



Project
MUSE[®]
Scholarly journals online

Intelligence Preparation of the Battlespace: A Methodology for Homeland Security Intelligence Analysis

Jin Kim and William M. (Bill) Allard

Of the many challenges faced by the Department of Homeland Security and its intelligence enterprise, developing a common culture remains one of the most daunting tasks. Intelligence Preparation of the Battlespace (IPB) provides an analytical methodology that could cultivate a common analytical culture in the homeland security intelligence community, which is key to the community's effectiveness in thwarting a terrorist attack against the United States.

At hearings before the Select Committee on Intelligence of the U.S. Senate in 1992, General Paul Gorman, U.S. Army (Retired), stated that “intelligence remains information, no matter how adroitly collected, and no matter how well analyzed, until it is lodged between the ears of a decision maker.”¹ Intelligence with a purpose drives decision making. This intelligence enables policymakers to focus on tactics, strategies, and policies to prevent, respond to, and recover from terrorist attacks on the United States. Intelligence that drives decision making is a form of structured argumentation in which one makes a case for or against a tactic or policy “in the context of a framework that makes assumptions, reasoning, rationale, and evidence explicit and transparent.”² Intelligence Preparation of the Battlespace (IPB) is an ana-

Jin Kim is a Principal Analyst for CENTRA Technology, Inc, and currently supports strategic risk methodology and analysis for the U.S. Department of Homeland Security. Mr. Kim has worked in the intelligence community for over ten years—from tactical Army assignments to strategic assignments supporting the Department of Defense. He has a B.S. in General Engineering from the United States Military Academy and an M.A. in Security Studies from Georgetown University’s School of Foreign Service.

William M. (Bill) Allard is a Senior Analyst for CENTRA Technology, Inc, currently providing intelligence analytical support to U.S. Government client agencies. Mr. Allard is retired from the U.S. Marine Corps, has been a member of the National Intelligence Community for 27 years and is the former Open Source Intelligence Chief for the DHS-Intelligence and Analysis Directorate. He contributed to the development of DHS’s Open Source Intelligence Strategy and contributed to the formulation of the National Open Source Enterprise.

lytical methodology utilized by the U.S. Army and military professionals to reduce uncertainty about the adversary or threat.

Through methodical analysis and the aggregation of component steps, IPB provides a framework for intelligence professionals to continually update their situational awareness of the adversary or threat and build upon layers and layers of information. IPB provides a general framework for managing information, knowledge, and analysis to provide purposeful intelligence for planners and decision makers. In the military, the IPB framework allows the intelligence professional to reduce uncertainty about the threat, its capability, and its intentions, so that the commander can make decisions and apply plans (tactics, resources, communications, etc.) to achieve the mission's purpose. Applying IPB helps reduce policy risk by providing better situational understanding of the threat. In the fog of partial information and uncertainty, IPB provides a methodology to help extrapolate hypotheses.

After the attacks of September 11th and the creation of the Department of Homeland Security (DHS), the deficiency in homeland security intelligence (HSINT) has been clear and prominent. The National Commission on Terrorist Attacks upon the United States (commonly known as the 9/11 Commission) highlighted the need for the United States to bridge the divide between foreign and domestic intelligence.³ Breaking down the barrier between foreign and domestic intelligence is a critical mission for DHS—a mission that has additional hurdles beyond the normal fog of partial information, including structural and functional barriers from long-standing practices of not sharing information. Due to the added difficulties in HSINT, a common analytical methodology is needed. By applying the principles of Intelligence Preparation of the Battlespace, DHS can create intelligence with a purpose, focused on managing and mitigating risks to the U.S. homeland.

This paper will define IPB and the domain of risk analysis and risk mitigation within homeland security. It will also discuss the application of IPB to homeland security and intelligence. Additionally, this paper will discuss the importance of open source information and describe how open source information can help create a culture of homeland security intelligence analysis.

