Introduction

In the post-9/11 era, the homeland security professional has developed into a major intelligence customer. Most federal counterterrorism, cybersecurity, and other homeland security professionals understand the importance of intelligence in helping them do their jobs. But the homeland security enterprise includes hundreds of thousands of state and local government and private-sector professionals who are still learning how to use intelligence, how to have it tailored to meet their needs, and how to ensure that such intelligence is delivered to them in a timely fashion. This book is designed to help these professionals understand, clarify, and shape the role of intelligence in the two most dynamic dimensions of homeland security: counterterrorism and cybersecurity.

As a senior Central Intelligence Agency (CIA) officer, I spent more than three decades producing and delivering intelligence to the major national security policy actors, the intelligence customers of the pre-9/11 era—the president, his senior advisors, and the National Security Council (NSC) staff; the civilian and military leadership at the Pentagon; and the U.S. diplomatic corps at home and abroad. At NSC working group meetings, I could look around the table and predict with high accuracy exactly how the various interagency participants would react to any particular piece of new intelligence I put before them. For example, the Joint Chiefs of Staff (JCS) two-star general would have a greater interest in intelligence regarding the discovery that China had developed a new type of surface-to-air missile than would the State Department assistant secretary and the NSC senior advisor sitting on either side of him. In turn, the JCS representative would be less interested in the latest coup plots in remote areas where the United States had little or no presence.

In the months after 9/11, the participants around the table changed. I began going to meetings with representatives from the Federal Emergency Management Agency (FEMA), Customs, and other nontraditional national security customers. I could no longer gauge the specific nature of their intelligence needs,

much less predict how they would respond to new intelligence. But these dynamics were even more difficult for the new players at the NSC table. I recall one meeting chaired by a new NSC director where we were discussing the adequacy of emergency U.S. cash stockpiles. After everyone was seated, he began the meeting by asking if anyone knew how the NSC process was supposed to work, because he had just arrived in his position after a 20-year career as a firefighter in a major U.S. city. At that moment, I knew the world of U.S. intelligence in support of policymakers had changed in the most profound and fundamental way.

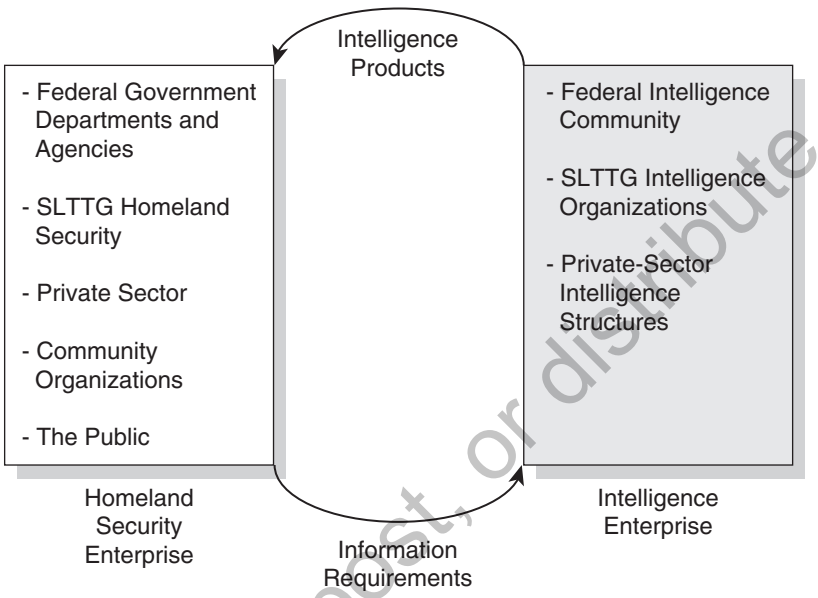
After I retired from the CIA in early 2006, Charlie Allen, the senior intelligence officer at the Department of Homeland Security (DHS) and a longtime friend and colleague at the CIA, asked me to become his unofficial intelligence representative to the New York State Homeland Security advisor in Albany, New York. For the next 2 1/2 years, I worked with Brig. Gen. David Sheppard, director of the New York State Office of Homeland Security, to help ramp up his homeland security and counterterrorism programs. Along the way, I met dozens, if not hundreds, of professionals in state and local law enforcement, National Guard, firefighting, emergency services, cybersecurity, critical infrastructure protection, and many other homeland security fields. With the exception of the National Guard and law enforcement officers, most of these professionals initially had only a cinematic perspective of the intelligence profession and product, and almost none of them realized they were intelligence customers. This situation is changing rapidly, and I hope this book will facilitate the learning process in undergraduate and graduate homeland security courses, as well as in government and corporate training courses for intelligence officers and other homeland security professionals.

