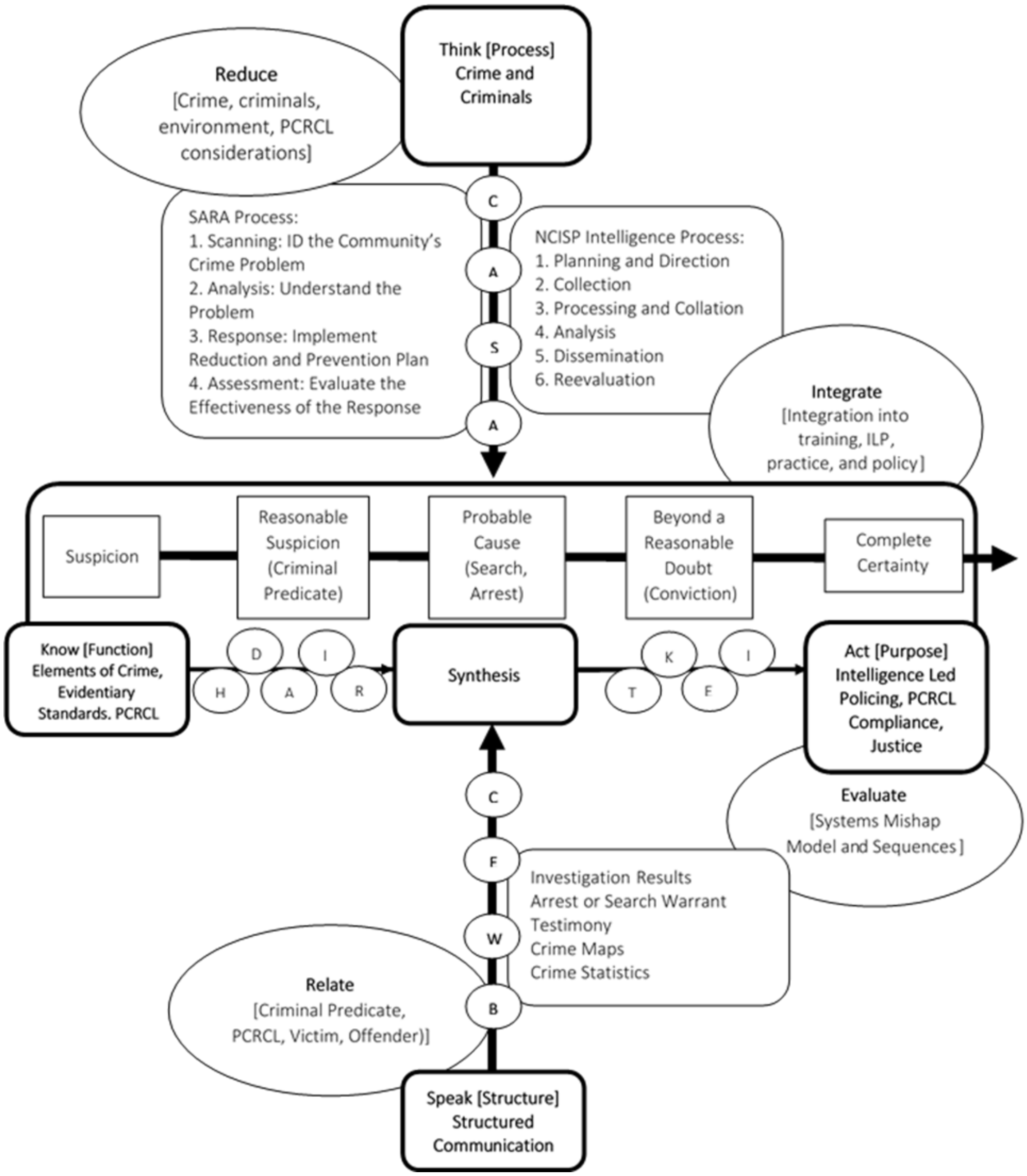
Reduce
[Crime, criminals, environment, PCRCL considerations]
Think [Process] Crime and Criminals
C
A
S
A
SARA Process:
1. Scanning: ID the Community's Crime Problem
2. Analysis: Understand the Problem
3. Response: Implement Reduction and Prevention Plan
4. Assessment: Evaluate the Effectiveness of the Response
NCISP Intelligence Process:
1. Planning and Direction
2. Collection
3. Processing and Collation
4. Analysis
5. Dissemination
6. Reevaluation
Integrate
[Integration into training, ILP, practice, and policy]
Suspicion
Reasonable Suspicion (Criminal Predicate)
Probable Cause (Search, Arrest)
Beyond a Reasonable Doubt (Conviction)
Complete Certainty
Know [Function] Elements of Crime, Evidentiary Standards. PCRCL
D
I
H
A
R
Synthesis
K
I
T
E
Act [Purpose] Intelligence Led Policing, PCRCL Compliance, Justice
Evaluate
[Systems Mishap Model and Sequences]
C
F
W
B
Investigation Results
Arrest or Search Warrant
Testimony
Crime Maps
Crime Statistics
Relate
[Criminal Predicate, PCRCL, Victim, Offender)]
Speak [Structure] Structured Communication

Figure 29. An Interdisciplinary Adversarial and Law Enforcement AH-ISM Example: The Law Enforcement SARA Process, the NCISP Intelligence Process, and The Burden-of-proof Continuum. This figure represents the entire AH-ISM from an adversarial and law enforcement disciplinary perspective. It depicts the dual DIKI and HARTE functions alongside the burden-of-proof function. It also depicts the CASA process alongside the SARA and NCISP processes as inputs into the knowledge generation and applied intelligence purpose. It also depicts the CEWB structured communication input alongside law enforcement formatted reports and other products. The output of this adversarial and law enforcement AH-ISM is risk-informed applied intelligence that is PCRCL compliant. This figure is the result of research synthesis from previously cited sources.

The cybersecurity and law enforcement AH-ISM. The combined cybersecurity and law enforcement CASA-think process is depicted by two complementary processes that promote the critical reasoning and knowledge organization core competencies: the SARA intelligence and cyber defense processes (Carter, 2009; Eck et al., 2018; Lockheed Martin, 2015; Ratcliffe, 2016). Both of these adversarial and cyber-crime analysis models emphasize the systemic collection, analysis, synthesis, and application of relevant data about crime and criminals. Together, they provide key evidential data inputs into the cybersecurity focused AH-ISM.

The DIKI and HARTE-know functions are depicted by the combined cyber kill chain and cyber-response function models that emphasizes the necessity of processing raw cyber-forensic data into useable information; then, into knowledge and intelligence for effective cybersecurity response and forensics. The CEWB structured communication is depicted by the various law enforcement relevant products related to cyber forensics, crime statistics, investigative reports, crime maps, and testimony and their emphasis on the knowledge transfer and communication skills core competencies. Finally, applied cyber-crime intelligence is depicted as integrated cyber-crime and cybersecurity policies, programs, training, or even judicial conviction based on the complete certainty of persuasive cyber-forensic evidence derived from cyber-intelligence synthesis (see figure 30).