Intelligence Preparation of the Battlespace

If you know the enemy and yourself, you need not fear the result of a hundred battles. If you know yourself and not the enemy, for every victory gained you will also suffer a defeat. If you know neither yourself nor the enemy, you will succumb in every battle.

Sun Tzu - Art of War, c. 400 BC⁴

Intelligence Preparation of the Battlespace (IPB), previously known as Intelligence Preparation of the Battlefield, is a systematic and continuous methodology to conduct intelligence analysis with the purpose of providing

information about the threat or adversary in order to drive decision making. Derived from the Army and its Field Manual (FM 34-130, *Intelligence Preparation of the Battlefield*) and the Joint Publication for IPB (JP 2-01.3, *Joint Tactics, Techniques, and Procedures for Joint Intelligence Preparation of the Battlespace*), IPB is a methodology practiced at all echelons of the armed forces. The Army incorporated IPB as its systematic process for reducing uncertainty in adversary analysis with the publication of its Army Field Manual 34-130, *Intelligence Preparation of the Battlefield* in 1994.⁵ As other services adopted IPB, the term *battlespace* replaced *battlefield* to better represent all aspects of the environment.⁶ The Joint Staffs of the United States released the Joint Publication for IPB in 2000 with the new term, *battlespace*.⁷ Decomposed, IPB is a four step continuous process that builds on layers of analysis with each subsequent step: Define the Battlespace Environment, Describe the Battlespace Effects, Evaluate the Threat, and Determine Threat Courses of Action.

IPB, often misconstrued as merely terrain analysis, is an analytical methodology that is applicable to all environments. This inaccurate association likely stems from the fact that the terrain is the basis for all analysis in the domain of conventional warfare in the Army. Defining the environment refers to not only the land terrain, but also the sea, air and other physical dimensions, plus political, social, economic, and other human factors of the environment.⁸ This step requires rigor, as analysts must identify the components of the environment for further analysis. In the second step, describing the effects of the environment, analysts examine the impacts and effects of the environment—including friendly actions and activities—on generic threat capabilities. The third step of IPB, evaluating the threat, encompasses all the traditional processes of intelligence analysis, thus creating the knowledge base of threat capabilities and intentions. Adding the third layer to the analysis adjusts the model of the threat based upon the constraints of the environment. This leads to the fourth and final step, determining the adversary's courses of action or developing competing hypotheses. Based upon threat capabilities, intentions, and the constraints of the environment, analysts can develop hypotheses for what the adversary will do. In this step, adding evaluation measures such as feasibility, difficulty, or consequence will add more sophistication to the outcome. The basic methodology of IPB, if properly applied and tailored, can add a baseline methodological framework for analysis throughout the DHS Intelligence Enterprise.

Risk and the Department of Homeland Security

Risk-based decision making and risk-based approaches in decision making are terms frequently used to indicate that some systematic process that deals with uncertainties is being used to formulate policy options and assess their various distributional impacts and ramifications. Today an ever-increasing number of professionals and managers in industry, government, and academia are devoting a large portion of their time and resources to the task of improving their understanding and approach to risk-based decision making.⁹