SCOPE OF THE BOOK

After a brief introduction to the homeland security and intelligence fields, this book systematically examines intelligence support to major homeland security actors in the federal government; state, local, tribal, and territorial (SLTT) governments; the private sector; community organizations; and even the public (see Figure I.1).

Specifically, for each homeland security mission, the book first identifies the major intelligence customers and their role in accomplishing the mission. It then identifies the intelligence organization that provides intelligence support to this customer. It then presents actual (unclassified or declassified) intelligence documents to demonstrate how intelligence can help that customer do his or her job. Finally, real-world cases and fictional scenarios (often based

Figure I.1 ▶ Intelligence Support to Homeland Security: The Enterprise



loosely on actual cases) are used to provide hands-on perspective of what an intelligence product tailored to a customer's information needs looks like.

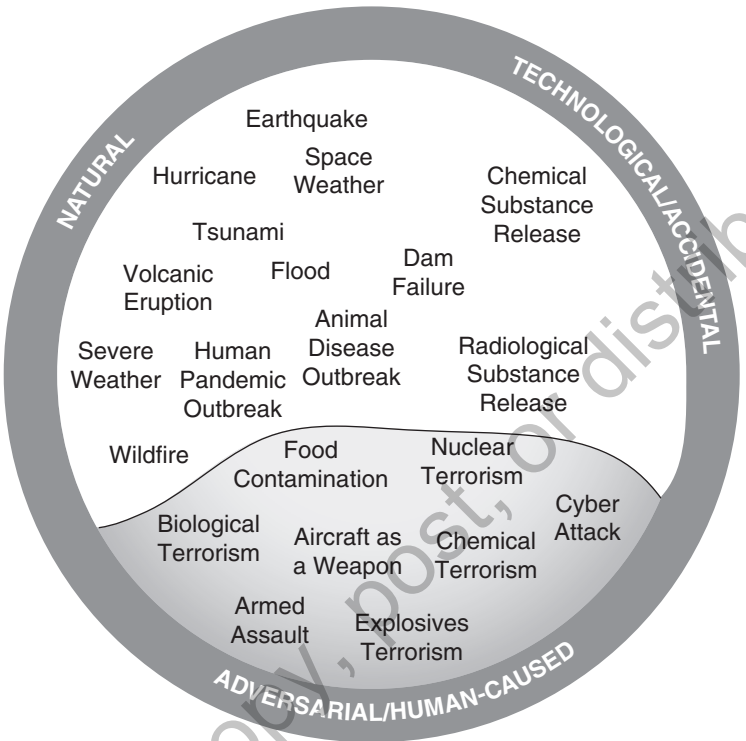
By the end of this book, the student or professional will have a thorough and in-depth picture of who in the intelligence enterprise is providing support to each homeland security customer and what that intelligence support should look like.

It is worth noting what this book is not. It is not a textbook on U.S. intelligence. We do look at today's U.S. Intelligence Community, producer–consumer relations, and the content of intelligence reports, but the book does not address the complex, internal dynamics of intelligence collection and analysis.[1] It also is not a critique of the existing structures or organizations, with suggestions on how they could be made better. But where there are widespread criticisms, those will be reported.

Finally, the scope of this book is limited to what DHS terms "adversarial/human-caused threats" (see Figure I.2), particularly terrorism and cyber attacks, the two most dynamic areas of homeland security, where intelligence plays a dominant role in meeting and defeating threats.

As such, it does not address threats that are not susceptible to intelligence analysis. For example, frequency and hazard analyses, rather than intelligence,

Figure I.2 ▶ A Focus on Adversarial/Human-Caused Threats



are used to anticipate natural disasters and technological/accidental events. Similarly, because the book attempts to cover thoroughly the newer counterterrorism dimension of our comprehensive transborder security apparatus, it does not dwell at length on the more traditional elements of law enforcement intelligence efforts that support DHS programs to control broader, long-established criminal threats at the border, such as drug, human, and other smuggling, as well as nationwide efforts to reduce immigration violations.