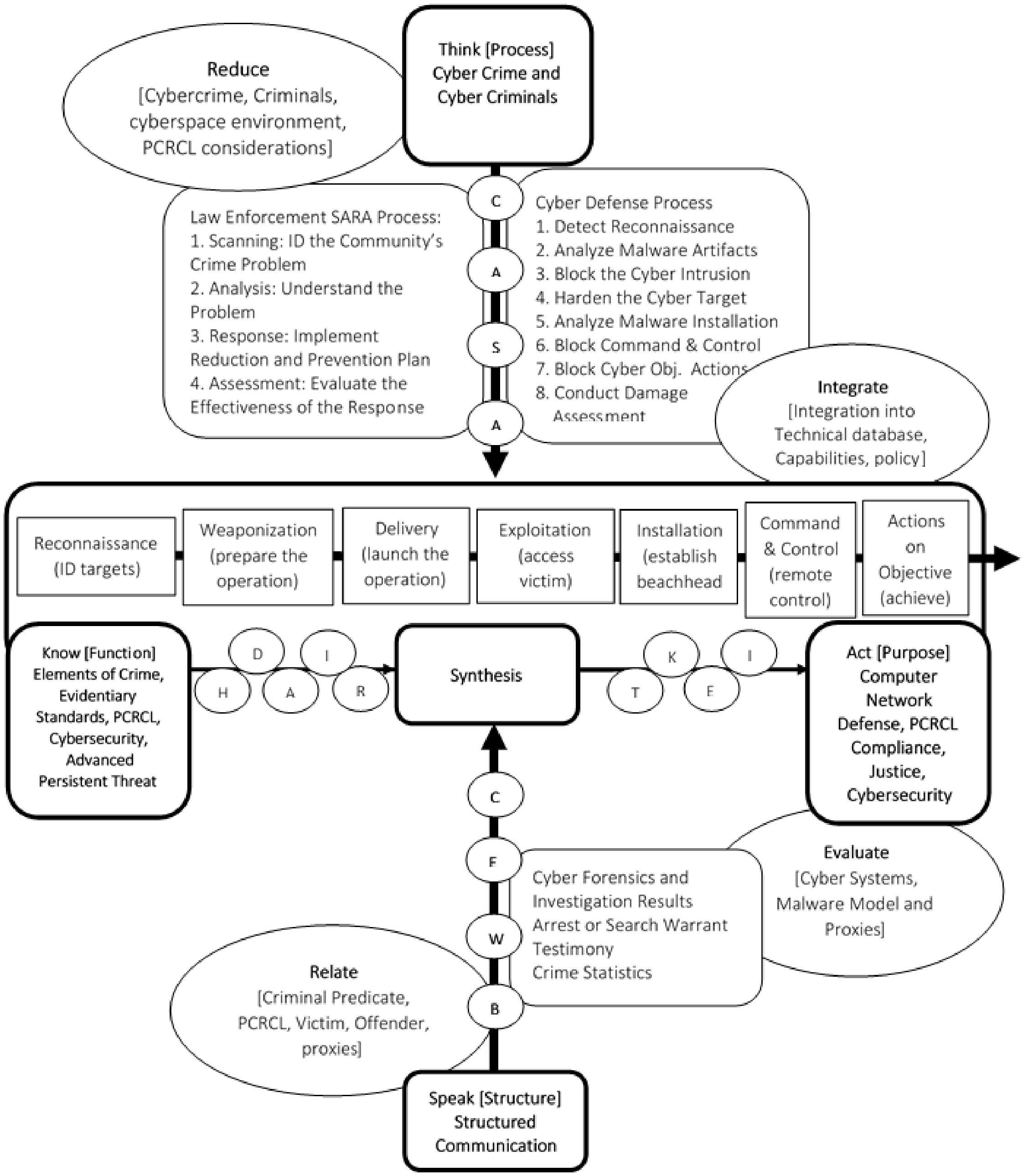
Think [Process] Cyber Crime and Cyber Criminals
Reduce [Cybercrime, Criminals, cyberspace environment, PCRCL considerations]
Law Enforcement SARA Process:
1. Scanning: ID the Community's Crime Problem
2. Analysis: Understand the Problem
3. Response: Implement Reduction and Prevention Plan
4. Assessment: Evaluate the Effectiveness of the Response
C
A
S
A
Cyber Defense Process
1. Detect Reconnaissance
2. Analyze Malware Artifacts
3. Block the Cyber Intrusion
4. Harden the Cyber Target
5. Analyze Malware Installation
6. Block Command & Control
7. Block Cyber Obj. Actions
8. Conduct Damage Assessment
Integrate [Integration into Technical database, Capabilities, policy]
Reconnaissance (ID targets)
Weaponization (prepare the operation)
Delivery (launch the operation)
Exploitation (access victim)
Installation (establish beachhead
Command & Control (remote control)
Actions on Objective (achieve)
Know [Function] Elements of Crime, Evidentiary Standards, PCRCL, Cybersecurity, Advanced Persistent Threat
D
I
H
A
R
Synthesis
K
I
T
E
Act [Purpose] Computer Network Defense, PCRCL Compliance, Justice, Cybersecurity
C
F
W
B
Cyber Forensics and Investigation Results
Arrest or Search Warrant
Testimony
Crime Statistics
Evaluate [Cyber Systems, Malware Model and Proxies]
Relate [Criminal Predicate, PCRCL, Victim, Offender, proxies]
Speak [Structure] Structured Communication

Figure 30. An Interdisciplinary Cybersecurity AH-ISM Example: The Law Enforcement SARA Process, The Cyber Defense process, and the Cyber Kill Chain Continuum. This figure represents the entire AH-ISM from a cybersecurity, adversarial, and law enforcement disciplinary perspective. It depicts the dual DIKI and HARTE functions alongside the combined cyber kill chain and cybersecurity response functions. It also depicts the CASA process alongside the SARA and cyber-defense processes as inputs into the knowledge generation and applied cyber-intelligence purpose. It also depicts the CEWB structured communication input alongside cybersecurity and cyber-forensics law enforcement formatted reports and other products. The output of this cybersecurity, adversarial, and law enforcement AH-ISM is risk-informed applied cyber-intelligence that is PCRCL compliant. This figure is the result of research synthesis from previously cited sources.

The technological mishap AH-ISM. The systems safety engineering CASA-think process is depicted by two complementary processes that promote the critical reasoning and knowledge organization core competencies: the systems safety research and systems engineering processes (Ericson, 2016). Both of these technological hazard analysis models emphasize the systemic collection, analysis, synthesis, and application of relevant data about technological hazards, mishaps, and accidents. Together, they provide key evidential data inputs into the technological mishap investigation focused AH-ISM.

The DIKI and HARTE-know functions are depicted by the technological hazard and mishap continuum that emphasizes the necessity of processing data into useable information; then, into knowledge and intelligence for effective technological mishap and accident investigations. The CEWB structured communication is depicted by the various accident investigation and systems engineering products related to technological accidents and their emphasis on the knowledge transfer and communication skills core competencies. Finally, applied systems safety engineering intelligence is depicted as integrated systems engineering and safety policies, programs, training (see figure 31).