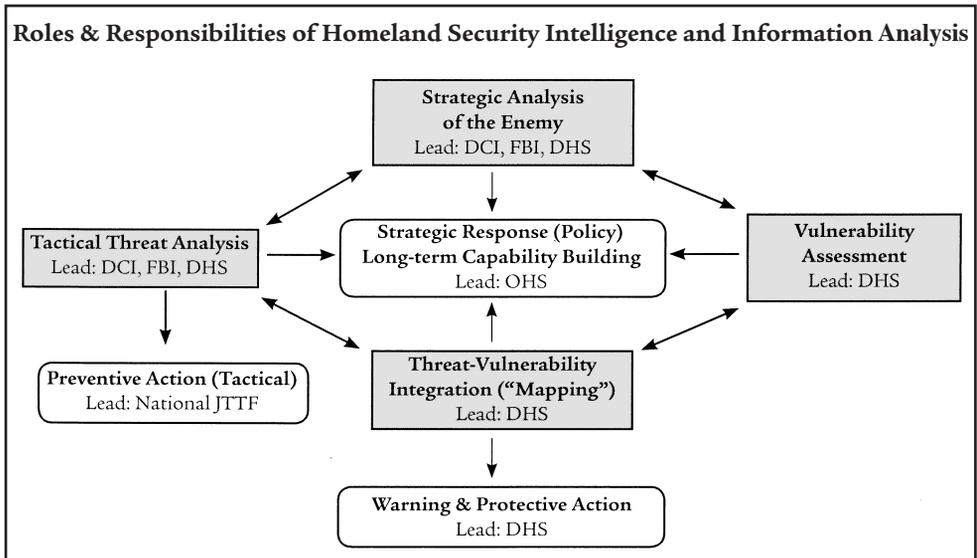
DHS, with its mission to protect the United States from terrorist acts, is implementing a concerted effort to insert risk into its decision making process to reduce uncertainty and optimize investment of its resources to protect the nation.¹⁰ DHS evaluates risk based upon three components: threat, vulnerability, and consequence, where threat is the probability of attack, vulnerability is the probability of that attack's success, and consequence is the magnitude of the damage given. Understanding consequence is "knowing yourself," whereas understanding threat and vulnerability is "knowing your enemy." Currently at DHS, the consequence component is the predominant understanding of risk; understandings of threat and vulnerability are less prevalent and not as mature. This gap in the development of risk components stems in part from the short history of the DHS itself—a history that initially did not have a true intelligence component.

Although bridging the gap between foreign and domestic intelligence was a main deficiency found by the 9/11 Commission and one of the main reasons for the creation of the department, DHS has only recently organized its own intelligence analysis capability, with the designation of a Chief Intelligence Officer in 2005.¹¹ Within the Office of Intelligence and Analysis, DHS is undergoing changes to adequately fulfill the roles and responsibilities for homeland security intelligence assigned to it by the National Strategy for Homeland Security, July 2002, focusing on threat and vulnerability.¹²

Interconnected with any structural reform of intelligence operations is the need for accompanying reform of the DHS's analytic culture. Currently this culture is a mix of the numerous intelligence and law enforcement cultures from which the analysts predominantly learned their craft. As Rob Johnston found in his ethnographic study, *Analytic Culture in the U.S. Intelligence Community*, "the methods and techniques of analysis are informal, idiosyncratic, unverifiable, and perhaps even unexplainable."¹³ Within DHS, what the analysts have brought with them are the practices and techniques of their former organizations. Applying IPB as a methodology for intelligence analysis at DHS will provide a general framework for rigorous analysis of threat and vulnerability that will further develop an integrated homeland security analytic culture that is inherently risk-based.

IPB Applications to Homeland Security

Homeland security involves the government and law enforcement at the federal, state, and local levels, as well as the private sector. Intelligence analysis in this collection of organizations goes against the grain of customary foreign intelligence analysis in the intelligence community. State and local law enforcement practice a bottom-up approach of gathering evidence in order to prosecute criminals, whereas the federal authorities use a top-down model.¹⁴ This disparity is evident within DHS alone. Headquarters and its Office of Intelligence and Analysis possess traditional intelligence analysis capabilities that are tied to the U.S. Intelligence Community, whereas other DHS components including Customs and Border Protection (CBP), Immigration and Customs Enforcement, Transportation Security Administra-



tion, and the Coast Guard, all have unique intelligence organizations and methods.¹⁵ Add state and local governments and law enforcement to the mix, and the homeland security intelligence community becomes diverse in background, as well as in tactics, techniques, and procedures.