Part I: U.S. Homeland Security and U.S. Intelligence

In Chapter 1, I begin with the various U.S. Government definitions of *homeland security* and then focus on emerging threats in the terrorism and cyber areas. I use federal government documents to examine the breadth and

depth of our national homeland security effort, including its functions, organizations, participants, and risk management methodology. Before we can examine what federal, state, and local government agencies actually do to promote homeland security, we must look at what they want to do and what by law they are compelled to do. That means looking at their overall strategies and seeing how those are translated to specific policies, as well as how those policies become specific mission programs. Finally, we look at how those programs become actions.

At the federal level, I examine the U.S. National Security Strategy and the Quadrennial Homeland Security Review. Taken together, they portray a consistent intent on the part of the past two presidents and their administrations to give their highest priority in funding and management focus to homeland security. The Obama Administration has adopted a "whole-of-the-nation" approach that spells out the roles of the various homeland security players in a series of functional frameworks. These and other homeland security policy documents also introduce the risk management process that is central to homeland security resource allocation and decision making, and the paradigm of Prevent, Protect, Mitigate, Respond, and Recover missions that is used in this book as a way of functionally categorizing the operational activities within homeland security. We will see that, unlike most national security issues, large segments of homeland security responsibilities are state, local, and private-sector mandates, especially in the areas of critical infrastructure protection, mitigation, emergency response, and economic recovery. For example, our police, fire, and emergency medical services are primarily state and local organizations, and so state and local leaders have final control over their policies and resources. To further complicate matters, the areas emphasized by each state are highly dependent on the threats (adversarial, accidental, and natural) each faces.

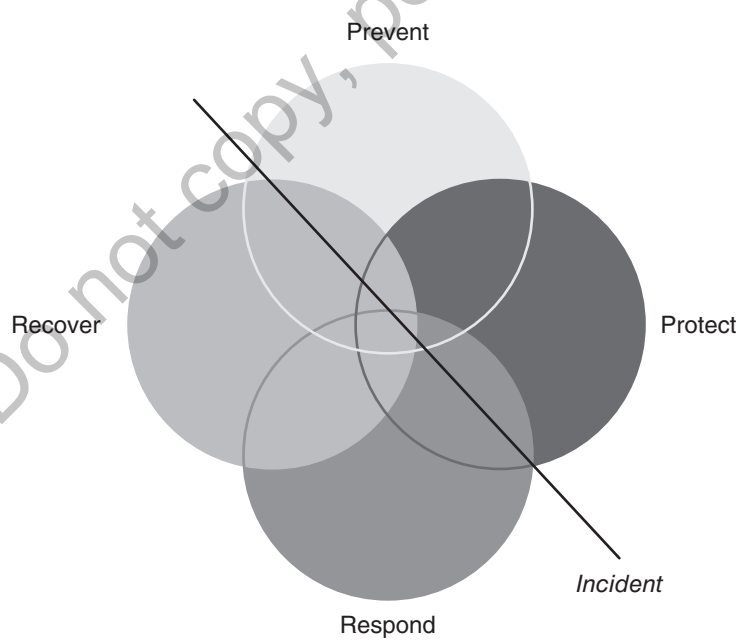
In Chapter 2, I introduce U.S. intelligence, beginning with a look at alternative definitions of intelligence that settle on the deceptively simple construct, "intelligence is the timely flow of analyzed information." The intelligence cycle is introduced, as are the human and technical collection disciplines. The chapter's major focus is on today's (post-9/11) intelligence enterprise. At the federal level, we will see that the emerging threats posed by terrorism and cyber adversaries led to a restructuring and expansion of the federal Intelligence Community, in large part to support DHS and federal law enforcement efforts. An even more radical picture of new intelligence capabilities presents itself at the state and local government level and within the private sector. In addition

to reorienting existing modest intelligence capabilities, large new intelligence organizations are now in place to support homeland security programs beyond the Beltway.

In Chapter 3, I start bringing the homeland security and intelligence worlds together by tracing the demand for intelligence support and the development, delivery, and use of that product. Our vehicle for putting content on these producer–consumer dynamics is a declassified intelligence product on the terrorism threat that was prepared by the National Intelligence Council in 2006 for use by the president and his most senior advisors (the customer set) as they grappled with establishing a new counterterrorism strategy. In this ideal example, we can see how intelligence judgments framed the national strategy.