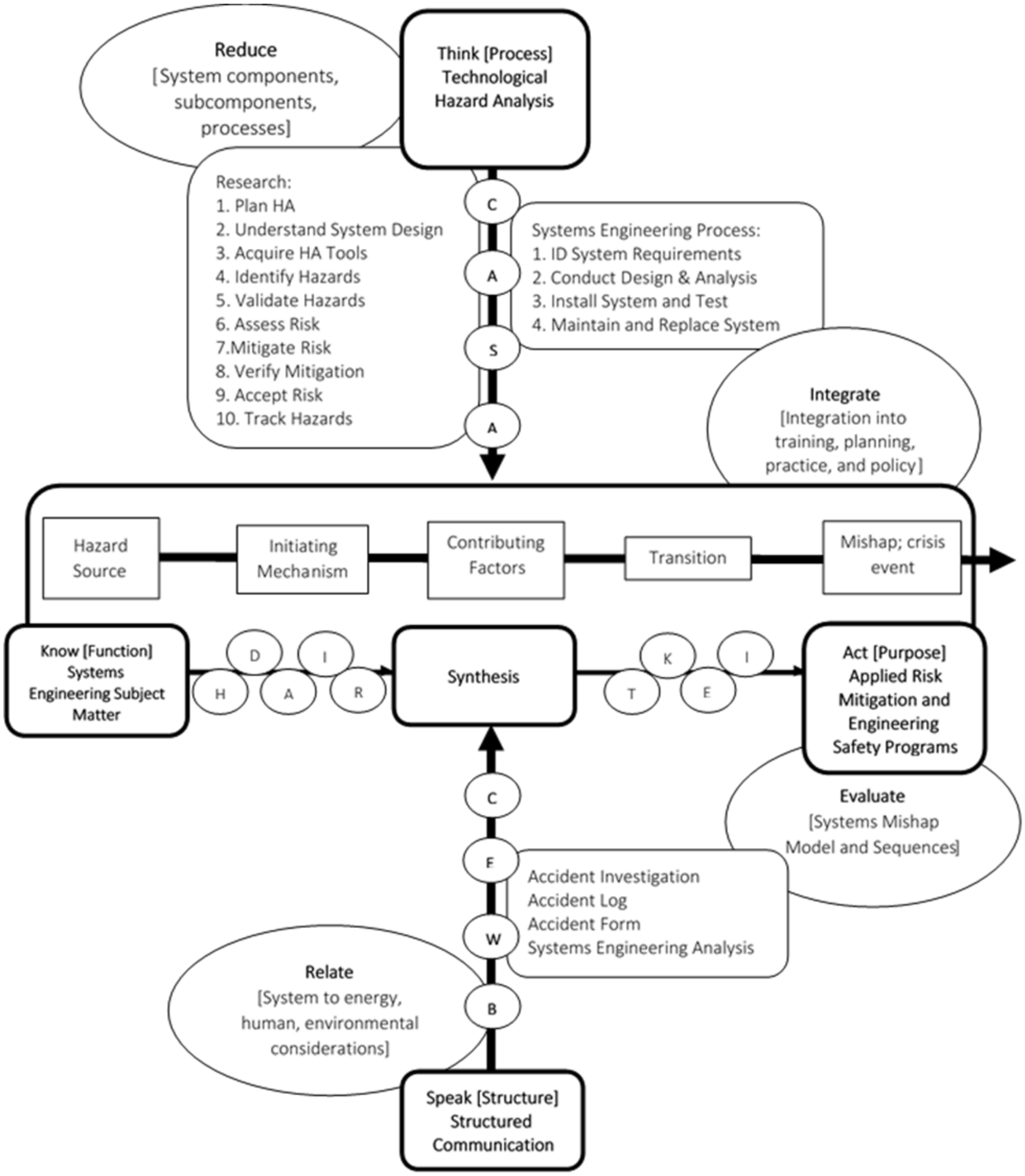
Reduce
[System components, subcomponents, processes]
Think [Process] Technological Hazard Analysis
Research:
1. Plan HA
2. Understand System Design
3. Acquire HA Tools
4. Identify Hazards
5. Validate Hazards
6. Assess Risk
7.Mitigate Risk
8. Verify Mitigation
9. Accept Risk
10. Track Hazards
C
A
S
A
Systems Engineering Process:
1. ID System Requirements
2. Conduct Design & Analysis
3. Install System and Test
4. Maintain and Replace System
Integrate
[Integration into training, planning, practice, and policy]
Hazard Source
Initiating Mechanism
Contributing Factors
Transition
Mishap; crisis event
Know [Function] Systems Engineering Subject Matter
D
I
H
A
R
Synthesis
K
I
T
E
Act [Purpose] Applied Risk Mitigation and Engineering Safety Programs
Evaluate
[Systems Mishap Model and Sequences]
C
F
W
B
Accident Investigation
Accident Log
Accident Form
Systems Engineering Analysis
Relate
[System to energy, human, environmental considerations]
Speak [Structure] Structured Communication

Figure 31. An Interdisciplinary Technological Mishap AH-ISM: The System Research Process, the Systems Engineering Process, and the System Mishap Continuum. This figure represents the entire AH-ISM from a technological and systems engineering disciplinary perspective. It depicts the dual DIKI and HARTE functions alongside the technological mishap and safety engineering functions. It also depicts the CASA process alongside the systems safety research and systems engineering processes as inputs into the knowledge generation and applied technological hazard and mishap investigation and intelligence purpose. It also depicts the CEWB structured communication input alongside systems safety and investigation formatted reports and other products. The output of this technological mishap AH-ISM is risk-informed applied investigative and intelligence products that are, if applicable, PCRCL compliant. This figure is the result of research synthesis from previously cited sources.

The natural hazard (earthquake) AH-ISM. The earthquake natural hazards CASA-think process is depicted by two complementary processes that promote the critical reasoning and knowledge organization core competencies: the geological, geographic, and environmental research process and the scientific problem-solving process (Montello & Sutton, 2013; Pherson & Pherson, 2017). Both of these natural and environmental hazard analysis models emphasize the systemic collection, analysis, synthesis, and application of relevant data about natural hazards, threats, and crises. Together, they provide key data inputs into the natural hazard analysis and intelligence synthesis focused AH-ISM.

The DIKI and HARTE-know functions are depicted by the earthquake crisis event continuum that emphasizes the necessity of processing geological and seismic data into useable information; then, into knowledge and intelligence for effective natural crisis event study. The CEWB structured communication is depicted by the various geological and environmental products related to natural hazards and emphasize the knowledge transfer and communication skills core competencies. Finally, applied natural hazards research and intelligence are depicted as applied homeland security domain safety, security, and resilience policies, programs, training (see figure 32).