Although the organizational growing pains within DHS and the broader intelligence community will continue as information stovepipes break and collaboration between entities increases, the opportunity to leverage the expertise and practices of state and local law enforcement along with the traditional foreign intelligence expertise of the federal agencies outweighs any hassles of reorganization. The demand for domestic intelligence capabilities has increased because “countering terrorism has increased the need to collect domestic intelligence, but threats to domestic security will increase even more in the future due to growth in technological capacities.”¹⁶ However, because there will be chaos in creating an increased domestic intelligence capability, there needs to be a standard analytical methodology to provide framework, guidance, and direction.

For the purposes of this paper, we divide homeland security intelligence analysis into three familiar levels: strategic, operational, and tactical. Strategic intelligence analysis supports national-level requirements and policies. The DHS headquarters Office of Intelligence and Analysis, with its national intelligence reach capabilities, is an office that operates within the scope of the strategic level of analysis. Operational intelligence analysis supports those organizations that have sub-domains of the homeland security mission, such as Customs and Border Protection, Transportation Security Administration, and Immigration and Customs Enforcement. Tactical intelligence analysis covers state and local law enforcement.

Step One: Define the Battlespace Environment

IPB’s first step, defining the battlespace environment, includes both geographic and non-geographic information and serves as the base layer for

analyzing the threat. This essential first step incorporates the mission of the intended decision maker or customer and provides boundaries for the analysis. The vision of the Department of Homeland Security Intelligence Enterprise is “to provide a decisive information advantage to the guardians of our homeland security.”¹⁷ At every level of the Homeland Security Intelligence Enterprise, intelligence analysts can define their battlespace environment based upon the mission of their own organization. One of the critical objectives of this step is to identify current intelligence gaps in order to define assumptions, constraints, and limitations for analysis and to focus the collection of information.

At the strategic level, homeland security intelligence analysis focuses on terrorist threats to the entire United States; therefore coordination with and leveraging of the US Intelligence Community is vital. Defining the battlespace environment at the operational level would be the task of such agencies as the Transportation Security Administration, which would be charged with identifying systems, networks, and environmental variables

[H]omeland security intelligence analysis focuses on terrorist threats to the entire United States . . .

that shape transportation security. Tactically, the analysis for step one would focus more narrowly on state and local information, such as detailed geographic information on cities and neighborhoods, demographics on criminal activity, or income levels. At all levels, the first step of IPB involves data collection and coordination with specialists to take into account all environmental variables that may affect terrorist operations.

Step Two: Describe the Battlespace Effects

Describing the battlespace effects builds on the characterization of the battlespace in step one and explains how it influences the threat entities in their behavior, tactics, and operations. This step also explains the effects upon the guardians of homeland security. By focusing on the general capabilities of the threat and the vulnerabilities of homeland security, this step helps the analyst identify the limitations and opportunities the battlespace environmental variables present to the potential threat and homeland security operations.¹⁸ The vulnerability analysis in this step is critical for development of the threat’s potential courses of action because it allows the analyst to step into the mind of the threat to homeland security. Therefore, this step in IPB requires coordination between intelligence analysts and operations analysts or planners. In DHS, this rapport is between infrastructure analysts and intelligence analysts; at CBP, the link is between customs and border protection agents and planners and the intelligence analysts; at the state and local level, the relationship is between law enforcement officers and the analysts. Building on the first step of IPB, describing the battlespace effects focuses the analyst on vulnerabilities and opportunities of both the threat and homeland security guardians.

Step Three: Evaluate the Threat

This step of IPB begins the classical process of intelligence analysis: searching and developing databases of information and applying historical models of the threat.¹⁹ For homeland security, it involves developing information flow in all directions to break down barriers to information sharing. Evaluating the threat is about managing information and knowledge to begin to connect the dots. Connecting the dots, however, begins with being able to manipulate the data and apply models or templates to infer gaps in the data. Doctrinal templates are models of the threat based upon ideal conditions for the threat to operate, incorporating historical data about how the threat has carried out past operations. Situation templates are an application of the doctrinal template to the current operating environment defined in steps one and two.