Intelligence support to the Prevent, Protect, Mitigate,[2] Respond, and Recover missions are covered in the remainder of the book (see Figure I.3).

Figure I.3 ▶ The Homeland Security and Emergency Management Continuum



In Figure I.3, the straight line represents a major incident such as a terrorist or cyber attack. Two sets of activities—those aimed at preventing an attack and those that protect likely targets—occur before (above) the attack. There are some actions in these two missions that occur after the event, primarily a "lessons learned" segment. On the other hand, while most of the actual "respond" and "recover" actions take place after (below) the event, a considerable amount of planning, training, and exercising to prepare for such attacks occurs before the incident.

Using the formal "frameworks" developed by DHS for each of these four homeland security mission areas, we identify the federal actors, their specific responsibilities and programs, and the source and role of intelligence in helping them meet their goals. This section is followed by an analogous discussion of the other participants in our "whole-of-the-nation" effort—SLTT governments, the private sector, community organizations, and even the public (as appropriate). To ensure that students understand the structure and content of intelligence, I utilize, whenever possible, actual intelligence documents produced to support the various mission actors, as well as fictional scenarios.

The bulk of the discussion of homeland security programs and examples of intelligence products in this book focuses on terrorism, but Chapter 8 is devoted entirely to cybersecurity programs and the intelligence needed to make them effective. The federal government treats the cyber realm as an element of the "protect" critical infrastructure mission, but differences in the fundamental characteristics of the terrorism and cyber threat streams are so significant that a hybrid presentational approach is needed.

Part II: Taking the Offensive:
Intelligence Support to the PREVENT Mission

Intelligence is critical to the offensive ("prevent") dimension of counterterrorism. Starting with traditional national security actors—military, diplomatic, law enforcement, and covert action (CIA)—we explore U.S. counterterrorism efforts overseas (Chapter 4). Moving closer to home, the Federal Bureau of Investigation (FBI) takes the domestic lead in preventing a terrorist attack, and it organizes the federal, state, and local law enforcement team effort through the Joint Terrorism Task Force structure (Chapter 5). Most of the federal actors are longtime intelligence consumers, and all have their own significant

intelligence subcomponents that tailor the intelligence they need to pursue their missions. The major restructuring of the federal Intelligence Community in 2004 was designed to ensure comprehensive intelligence support to these federal counterterrorism warriors, law enforcement officers, diplomats, and other homeland security officials. Since 9/11, state and local fusion centers were created and designated as focal points connecting the federal Intelligence Community to new or expanded state and local intelligence units. Fusion centers play many roles, but one of the most important is supporting the all-hands approach to preventing an imminent attack, such as the search for the Boston Marathon bombers.

Part III: Securing the Homeland:
Intelligence Support to the PROTECT Mission

The Defense Department is responsible for protecting the country from an attack by foreign military forces—the central element of its homeland defense mission. This military function is normally deemed distinct from homeland security, with the exception of securing the airspace over the United States, which is considered both a homeland defense and a homeland security function. The Defense Department has additional duties in the homeland security Protect mission, such as hardening defense installations and industry, as well as providing specialized assets to support civilian authorities (Chapter 6).

DHS's Protect mission consists of three major dimensions. In Chapter 6, we explore DHS's dominant role in protecting the nation's borders. DHS inherited and restructured several large federal organizations such as the U.S. Coast Guard and the Border Patrol, which protect our international boundaries. Once again, these major DHS components are longtime producers and consumers of the intelligence they need to do their jobs.

DHS also has been assigned the lead federal role in conceptualizing and then coordinating the implementation of a plan for protecting our critical infrastructure, including the cyber dimension (Chapter 7). State and local governments also have a coordinating role, but we will see that the private sector carries the major responsibility for protecting its own facilities, personnel, and networks, and therefore is a legitimate customer for intelligence products, especially those that examine terrorist practices in attacking private-sector facilities and cybernetworks. For example, the hotel industry in New York City needs to understand the November 2008 attack in Mumbai to gain insights

into how their own hotels could be targeted—and thus plan how to better protect them.

As noted above, Chapter 8 is devoted to cybersecurity, clearly the fastest-growing and most quickly changing homeland security threat. Because of this growth and change, the cyber challenge now rivals and possibly surpasses terrorism as the primary homeland security threat requiring intelligence support to ensure our well-being. The president himself, in his 2013 State of the Union Address, called for a massive, whole-of-the-nation effort to protect our cyber assets.