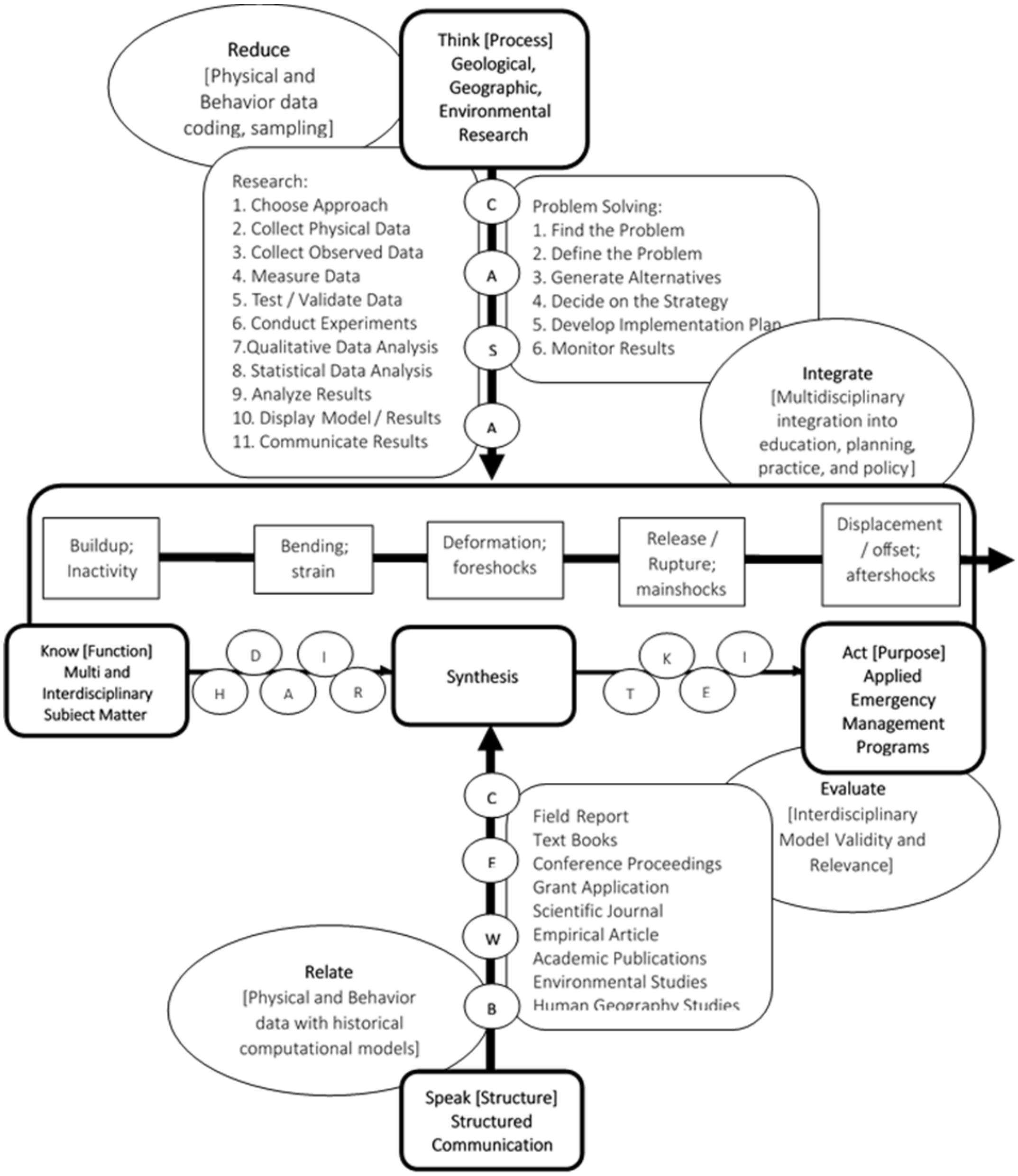

Figure 32. An Interdisciplinary Natural Hazard AH-ISM Example: The Geological, Geographic, and Environmental Research Process, the Scientific Problem-Solving Process, and the Earthquake HARTE Continuum. This figure represents the entire AH-ISM from a natural hazards perspective. It depicts the dual DIKI and HARTE functions alongside the earthquake crisis event process. It also depicts the CASA process alongside the geological and scientific problem-solving processes as inputs into the knowledge generation and applied natural hazard intelligence and research purpose. It also depicts the CEWB structured communication input alongside scientific research and study formatted reports and other products. The output of this natural hazard AH-ISM is risk-informed applied intelligence and research products that are, if applicable, PCRCL compliant. This figure is the result of research synthesis from previously cited sources.

The natural hazard (disease or Contamination) AH-ISM. The disease or contamination natural hazards CASA-think process is depicted by two complementary processes that promote the clinical reasoning and knowledge organization core competencies: the diagnosis and prognosis clinical reasoning processes and the epidemiological and diagnosis test-treatment processes (Gordis, 2014; Stern et al., 2015). Both of these natural disease and epidemiological hazard analysis models emphasize the systemic collection, analysis, synthesis, and application of relevant data about natural hazards, threats, and crises. Together, they provide key data inputs into the natural hazard analysis and intelligence synthesis focused AH-ISM.

The DIKI and HARTE-know functions are depicted by the disease or contamination diagnostic continuum that emphasizes the necessity of processing diagnostic and epidemiologic data into useable information; then, into knowledge and intelligence for effective natural crisis event investigation and research. The CEWB structured communication is depicted by the various diagnostic and investigative medical research products related to natural hazards and their emphasis on the knowledge transfer and communication skills core competencies. Finally, applied natural hazards research and intelligence is depicted as applied homeland security domain safety, security, and resilience policies, programs, training (see figure 33).

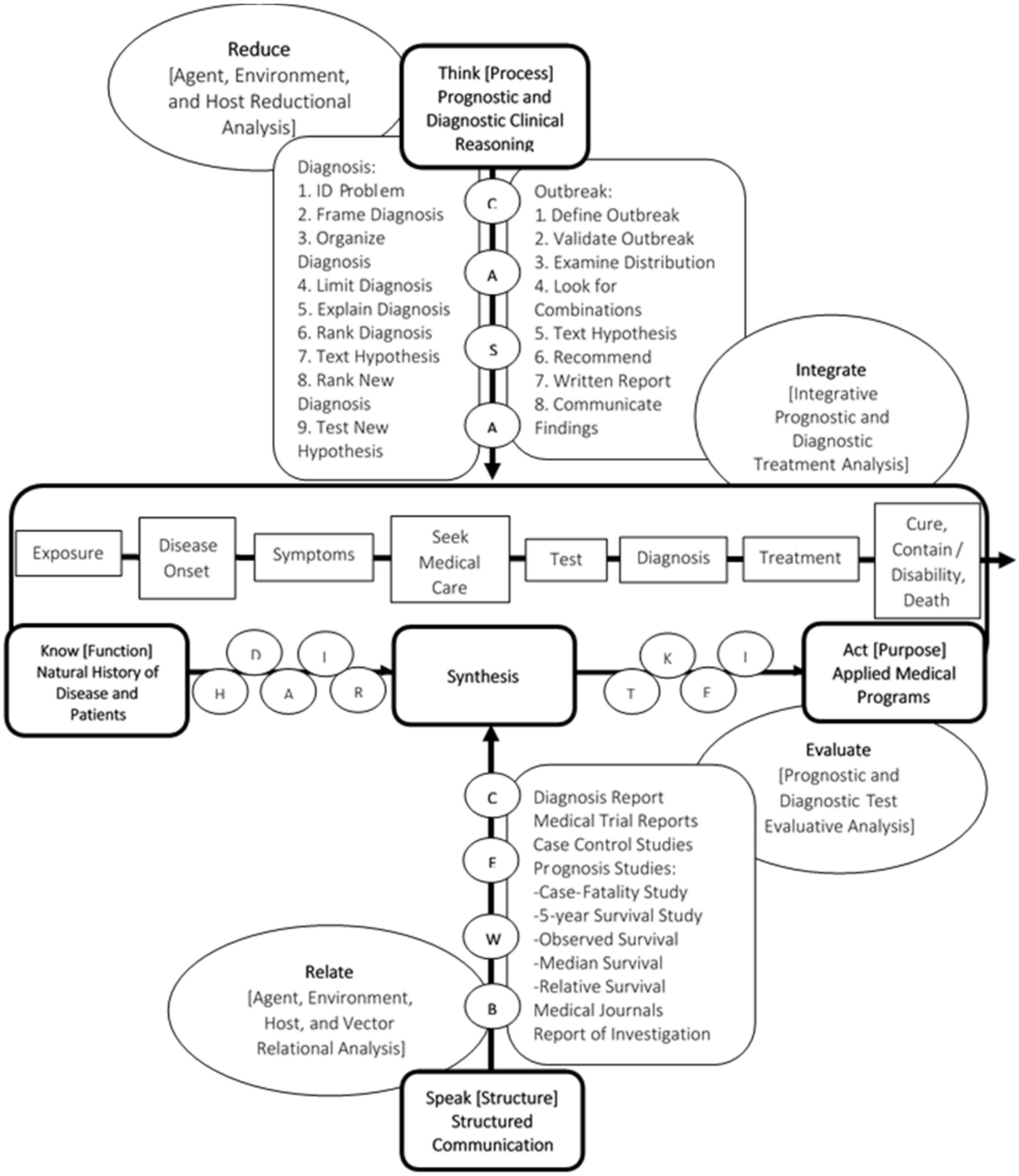

Figure 33. An Interdisciplinary Natural Disease or Human Caused Toxin Illness AH-ISM Example: The Diagnosis and Prognosis Clinical Reasoning Processes and the Epidemiological and Diagnosis Test-Treatment Continuum. This figure represents the entire AH-ISM from a natural hazards and epidemiologic perspective. It depicts the dual DIKI and HARTE functions alongside the disease or contamination diagnostic continuum. It also depicts the CASA process alongside the diagnostic and epidemiological clinical reasoning processes as inputs into the knowledge generation and applied natural hazard intelligence and research purpose. It also depicts the CEWB structured communication input alongside medical research and study formatted reports and other products. The output of this natural hazard AH-ISM is risk-informed applied intelligence and research products that are, if applicable, PCRCL compliant. This figure is the result of research synthesis from previously cited sources.

The CORE Reflexivity Discussion

The CORE process of (1) critical examination, (2) organization, (3) reflection, and (4) evaluation helped me evaluate the process, analysis, and results of my research. The CORE process is intended to be done in a multimodal context to help researchers with the triangulation of data, information, and analytic findings by cross-examination of multiple types of literature sources—MODES or MODES-S/I. It also is intended to help the researcher to flush out any biases and discrepant information. Therefore, it is a dual-purpose method meant for research process improvement and professional development of the researcher. The CORE process of critical examination is based on six questions related to knowledge of organization (i.e., the research process), knowledge generation (i.e., the subject matter content), knowledge transfer (i.e., understanding and communicating with the audience), and knowledge application (i.e., understanding the operational context):

- Critical examination: What did I learn and why?
- Organization: How can I organize and display the content of what I learned?
- Reflection: What was the research process or analysis method like and did it work? How does it relate to the central research questions? Were there any biases or discrepancies?
- Evaluation: What is my conclusion and how can it be integrated into my overall research?