Step Four: Determine Threat Courses of Action

The final step of IPB is where the pieces of the puzzle come together, as analysts connect the dots and develop hypotheses of what the threat is going to do. Integrating the previous three steps of IPB, step four asks, “given what the threat normally prefers to do, and the effects of the specific environment in which he is operating now, what are his likely objectives and the courses of action available to him?”²⁰ Determining threat courses of action is where the art of intelligence analysis meets the science of the IPB methodology. Through corporate knowledge, each level of homeland security intelligence analysis brings a unique perspective. Organizational standards, processes, and knowledge only provide a baseline for this step; the creativity and critical thinking needed for intelligence analysis comes from the power of thinking analytically, a craft in its own right that demands practice and training.²¹ In this final step of IPB, homeland security intelligence can realize the full potential of analytic power by creating a unique homeland security intelligence culture that from the bottom up eliminates the traditional stovepipe and bureaucracy problem.

IPB and Mitigating Risk

For homeland security, risk is the product of threat, vulnerability, and consequence; different organizations use different variations of this in their risk methodology, but the general framework is consistent. IPB is a methodology that helps analysts reduce uncertainty about the threat and point out vulnerabilities in homeland security. Ultimately this methodology helps decision makers develop plans and allocate resources to prevent and protect the nation from terrorist attacks.²² As decision makers implement measures to prevent and protect, the continuous cycle of IPB enables analysts to update assessments and threat courses of action based upon the risk-reduction measures.

Open Source—Tapping into the Well

Because of the complex composition of homeland security, encompassing federal, state, and local governments, tribes and the private sector, sharing information poses many challenges. However, open source information is the common denominator among homeland security organizations at all levels. Homeland security intelligence's use of open source information is therefore vital to its culture and mission.

A strategy is a statement of fundamental values, highest priorities, and orientation toward the future, but it is an action document as well. For U.S. national intelligence, the time for change is now. There are no easy answers to the risks contemplated here, or the risks that might emerge. This strategy therefore accepts risk as intelligence's natural and permanent field of action and is based on the proposition that to preserve our security in a dangerous century, vigilance is not enough. U.S. national intelligence must do more.²³

When Ambassador Negroponte penned these words in the National Intelligence Strategy of the United States published in October 2005, almost certainly one of the areas where he intended change to be made was in the expanded use of a virtually untapped well of information, open source information. Open source information and subsequently open source intelligence (OSINT) has been a recognized resource for decades, and has frequently made significant contributions to the efforts of the United States Intelligence Community. Open source information differs from OSINT in that OSINT is the culmination of directed open source information gathering and focused analytical scrutiny. In broader terms, OSINT is no different than SIGINT, HUMINT or any other "INT," in that OSINT is information that has been deliberately discovered, discriminated, distilled, and disseminated to a select audience in order to address a specific question.²⁴

Open source information, however, has often been an afterthought in the minds of trained all-source intelligence analysts, their leaders, and their managers, particularly when faced with sifting through mounds of other intelligence-discipline material. In implementing a new strategy, the U.S. Intelligence Community has perhaps discovered the intrinsic value that open source information can play in the modern era, especially at a time when it finds itself squarely at odds with the fundamentally asymmetric problem of terrorism around the world and at home. Open source information venues, including traditional media sources, commercial or premium (pay) content, commercial geospatial data, professional and academic journals, and "grey literature," must be viewed as an entirely separate dimension in defining the contemporary battlespace. Grey literature is that information that is both legally and ethically available, but only from specialized channels or through direct local access. Generally, grey literature is considered information whose distribution is not controlled by commercial publishers, and/or that information that is not published, distributed, catalogued or acquired through commercial booksellers and subscription agencies. Grey literature includes working papers, pre-prints, technical reports and technical stan-

dards documents, dissertations and other academic papers, data sets, and commercial imagery.²⁵

Understanding the permissive environment wherein the adversary conducts his business is essential to understanding and validating potential threat information. In terms of terrorist pre-operational activity—that is, what terrorists do before they strike—we know that they and their supporters communicate in open forums on the Internet.²⁶ We know they elicit support, proselytize, recruit, and mine for data, and there is no