Part IV: Preparing for the Aftermath: Intelligence Support to the RESPOND and RECOVER Missions

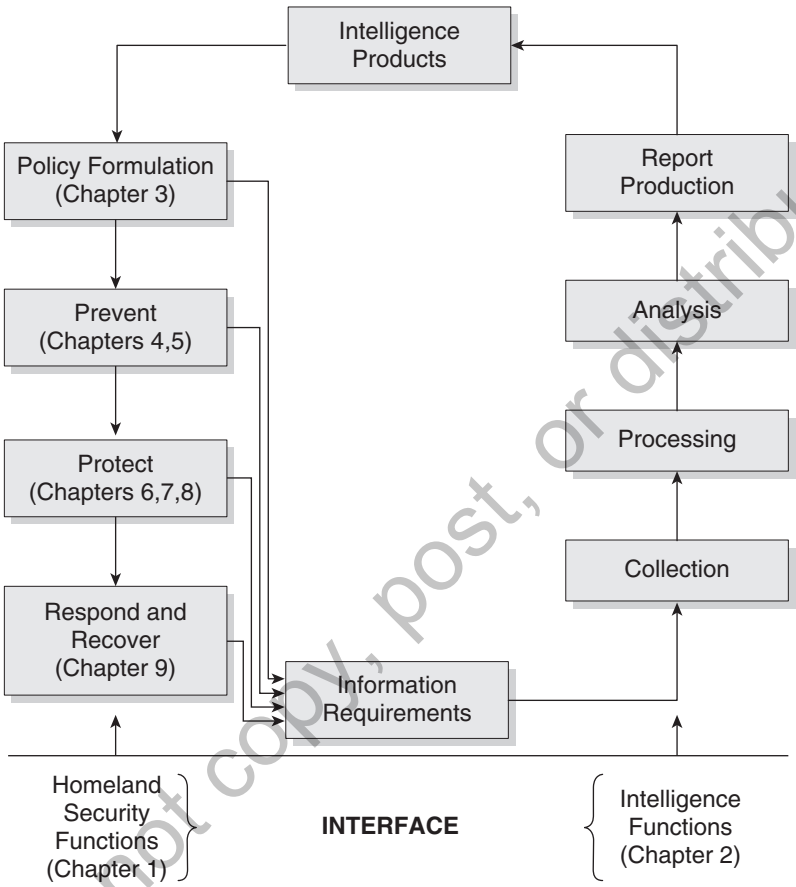
There is a long history of governmental, private, and public-sector analysis, training, and investment in preparing to respond to and recover from natural disasters. FEMA has the lead federal role in responding to a terrorist attack, as well as to the more familiar natural disasters and accidental man-made incidents. It provides training, funding, and guidance, but the vast majority of first responders are at the state and local level, and we will hone in on these policemen, firemen, and emergency medical practitioners. In some cases, responding to a terrorist incident (bombing, shooting, or fire) is similar to responding to a natural disaster or other man-made event, but there can be substantial differences, especially if a terrorist group uses weapons of mass destruction such as chemical, biological, nuclear, radiological, or high-yield explosive weapons, or if first responders are actually targeted by the terrorists. First responders need intelligence information on terrorist training, techniques, and patterns of behavior to improve their situational awareness (Chapter 9).

Intelligence also plays a role in helping customers take actions now to lessen the impact of a successful attack, and to prepare to respond to and recover from an attack. The risk management process identifies cost-effective investments and training programs that, if implemented before an attack, can save lives, reduce physical damage, and speed economic recovery. Intelligence is central to the homeland security risk management process.

The plan of the book is summarized in Figure I.4.

The book concludes with a short, bottom-line assessment of what works and what major challenges remain in the maturation of homeland security intelligence.

Figure I.4 ▶ Intelligence Support to Homeland Security: Functions



NOTES

1. See Mark Lowenthal, *Intelligence: From Secrets to Policy,* 5th ed. (Thousand Oaks, CA: CQ Press/Sage, 2012).

2. Mitigation actions are common to, and actually weave throughout, all homeland security missions. The risk-management process often results in mitigation actions being taken to improve resiliency in the other four missions. Mitigation is not treated as a separate mission in this book.