I will reword these CORE questions to reflect the homeland security and intelligence domains context of my research which also will serve as a fitting summary and conclusion to this thesis.

Critical examination of the AH-ISM's applicability. What did I learn about all-hazards risk-informed applied intelligence and why is it important to the HSIE? Framing my research in the bricolage philosophy allows for using already available and proven tools, methodologies, and ideas in a new and innovative way to advance understanding and knowledge about a topic. I have attempted to do this during my research about all-hazards analysis. All the institutional programs, professional competencies, and systemic perspectives that I have drawn upon are currently being implemented in the homeland security intelligence domain. What I have accomplished is a reframing of the *know-what* and *know-how* abilities of HSIE analysts into an alternate conceptual framework for visualizing and conducting all-hazards risk-informed applied-intelligence synthesis that is PCRCL compliant.

Central research question. What is a unifying interdisciplinary all-hazards analysis and intelligence synthesis model for providing risk-informed applied intelligence in support of the United States National Preparedness Goal by the homeland security intelligence enterprise? As discussed in chapters IV and V, the AH-ISM is a unifying conceptual framework that is pluralistic (e.g., transdisciplinary, interdepartmental, and cross-jurisdictional). It contributes to understanding what (i.e., knowledge content) and how (i.e., knowledge generation, transfer, and application) HSIE analysts support the planning processes, policy formulation, and practical application of the NPG by DHS, its operational components, CIPs, and HSOE partners (see figures 29 – 33).

Research questions.

1. What are the current and common all-hazards analysis and intelligence synthesis methods used by analysts in the homeland security intelligence enterprise at fusion centers and in other intelligence production and information sharing organizations? HSIE analysts employed at fusion centers, ISACS, or DHS CIPs utilize a variety of analytic methodologies to identify and analyze ACTN hazards, threats, and crisis events as well as STE assets and resources. My research has presented three common analytical approaches, as many as 45 APOEs, and four analytical steps (see section *analytic approaches and points-of-entry* on page 117) that are used and available to HSIE analysts that are derived from academic textbooks, governmental publications, private publications, and other academic teaching and training resources about intelligence analysis.

2. To what extent does current homeland security intelligence enterprise approved training and certification courses teach common all-hazards analytic methodologies to intelligence analysis students? HSIE analysts, OPM professional series 0132, are primarily trained in law enforcement crime analysis techniques taught by DHS approved or certified institutions and contracted training courses. Professional career advancement for analysts emphasized the importance of being subject-matter-experts not only in their educational disciplines, but also in selected ACTN topics. Advancement in managerial and leadership positions requires a broader understanding of all-hazards (see the *professional development* section on page 147).

3. What, if any, are the knowledge-centric and intelligence operations principles, programs, or policies that are relevant to the all-hazards analysis and intelligence

synthesis model? Intelligence synthesis and all-hazards intelligence analysis are grounded in four institutional programs and processes about knowledge, information, risk, and analysis. Also, analysts obtain four professional competencies from these programs that are relevant to all-hazards risk-informed applied-intelligence production (see figures 14 and 15).

4. What, if any, are the homeland security operational environment's socio-technological-environmental system components that are relevant to the all-hazards analysis and intelligence synthesis model? The social, technological, and environmental systems that comprise the HSOE's assets, resources, and their ACTN hazard sources includes the national population, social communities, critical infrastructure, security institutions, economic resources and institutions, and environmental resources to name a few (see *deconstructing the homeland security operational environment* section on page 85).

5. What, if any, are the consequential relationships among socio-technological-environmental systems and adversarial, cyber, technological, and natural hazards, threats, and crisis event systems? The consequential relationships and activators among social, technological, and environmental systems that comprise the HSOE's assets, resources, and their ACTN hazard sources includes crisis events such as incidents, disasters, and catastrophes. The interactions between them led to the development of the HARTE crisis event model and continuum (see figure 7).

6. To what extent is the all-hazards analysis and intelligence synthesis model replicable and applicable as an analytic model in the interdisciplinary homeland security intelligence enterprise? The AH-ISM is a scalable, replicable, and an enduring model

because it’s system-based structure is universal and easily adapted to include more interdisciplinary processes, functions, and communication formats. However, the purpose of the model to produce all-hazards risk-informed applied-intelligence does not change. The AH-ISM is replicable for the same reason that its scale and scope can be changed. It can be universally replicated in all disciplines that are concerned with systems, system components, and entities (tangible and intangible).

The AH-ISM is enduring because, as a conceptual framework, its core competencies are not entirely dependent upon contemporary technology and technical capabilities. Certainly, technology and information management systems greatly enhance the application of the AH-ISM but its critical reasoning ability, DIKI and HARTE functions, and CEWB structured communication are conceptual frameworks that can endure exclusively within the analysts’ mind. The AH-ISM can be scaled, replicated, and endure the test of time solely as a mindset, written down on paper in pencil, or in the microprocessor of a computer (see figures 14, 15, and 29 – 33).

Organization of the AH-ISM’s content. How did I organize the knowledge generated about pluralistic intelligence synthesis and display the content of what I learned so it contributes to the homeland security studies body of knowledge? The AH-ISM is a conceptual model that simplifies reality, so it required numerous visual models to convey its core concepts. I relied upon triadic models to simplify the depiction of interdisciplinary systems, entities, and their relational links to show their similarities (e.g., the interdisciplinary all-hazards crisis event predicate in figure 5). I also used continuums depicted by arrows to show directional flow in time and space to build the structure of the AH-ISM (e.g., the baseline ISM in figure 13).

The frame (i.e., structure) of the model, based on informational and procedural flows, allowed for the visual inclusion of quadruple zones to depict areas of analytic activity (e.g., the AH-ISM including the RREI analytic process in figure 15). These activity areas also included the core institutional and professional competencies of intelligence activities and analysts. The positioning of these activities in four quad-chart zones also demonstrated their functional and sequential characteristics in the AH-ISM. Lastly, I used acronyms and mnemonics as memory aids such as think-know-speak-act. Another creative example is: ACTioN is the CORE MODE of the HSIE's HARTE and CASA. Analysts can have hours of fun in the break room creating their own (see figure 19). Regardless of the acronyms and mnemonic memory aids used, the AH-ISM is essentially a visual model that helps frame the conceptual framework of systems-based intelligence production.

Reflection about the AH-ISM research process and research questions.

Bricolage, CASA, MODES, RREI, CEWB, and CORE. What was the bricolage research philosophy, CASA process, MODES resources, RREI analysis method, CEWB structured communication, and CORE method like and did it work? Bricolage is a worldview as well as a research philosophy focused on social, political, and historical context. It involves the researcher's interpretation and making-sense about "the complexity of everyday life and the data it constantly throws at us." (Kincheloe & Berry, 2004, p. 82) Also, bricoleurs focus on "the act of interpretation in research, appreciating the distinction between describing a phenomenon and understanding it." (Kincheloe & Berry, 2004, p. 83) I have attempted to follow five principles of bricolage in my research to better interpret, describe, and understand the phenomena of intelligence synthesis, hazards, threats, and crisis events. The five principles are:

- connecting the research objects to their many context.
- appreciating the relationship between myself (the researcher) and the research topic.
- connecting meaning-making to the human experience.
- using textual references while not forgetting that meaning-making is a human experience.
- building a bridge between these principles about understanding and meaning-making to informed action (Kincheloe & Berry, 2004, p. 83).

Throughout my research, I followed the collect, analyze, synthesize, and apply process. Notably, the format of the thesis chapters follows it: the introduction in chapter I established my analytic approach and APOE; the literature review in chapter II presented the collected materials; the analysis methodology in chapter III and the analysis results were given in chapter IV; and chapter V displayed and discussed the synthesis and application of my research. I effectively used the MODES method to access and assess references, applied the RREI analysis steps during analysis, and attempted to follow the CEWB structured communication standard in my writing. Finally, the CORE method has offered an appropriate structured method for conducting and communicating my research evaluation. I assess the processes and methods that I used are suitable frameworks for conducting research and analysis.