Homeland security intelligence's use of open source information is . . . vital to its culture and mission.

doubt some of that data is intended as targeting information for their own operations. Overlaying open source information in an Event Template scenario, trained open source analysts are able to understand what an adversary is capable of, what they have done, and possibly what they are currently doing. Based on validated open source information, analysts are then able to assess potential courses of action that the adversary may choose from or be in favor of. However, the accuracy of any open source assessment is based on two factors: the veracity of the data or source, and the ability of the analyst, which includes the ability to recognize and assess source credibility, discern factual data from opinion, understand the political light information is being cast in, if any, and assemble disparate pieces of information into cogent and concise format for immediate consumption.

The profusion of publicly available open source information today is abundant to the point of being inexhaustible. In terms of battlespace depth, identifying and exploiting specific targets in the sheer expanse of the Internet alone demands substantial investment in both human capital and financial resources. While federal, state, local, and tribal government administrations face the constant struggle to balance financial investment, trained OSINT exploitation and analysis assets are in short supply and will take years to cultivate.²⁷ For DHS, State Offices of Homeland Security, and the relatively new State and Local Fusion Centers (SLFC), the challenge is in balancing the targeting and collection of publicly available open source information pursuant to their respective missions without unlawfully intruding on civil liberties. Moreover, legal authorities for the collection of open source material may vary from state-to-state, county-to-county, and even jurisdiction-to-jurisdiction.

DHS and the Department of Justice (DOJ) both recognize the value of open source information. The daunting tasks before them are to utilize open source information as efficiently as possible and to train SLFC members in how information becomes intelligence. For instance, in defining Collection [of information] in the “*Intelligence Process*,” the DOJ states:

Collection is the gathering of the raw data needed to produce intelligence products. Data may be collected from many sources, including but not limited to public records, the Internet, confidential sources, incident reports, and periodicals.²⁸

The components of “raw information” contained in this Justice Department definition are almost exclusively based on open source resources. Competent open source exploitation and analytical resources remain deficient in the national intelligence apparatus. Unfortunately, despite the recognized importance of open source information, open source research habitually remains a function of less-experienced or lower-grade intelligence personnel. Too frequently, all-source analysts are tasked with performing their own open source research that often results in nothing more than “Google™” searches.

In an age where there is simply too much information, haphazardly surfing the Internet in hopes of bumping into a credible source based on a keyword search undermines the purposes for establishment of SLFCs in the first place. SLFCs are on the forefront of information availability for both the intelligence and law enforcement communities, as they are embedded in key locations throughout the United States and have their finger on the pulse of America. Having trained open source professionals working in these SLFCs is not only prudent, but crucial to the success of information collection and analysis.

While open source information and OSINT can uncover “golden nuggets” in an analyst’s search, these tools are of far more utility as a facilitator for other aspects of information and intelligence gathering. A truism spoken by Mr. Eliot Jardines, the first and current Assistant Deputy Director of National Intelligence for Open Source, (ADDNI-OS), is that open source should be considered as a first resource, rather than the last resort. Open source provides a framework for more focused examination. When properly used, open source information can provide responses to many questions before it becomes necessary to employ more expensive or more intrusive methods of information collection. Open source information exploitation is an essential aspect of the IPB process for identifying, monitoring, investigating, and mitigating threats to the homeland.

Conclusion

The benefits of IPB as a common analytic methodology are its applicability to the analysis of all categories of threats, and its simplicity. The stepwise process for IPB provides a framework that serves both junior and senior analysts. IPB provides a systematic process for disaggregating the problem and building solutions through a layered approach. IPB is not only for the U.S. Army or the Armed Services, but is a methodology that provides core pillars that DHS can customize to meet its needs. IPB is a proven methodology of the U.S. Armed Services because it is not exclusive only to intelligence professionals; it is a methodology applied at all echelons—from strategic and operational to troop leading—and in all functional areas—from operations to logistics. The Army teaches IPB to soldiers, non-commissioned officers, and officers at all specialty schools, including: infantry, armor, signal, transportation, finance, and chemical. Permeating the IPB methodology to those outside the intelligence profession at DHS will build common expectations and an analytic culture that crosses functional boundaries.

IPB provides a core framework and approach that is compatible with other more focused analytical approaches. Analysts can utilize other methodologies under the IPB framework. Currently, DHS is developing a methodology for a new radicalization project that phases analysis and assessments by state or region through the State and Local Fusion Centers by: assessing national level intelligence and open sources, collaborating with the FBI and other Federal partners, and collaborating with state and local law enforcement.²⁹ Through this process, if DHS uses IPB as the common methodology, it would provide common expectations for assessment. Utilizing IPB with the radicalization project would produce multiple hypotheses, create a focus for collection, and provide a purpose for decision makers and planners to counter the threat. DHS is moving in the direction of developing a common culture; implementing an analytic methodology like IPB would provide both the top-down and bottom-up approach necessary.

IPB will help to define and develop the homeland security intelligence analysis culture, an aspect vital to shaping the nation's efforts to protect it from terrorist attacks. The strength of the IPB methodology is that it only provides a framework, while also allowing analysts the freedom to be creative and innovative. IPB also helps decision makers take ownership of intelligence and helps them to focus intelligence to support the mission. In this sense, IPB is more about developing a common understanding or situational awareness between the intelligence analyst and the operator. Homeland security intelligence features many challenges because of the inherent difficulties in coordination and collaboration in the mission among many entities at all levels of government. Many top down policies are currently being implemented within homeland security intelligence to define a new culture. However, culture is about people. IPB will help develop a culture of homeland security intelligence analysts from the bottom up in conjunction with the definitions coming from the top down. The immense potential in homeland security intelligence comes from the diversity of its people—operators and analysts—that represent the breadth and depth of government at all levels, the private sector, and academia. The collaborative potential, if properly harnessed, will provide the ultimate support to the mission of homeland security.

Notes

¹ Statement of General Paul Goring. Hearings Before Select Committee on Intelligence of the U.S. Senate, S. 2198 and S. 421 (Washington: 1992), 262.

² Jermano, Jill. "Introduction to Structured Argumentation". *Genoa Technical Note*. Veridian Corp: Arlington, VA, May 2002. [Genoa was a Defense Advanced Research Projects Agency (DARPA) funded program.]

³ *The Final Report of the National Commission on Terrorist Attacks Upon the United States*. Washington: U.S. Government Printing Office, 2004. 399–428, <http://www.gpoaccess.gov/911/pdf/fullreport.pdf>.

⁴ Sun Tzu. "Part III: Attack by Stratagem, Verse 18." In *The Art of War*, translation and critical notes by Lionel Giles, 32. London: British Museum, 1910.

⁵ Field Manual 34–130, *Intelligence Preparation of the Battlefield*. Headquarters, Department of

the Army: Washington, DC, July 8, 1994, <https://atiam.train.army.mil/soldierPortal/atia/adlsc/view/public/11681-1/fm/34-130/toc.htm>.

⁶ *Department of Defense Dictionary of Military Terms*, April 12, 2001, <http://www.dtic.mil/doctrine/jel/doddict/data/b/00691.html>.

⁷ *Joint Tactics, Techniques, and Procedures for Joint Intelligence Preparation of the Battlespace*. Joint Chiefs of Staff: Washington, DC, 2000, http://www.dtic.mil/doctrine/jel/new_pubs/jp2_01_3.pdf.

⁸ Satterly, Lt. Col. Mark T., USAF, et. al. "Intelligence Preparation of the Battlespace — An Airman's Introduction." *Air and Space Power Journal*, 26 July 1999, <http://www.airpower.maxwell.af.mil/airchronicles/cc/Satterly.html>.