Biases and discrepancies. Were there any personal, professional, and academic biases or discrepancies revealed during my research process? How did the research process, biases, or discrepancies relate to the central research question about interdisciplinary all-hazards analysis and intelligence synthesis? My personal biases towards balanced human and eco-centric national level policies and programs are evident in my supportive views of PCRCL compliance by intelligence and security agencies and personnel. I believe in the government protection and civil respect of all people, regardless of race, ethnicity, religion, sex, and cultural heritage, who comprise the nation's population. Lastly, my personal biases are significantly influence by my personal experience with human vulnerability and those people who are disadvantaged during times of loss. It is during these times when individuals and families are overwhelmed, that reliable and fairly administered governmental protections and programs are needed the most. Accordingly, I believe, or rather hope, my research will somehow help in the efforts of homeland security practitioners who provide comfort, safety, and security to those in need.

My professional bias is grounded in selfless national service that is not infringed upon by my political party affiliation nor an extreme affinity to any one race, ethnicity, religion, sex, or cultural heritage. In my professional view, patriotism and loyalty to the ideals of the U.S. Constitution are paramount; yet, they are not inconsistent with acknowledge membership in the global community and respecting the dignity and civil liberties of all people in the world. My academic biases are evident in my thesis research topic that is limited to homeland security and intelligence in support of national safety, security, and resilience objectives that comply with human-centric PCRCL compliance and the preservation of natural resources. I believe constitutionally constructive limitations placed on the intelligence community are necessary forcing mechanisms to ensure only the highest quality intelligence products are put forth.

Evaluation of the AH-ISM's integration into the HSIE. What is my conclusion about the research process that I used, my analysis methods, and the results of my research about interdisciplinary all-hazards analysis and intelligence synthesis (i.e., the AH-ISM), and how can it be integrated into future research? It is my conclusion that the AH-ISM is a suitable model for visualizing and applying intelligence analysis and production. Although it is not presented in this thesis as the *only* solution to the problem of an insufficient unifying analytical mindset in the HSIE, the AH-ISM is a useful tool for (a) interdisciplinary teaching intelligence analysis and synthesis to HSIE students, (b) establishing an academic program of instruction for institutional and professional development courses, (c) a frame of reference or mindset for interdisciplinary practitioners in the homeland security and intelligence domains, and (d) a practical guideline for interagency, interdisciplinary, and multijurisdictional coordination and cooperation efforts. Also, the AH-ISM is meant to be used. It is intended to be applied as a pluralistic intelligence synthesis tool for intelligence generation and sharing to promote better operational planning, policy formulation, and field practice within the HSIE.

Recommendations for Future Research

Further research about interdisciplinary all-hazards intelligence synthesis is necessary because this thesis is only a cursory look at it from a systems perspective. Although the AH-ISM is a useful model, like useful information in the DIKI continuum, it is not a mature intelligence synthesis model and requires more research. It has not been scenario tested and practically applied as a proven intelligence model in the homeland security and intelligence domains. Therefore, I recommend no fewer than four concentration areas for future research based on my CORE evaluation:

- the extent of the AH-ISM's practical application as an interdisciplinary all-hazards teaching model to HSIE intelligence analysis students.
- the extent of the AH-ISM's practical application in establishing an academic program of instruction that is based on its four institutional core competencies, its four professional core competencies, U.S. Constitutional PCRCL compliance, and its systems component structure.
- the extent of the AH-ISM's usefulness as a systems-based framing mindset for interdisciplinary practitioners in the homeland security and intelligence domains.
- the extent of the AH-ISM's practical application in the pluralistic intelligence environment to include comprehensive modeling of transdisciplinary ACTN hazards, threats, and crisis events; STE systems, assets, and national resources for critical infrastructure protection; and FSLTT interagency and multijurisdictional applications as an all-hazards risk-informed applied-intelligence model.

Echoing my earlier comment, I hope future research on the applicability, suitability, and effectiveness of the AH-ISM will contribute to the body of knowledge in the emerging homeland security studies discipline.

wgr

REFERENCES

Abbott, P. L. (2017). *Natural disasters* (10 ed.). New York, NY: McGraw-Hill Education.

ACASA. (2018, March 29). *Types of systems*. Retrieved from Ackoff Collaboratory for the Advancement of the Systems Approach: http://www.acasa.upenn.edu/4sys.htm

Ackoff, R. L., & Emery, F. E. (2017). *On purposeful systems.* New York, NY: Routledge.

American Psychological Association. (2010). *Publication maual of the American psychological association.* Washington D.C.: American Psychological Association.

Andress, J. (2014). *The basics of information security* (2nd ed.). Waltham, MA.

Antony, R. T. (2016). *Data fusion support to activity-based intelligence.* Norwood, MA: Artech House.

Becerra-Fernandez, I., & Sabherwal, R. (2015). *Knowledge management* (2 ed.). New York, NY: Routledge.

Bejan, A., & Zane, J. P. (2012). *Design in nature.* New York, NY: Anchor Books.

Bickman, L., & Rog, D. J. (2009). *The SAGE handbook of applied social research* (2 ed.). Thousand Oaks, CA: SAGE Publications, Inc.

Biltgen, P., & Ryan, S. (2016). *Activity-based intelligence and applications.* Norwood, MA: Artech House.

Brougham, G. (2015). *The cynefin mini-book: an introduction to complexity and the cynefin framework.* C4Media.

Bullock, J. A., Haddow, G. D., & Coppola, D. P. (2016). *Introduction to homeland security* (Fifth ed.). Waltham, MA: Butterworth-Heinemann.

Bullock, J., Coppola, D., & Haddow, G. (2014). *Introduction to emergency management.* Waltham, MA: Elsevier Inc.

Burton, N. (2018, September 14). *Our hierarchy of needs*. Retrieved from Psychology Today: https://www.psychologytoday.com/us/blog/hide-and-seek/201205/our-hierarchy-needs

Capra, F., & Luisi, P. L. (2014). *The systems view of life.* Cambridge: Cambridge University Press.

Carter, D. L. (2009). *Law enforcement intelligence* (2 ed.). Washington D.C.: Department of Justice.

Clark, R. M. (2011). *The technical collection of intelligence.* Washington D.C.: CQ Press.

Clark, R. M. (2017). *Intelligence analysis: a target-centric approach* (5 ed.). Thousand Oaks, CA: CQ Press.

Creswell, J. W. (2014). *Research design* (4 ed.). Thousand Oaks, CA: SAGE Publications, Inc.

Dalby, S. (2013). Climate change and environmental security. In P. D. Williams, *Security Studies* (pp. 311-323). New York: Routledge.

Department of Defense. (2017). *DoD dictionary of military and associated terms (DOD Dictionary).* Washington D.C.

Department of Energy. (2018, September 14). *National security & safety*. Retrieved from Department of Energy: https://www.energy.gov/national-security-safety

Department of Homeland Security. (2010). *Considerations for fusion center and emergency operations center coordination.* Washington D.C.: Department of Homeland Security.

Department of Homeland Security. (2010). *DHS risk lexicon.* Washington D.C.: Risk Steering Committee.

Department of Homeland Security. (2011). *National disaster recovery framework.* Washington D.C.: Department of Homeland Security.

Department of Homeland Security. (2011). *National preparedness system.* Washington D.C.: Department of Homeland Security.

Department of Homeland Security. (2011). *Risk management fundamentals.* Washington, D.C.: Department of Homeland Security.

Department of Homeland Security. (2011). *The strategic national risk assessment.* Washington, D.C.: Department of Homeland Security.

Department of Homeland Security. (2013). *Civil rights / civillLiberties impact assessment: DHS Support to the National Network of Fusion Centers.* Washington D.C.: Department of Homeland Security.

Department of Homeland Security. (2013). *Intelligence / investigation function guidance and field operations guide.* Washington, D.C.: Department of Homeland Security.

Department of Homeland Security. (2013). *National incident management system* (2 ed.). Washington D.C.: Department of Homeland Security.

Department of Homeland Security. (2013). *National infrastructure protection plan.* Washington D.C.: Department of Homeland Security.

Department of Homeland Security. (2013). *Threat and hazard identification and risk assessment guide.* Washington D.C.: Department of Homeland Security.

Department of Homeland Security. (2015). *National preparedness goal* (2 ed.). Washington D.C.: Department of Homeland Security.

Department of Homeland Security. (2016). *2016 national network of fusion centers final report.* Washington D.C.: Department of Homeland Security.

Department of Homeland Security. (2016, February 24). *Critical infrastructures sectors*. Retrieved from Homeland Security: https://www.dhs.gov/critical-infrastructure-sectors

Department of Homeland Security. (2016). *Mitigation federal interagency operational plan.* Washington D.C.: Department of Homeland Security.

Department of Homeland Security. (2016). *National cyber incident response plan.* Washington, D.C.: Department of Homeland Security.

Department of Homeland Security. (2016). *National mitigation framework.* Washington D.C.: DHS.

Department of Homeland Security. (2016). *National prevention framework.* Washington D.C.: Department of Homeland Security.

Department of Homeland Security. (2016). *National protection framework.* Washington D.C.: DHS.

Department of Homeland Security. (2016). *National response framework.* Washington D.C.: Department of Homeland Security.

Department of Homeland Security. (2016). *Overview of the federal interagency operational plans.* Washington D.C.: Department of Homeland Security.

Department of Homeland Security. (2016). *Protection federal interagency operational plan.* Washington D.C.: Department of Homeland Security.

Department of Homeland Security. (2016). *Recovery federal interagency operational plan.* Washington D.C.: Department of Homeland Security.

Department of Homeland Security. (2016). *Response federal interagency operational plan.* Washington D.C.: Department of Homeland Security.

Department of Homeland Security. (2018, September 18). *Mature and strengthen the homeland security enterprise*. Retrieved from Homeland Security: https://www.dhs.gov/strengthen-security-enterprise

Department of Homeland Security. (2018, April 14). *Office of intelligence and analysis mission*. Retrieved from Homeland Security: www.dhs.gov

Department of Homeland Security. (2018, September 18). *Operatioal and support components*. Retrieved from Homeland Security: https://www.dhs.gov/operational-and-support-components

Department of Homeland Security. (2018, September 14). *Operational and support components*. Retrieved from Homeland Security: https://www.dhs.gov/operational-and-support-components

Department of Homeland Security. (2018, March 24). *Our mission*. Retrieved from Department of Homeland Security: https://www.dhs.gov/our-mission

Department of Homeland Security. (2018, September 13). *Our mission*. Retrieved from Homeland Security: https://www.dhs.gov/our-mission

Department of Homeland Security. (2018, September 13). *PCRCL for fusion centers*. Retrieved from Homeland Security: https://www.dhs.gov/pcrcl-fusion-centers

Department of Homeland Security. (2018, September 21). *Privacy overview*. Retrieved from Homeland Security: https://www.dhs.gov/privacy-overview

Department of Justice. (2007). *Minimum criminal intelligence training standards for law enforcement and other criminal justice agencies in the United States.* Washington D.C.: Department of Justice.

Department of Justice. (2008). *Common competencies for state, local, and tribal intelligence analysts.* Washington D.C.: Department of Justice.

Department of Justice. (2010). *Common competencies for state, local, and tribal intelligence analysts.* Washington D.C.: Department of Justice.

Department of Justice. (2012). *Law enforcement analytic standards.* Washington D.C.: Department of Justice.

Department of the Army. (2012). *ADRP 7-0 Training units and developing leaders.* Washington D.C.: Department of the Army.

Department of the Army. (2012). *FM 3-55 Information collection.* Washington D.C.: Department of the Army.

Department of the Army. (2014). *ATP 5-19 risk management.* Washington D.C.: Department of the Army.

Department of the Army. (2014). *FM 6-0 Commander and staff organization and operations.* Washington D.C.: Department of the Army.

Ducote, B. M. (2010). *Challenging the application of PMESSI-PT in a complex environment.* Fort Leavenworth: School of Advanced Military Studies.

Eck, J. E., Clarke, R. V., & Petrossian, G. (2018). *Intelligence analysis for problem solvers.* San Bernardino, CA.

Elder, L., & Paul, R. (2012). *The thinkers guide to analytic thinking* (2 ed.). Tomales, CA: The Foundation for Critical Thinking.

Ericson, C. A. (2016). *Hazard analysis techniques for system safety* (2 ed.). Hoboken, NJ: John Wiley & Sons.

Federal Emergency Management Agency. (1997). *Multi-hazard identification and risk assessment.* Washington D.C.: Federal Emergency Management Agency.

Federal Emergency Management Agency. (2011). *Crosswalk of target capabilities to core capabilities.* Washington D.C.: Federal Emergency Management Agency.

Federal Emergency Management Agency. (2018, September 21). *Emergency management institute*. Retrieved from FEMA Emergency Management Institute: https://training.fema.gov/

Federal Law Enforcement Training Centers. (2018, September 21). *Federal law enforcement training centers*. Retrieved from Federal Law Enforcement Training Centers: https://www.fletc.gov/

FEMA. (2008). *Incident command system training.* Washington D.C.: FEMA. Retrieved 10 1, 2018, from https://training.fema.gov/emiweb/is/icsresource/assets/reviewmaterials.pdf

Fennelly, L. J. (2017). *Effective physical security.* Cambridge, MA: Butterworth-Heinemann / Elsevier Inc.

Ferlemann. (2015). *Incident command system (ICS).* Lakeland: The Lightning Press.

Geary, M. (2014). *National security and civil liberty.* Durham, NC: Carolina Academic Press.

Global Advisory Committee. (2012). *Guide to conducting privacy impact assessments.* Washington D.C.: Bureau of Justice Assistance.

Gordis, L. (2014). *Epidemiology.* Philadelphia, PA: Elsevier Saunders.

Gunderson, L. H., & Holling, C. S. (2002). *Panarchy: understanding transformations in human and natural systems.* Washington D.C.: Island Press.

Hampson, F. O. (2013). Human Security. In P. D. Williams, *Security studies: an introduction* (pp. 279-294). New York, NY: Routledge.

Hassenzahl, D. M., Hager, M. C., & Berg, L. R. (2011). *Visualizing environmental science* (4 ed.). Hoboken, NJ: John Wiley and Sons.

Haynes, J., Hough, P., Malik, S., & Pettiford, L. (2011). *World politics.* Essex, England: Pearson Education Limited.

Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2018). *Cybercrime and digital forensics.* New York, NY: Routledge.

Homeland Security Committee. (2016). *Reviewing the department of homeland security's intelligence enterprise.* Washington D.C.: House Homeland Security Committee Majority Staff Report.

Hough, P. (2014). *Environmental security: an introduction.* New York, NY: Routledge.

Hough, P. (2015). Environmental security. In P. Hough, S. Malik, A. Moran, & B. Pilbeam, *International security studies theory andpPractice* (pp. 211-224). New York: Routledge.

Inch, E. S., & Warnick, B. (2010). *Critical thinking and communication* (6 ed.). Boston, MA: Pearson Education, Inc.

Interagency Security Committee. (2015). *Best practices for planning and managing physical security resources: an interagency security committee guide.* Washington D.C.: Interagency Security Committee.

Keller, E. A., & DeVecchio, D. E. (2015). *Natural hazards: earth's processes as hazards, disasers, and catastrophes* (4 ed.). New York, NY: Routledge.

Keller, E. A., & DeVecchio, D. E. (2016). *Natural hazards* (4 ed.). New York, NY: Routledge.

Kincheloe, J. L., & Berry, K. S. (2004). *Rigour and complexity in educational research.* New York, NY: Open University Press.