⁹ Haimes, Yacov Y. *Risk Modeling, Assessment, and Management*. John Wiley & Sons, Inc.: New Jersey, 2004, 3.

¹⁰ Chertoff, Michael. "Remarks by Homeland Security Secretary Michael Chertoff to the Sacramento Metro Chamber of Commerce, April 23, 2007." DHS Press Release. http://www.dhs.gov/xnews/speeches/sp_1177426083887.shtm.

¹¹ Mass, Todd. "Homeland Security Intelligence: Preceptions, Statutory Definitions, and Approaches." *CRS Report for Congress*. Congressional Research Service: The Library of Congress, August 18, 2006, 8.

¹² *The National Security for Homeland Security*. Homeland Security Council: Washington, DC, July 2002, p. 16, http://www.dhs.gov/xlibrary/assets/nat_strat_hls.pdf.

¹³ Johnston, Rob. *Analytic Culture in the U.S. Intelligence Community*. Center for the Study of Intelligence: Washington, DC, 2005, 18.

¹⁴ Mass, 4.

¹⁵ Department of Homeland Security Organizational Chart, April 2007. Department of Homeland Security Website. http://www.dhs.gov/xlibrary/assets/DHS_OrgChart.pdf.

¹⁶ Marrin, Stephen. "Homeland Security Intelligence: Just the Beginning." Homeland Security Institute Website. November 2003, <http://www.homelandsecurity.org/journal/Articles/marrin.html>.

¹⁷ *DHS Intelligence Enterprise Strategic Plan*. Department of Homeland Security: Washington, DC, January 3, 2006. <http://www.fas.org/irp/agency/dhs/stratplan.pdf>.

¹⁸ Field Manual 34–130, *Intelligence Preparation of the Battlefield*. Headquarters, Department of the Army: Washington, DC, July 81994, 1–2.

¹⁹ *Ibid*, 1–3.

²⁰ *Ibid*, 1–3.

²¹ Heuer, Jr., Richards J. *Psychology of Intelligence Analysis*. Center for the Study of Intelligence: Central Intelligence Agency, 1999, 2.

²² Chertoff, Michael. "DHS Secretary Michael Chertoff, Prepared Remarks at George Washington University Homeland Security Policy Institute (Mar. 16, 2005)." DHS Press Release. http://www.dhs.gov/xnews/speeches/speech_0245.shtm.

²³ *National Intelligence Strategy of the United States of America*. October 2005. Federation of American Scientists Website. <http://www.fas.org/irp/offdocs/nis.pdf>. 2.

²⁴ *NATO Open Source Intelligence Handbook*, November 2001. Open Source Solutions Website. http://www.oss.net/dynamaster/file_archive/030201/ca5fb66734f540fbb4f8f6ef759b258c/NATO%20OSINT%20Handbook%20v1.2%20-%20Jan%202002.pdf. 2-3.

²⁵ *Ibid*, 8–9.

²⁶ "*www.terror.net, How the Modern Terrorist Uses the Internet.*" United States Institute of Peace Website, March 2004. <http://www.usip.org/pubs/specialreports/sr116.pdf>. 5.

²⁷ Generally, DHS acknowledges Native American tribal governments as integral participants in a variety of homeland security issues including law enforcement, border security, immigration, and counternarcotics, among others. In fact, U.S. Territorial governments, (Guam, Puerto Rico, etc.), are also generally included in Homeland Security decision making processes.

²⁸ *Fusion Center Guidelines-Developing and Sharing Information in a New Era*, August 2006. Department of Justice, Office of Justice Programs, Information Technology Initiatives Website. http://it.ojp.gov/documents/fusion_center_guidelines_law_enforcement.pdf. 20.

²⁹ Allen, Charles E. "Statement of Assistant Secretary Charles E. Allen Before the Subcom-

mittee on Intelligence, Information Sharing, and Terrorism Risk Assessment of the House Homeland Security Committee (March 14, 2007),” 5, <http://hsc.house.gov/SiteDocuments/20070314172258-47553.pdf>.