Lahneman, W. (2018, September 15). *Fusion centers.* Retrieved from CHDS/ED: https://www.chds.us/ed/items/398

Lahneman, W. (2018, September 15). *Homeland security intelligence.* Retrieved from CHDS/ED: https://www.chds.us/ed/items/397

Lahneman, W. (2018, September 15). *The seven step intelligence process.* Retrieved from CHDS/ED: https://www.chds.us/ed/items/401

Leader to Leader Institute. (2004). *Be-know-do.* San Francisco, CA: Jossey-Bass.

Lockheed Martin. (2015). *Gaining the advantage: applying cyber kill chain methodology to network defense.* Bethesda, MD: Lockheed Martin.

Lowenthal, M. M. (2015). *Intelligence: From secrets to policy* (6 ed.). Thousand Oaks, CA: SAGE Publications, Inc.

Lowenthal, M. M., & Clark, R. M. (2016). *The 5 disciplines of intelligence collection.* Thousand Oaks, CA: CQ Press.

Malik, S. (2015). Human security. In P. Hough, S. Malik, A. Moran, & B. Pilbeam, *International security studies theory and practice* (pp. 57-71). New York: Routledge.

Maxwell, J. A. (2013). *Qualitative research design: an interactive approach* (3 ed.). Thousand Oaks, CA: SAGE Publications, Inc.

McEntire, D. A. (2006). The importance of multi- and inter-disciplinary research on disasters and for emergency management. In D. A. McEntire (Ed.), *The importance of multi- and inter-disciplinary research on disasters and for emergency management.* Washington D.C.: Federal Emergency Management Agency Emergency Management Institute.

Meadows, D. H. (2008). *Thinking in systems.* (D. Wright, Ed.) White River Junction, VT: Chelsea Green Publishing.

Miles, M. B., Huberman, A. M., & Saldaña, J. (2014). *Qualitative data analysis* (3 ed.). Thousand Oaks, CA: SAGE Publications, Inc.

Mileti, D. S. (1999). *Disasters by Design.* Washington D.C.: John Henry Press.

Montello, D. R., & Sutton, P. C. (2013). *An introduction to scientific research methods in geography and environmental studies.* Thousand Oaks, CA: Sage.

Moore, J. T. (2010). *Chemistry essentials for dummies.* Hoboken, NJ: John Wiley & Sons, Inc.

National Fire Protection Agency. (2013). *NFPA 1600: Standard on disaster / emergency management and busiess continuity programs* . Quincy: National Fire Protection Agency.

Newsome, B. (2014). *Security and risk management.* Thousand Oaks: Sage Publications, Inc.

Newsome, B. O. (2016). *An introduction to research, analysis, writing.* Thousand Oaks, CA: SAGE Publications, Inc.

Office of Personnel Management. (2009). *Handbook of occupational groups and families.* Washington D.C.: Office of Personnel Management.

Onwuegbuzie, A. J., & Frels, R. (2016). *7 Steps to a comprehensive literature review: A multimodal & cultural approach.* Thousand Oaks, CA: SAGE Publications, Inc.

Osborne, D. (2006). *Out of bounds: innovation and change in law enforcement intelligence analysis.* Washington D.C.: JMIC Press.

Pherson, K. H., & Pherson, R. H. (2017). *Critical thinking for strategic intelligence* (2 ed.). Thousand Oaks, CA: CQ Press.

Pine, J. C. (2015). *Hazards analysis.* Boca Raton, FL: CRC Press.

Pritchard, C. L. (2015). *Risk management concepts and guidance.* Boca Raton, FL: CRC Press.

Project Management Institute. (2017). *A guide to the project management body of knowledge-PMBOK Guide* (6 ed.). Newtown Square, PA: Project Management Institute.

Radvanovsky, R., & McDougall, A. (2013). *Critical infrastructure homeland security and emergency preparedness.* Boca Raton, FL: CRC Press.

Ratcliffe, J. H. (2016). *Intelligence-led policing* (2 ed.). New York, NY: Routledge.

Richelson, J. T. (2016). *The US intelligence community* (6 ed.). Boulder, CO: Westview Press.

Sandia National Labratories. (2007). *Categorizing threat: building a generic threat matrix.* Albuquerque, NM: Sandia National Labratories.

Schleicher, A. (2018). *World class: how to build a 21st-century school system.* Paris, France: OECD Publishing.

Singer, P. W., & Friedman, A. (2014). *Cybersecurity and cyberwar.* New York: Oxford University Press.

Smith, E. (2015). The traditional routes to security: realism and liberalism. In P. Hough, S. Malik, A. Moran, & B. Pilbeam, *International security studies theory and practice* (pp. 12-30). New York: Routledge.

Steiner, J. E. (2015). *Homeland security intelligence.* Thousand Oaks, CA: CQ Press.

Stern, S. C., Cifu, A. S., & Altkorn, D. (2015). *Symptoms to diagnosis* (3 ed.). New York, NY: McGraw Hill Education.

The Global Advisory Committee. (2015). *Analyst professional development road map.* Washington D.C.: Department of Justice.

U.S. Army Acquisition Support Center. (2018, September 19). *Distributed commong ground system-army (DCGS-A)*. Retrieved from U.S. Army USAASC: https://asc.army.mil/web/portfolio-item/iews-dcgs-a/

Vellani, K. H., & Nahoun, J. (2001). *Applied crime analysis.* Woburn, MA: Butterworth-Heinemann.

Verschuuren, G. M. (2017). *The holism-reductionism debate in physics, genetics, biology, neuroscience, ecology, and sociology.* Columbia, SC: Verschuuren, Gerard M.

Walker, J. T., & Drawve, G. R. (2018). *Foundations of crime analysis.* New York, NY: Routledge.

Walton, D. (2014). *Burden of proof, presumption and argumentation.* New York, NY: Cambridge University Press.

WePC. (2018, September 14). *2018 Video game industry statistics, trends & data*. Retrieved from WePC: https://www.wepc.com/news/video-game-statistics/#video-gaming-industry-overview

Whitman, G., & Kelleher, I. (2016). *Neuro teach: brain science and the future of education.* Lanham, MD: Rowman & Littlefield.

VITA

Walter G. Reeves

Sam Houston State University
College of Criminal Justice
Department of Homeland Security Studies
Huntsville, Texas

Education:

Master of Science in Homeland Security Studies, Sam Houston State University, 2018
U.S. Army Command and General Staff College (resident), 2003
U.S. Army Imagery Intelligence Officer Course, 1996
U.S. Army Intelligence in Combating Terrorism Course, 1994
U.S. Army Military Intelligence Officer Advanced Course, 1994
U.S. Army Air Defense Artillery Officer (PATRIOT) Course, 1990
Bachelor of Science, Criminal Justice, Sam Houston State University, 1989

Professional Experience:

Walter G. Reeves, LTC, Retired, is an intelligence and security professional with over 22 years' experience, including nearly nine continuous years of employment and service in the Republic of Korea supporting the United States Forces Korea, the 8th United States Army, its major subordinate commands, and the Theater Intelligence Brigade. Throughout his military intelligence assignments, he was responsible for intelligence collection, analysis, and product dissemination supporting divisional to theater level priority intelligence requirements including preparation of intelligence assessments concerning domestic and foreign threats in a combined South Korean and U.S. forces collaborative environment. His leadership and intelligence officer responsibilities also spanned the tactical, operational, and strategic levels of military operations in support of current and future wartime operations plans in key developmental intelligence officer positions.

Mr. Reeves' military intelligence and strategic air defense experiences as a PATRIOT air defense system officer, supported worldwide operational deployments and missions. He is a Gulf War veteran, taught U.S. Army ROTC courses at St. Bonaventure University, and was employed by the MITRE Corporation in Korea before returning to his alma mater Sam Houston State University to earn his master's degree in Homeland Security Studies. Mr. Reeves has valued professional experience of the U.S. Army, joint service, the combined intelligence community, and he has personal experience in natural disaster recovery after Hurricane Harvey.