



The Mosaic of Homeland Security Intelligence

As Seen Through the Oklahoma City and 9/11 Attacks

COL. James F. Chastain, USA (Ret.)

Colonel Chastain has served nearly three decades in the US Army and Intelligence Community. He is presently the course chair in the CORE Professional Intelligence Program at the DHS Office of Intelligence & Analysis Intelligence Training Academy, among other training assignments at DHS. While still in uniform, he served in leadership roles in DIA and NSA. He is a doctoral candidate at Vanderbilt University.

Jeffrey Toobin's *Homegrown: Timothy McVeigh and the Rise of Right-Wing Extremism* and Lawrence Wright's *The Looming Tower: Al-Qaeda and the Road to 9/11* examine terrorist attacks that emerged from very different ideological and organizational environments. Toobin reconstructs the radicalization and preparations of Timothy McVeigh and Terry Nichols before the 1995 Oklahoma City bombing. Wright traces the development of al-Qaeda, the efforts of US officials to understand it, and the intelligence failures preceding September 11, 2001. Read together, the books can be

counted among those published, including the *9/11 Commission Report*, in the years since these events occurred to demonstrate that terrorism succeeds not only through fanaticism and operational skill, but also through a variety of information gaps between institutions meant to prevent them. McVeigh exploited the limited national attention then devoted to domestic extremism, while al-Qaeda benefited from the separation of foreign intelligence, immigration administration, domestic law enforcement, and local public safety.

All statements of fact, opinion, or analysis expressed are those of the author and do not reflect the official positions or views of the US government. Nothing in the contents should be construed as asserting or implying US government authentication of information or endorsement of the author's views.

An “Intermestic” Challenge

The shared lesson of the literature is that protecting the United States requires a homeland-security enterprise capable of joining international intelligence with federal, state, local, tribal, and territorial action.

The central problem may be described as “intermestic”—a problem that simultaneously involves international and domestic factors, e.g, leadership, financing, ideology, communications, or training may originate abroad, while its operatives, preparations, targets, consequences, and necessary government responses appear inside the United States.^a

The attacks on September 11, 2001 were plainly intermestic in character. Al-Qaeda’s senior leadership and training infrastructure were overseas, but the hijackers entered, lived in, and carried out their preparations in US communities. They opened financial accounts, obtained identification, attended flight schools, drove on US highways, and boarded domestic aircraft.

Oklahoma City was more domestically rooted, yet McVeigh and

Nichols also moved across jurisdictional boundaries, acquired materials through ordinary commerce, used storage and transportation systems, and, like al-Qaeda’s operatives, turned extremist belief into a national catastrophe. Both cases reveal that bureaucratic boundaries can become operational opportunities for attackers.

Homegrown is most persuasive when Toobin shows that McVeigh did not move directly from political anger to mass murder. His fixation on Waco, Ruby Ridge, antigovernment conspiracy theories, separatist ideas, and *The Turner Diaries* became part of a progression from grievance to intent, preparation, and action.^b Terry Nichols mattered because he helped provide practical capacity through materials, storage, transportation, and trusted assistance. Toobin, therefore, complicates the “lone wolf” label. Even when one attacker dominates a plot, associates may supply the capabilities that make violence possible.

The book’s broader warning is that intelligence must distinguish constitutionally protected belief from observable mobilization toward violence. Extreme or offensive political opinions are not sufficient grounds for government

investigation. Target selection, acquisition of unusual materials, operational concealment, reconnaissance, logistical coordination, threats, and criminal facilitation are more meaningful indicators. Toobin’s reconstruction of McVeigh’s thinking and conduct shows that domestic terrorism is often preceded by a progression of behaviors that may become visible across different communities, businesses, jurisdictions, and government records.

The Looming Tower offers the corresponding international story.^c Wright’s narrative follows Osama bin Laden, Ayman al-Zawahiri, Saudi intelligence chief Prince Turki al-Faisal, and FBI counterterrorism official John O’Neill. Its great strength is showing how ideology, personalities, terrorist sanctuary, organizational rivalry, and failed information sharing converged before September 11.

Wright makes those failures vivid through individuals, especially O’Neill, but the deeper problem was structural: information was collected by separate organizations without a manager consistently responsible for integrating foreign and domestic leads into joint action.

a. The term “intermestic” originated with Bayless Manning, a former president of the Council of Foreign Relations (1971–77), who introduced it in a *Foreign Affairs* article in January 1, 1977: “The Congress, the Executive, and Intermestic Affairs, Three Proposals”—per ChatGPT. The word was often used by scholars, including Joseph Nye, in the 1980s and 1990s and beyond. (Among the latter is Donald M. Snow in *National Security for New Era: Globalization and Geopolitics* (Pearson/Longman, 2004).

b. Jeffrey Toobin, *Homegrown: Timothy McVeigh and the Rise of Right-Wing Extremism* (Simon & Schuster, 2023).

c. Lawrence Wright, *The Looming Tower: Al-Qaeda and the Road to 9/11* (Knopf, 2006).

Missed Opportunities

The pre-attack record contained evidence of significant warning opportunities. Intelligence agencies knew or could have known that Khalid al-Mihdhar and Nawaf al-Hazmi were connected to an important al-Qaeda meeting and had traveled to the United States, yet their identifying information was not promptly developed and transmitted for effective watch-listing. During the summer of 2001, threat reporting became intense, but domestic agencies often lacked clear direction. Late leads concerning Mihdhar, Hazmi, and Zacarias Moussaoui were not connected effectively to the broader strategic warnings reaching senior leaders.^a

Immigration violations and routine police encounters demonstrate how the intermestic plot repeatedly touched domestic systems. Mohamed Atta exceeded a period of authorized admission and later lacked the proper vocational-school status; Ziad Jarrah attended school without properly adjusting his immigration status; Hani Hanjour failed to enroll after entering as a student; and Satam al-Suqami and Nawaf al-Hazmi remained beyond their authorized admissions. Most of the later-arriving “muscle” hijackers, however, remained legally admitted through September 11.

The lesson is not that every hijacker was an easily removable visa violator, but that immigration, travel, intelligence, and law-enforcement records were not integrated well enough to distinguish ordinary noncompliance from activity associated with a known terrorist network.

Several hijackers also encountered state or local police for speeding, licensing, or other driving-related matters. Nawaf al-Hazmi received a speeding ticket in Oklahoma, Mohamed Atta was stopped in Florida, and Ziad Jarrah received a speeding ticket in Maryland shortly before the attacks. The officers involved could not reasonably infer terrorism from an ordinary traffic violation when no national-security alert existed, but the hijackers' collective actions could have been identified and connected to immigration status and other violations of law through a simple integration of local and federal databases.

The missed opportunity was systemic, not principally the fault of the officer at the roadside. Foreign intelligence had to identify the person, federal systems had to make that information discoverable, and officers needed lawful instructions for confirming identity and notifying the appropriate agency.

Local information also had to travel upward so that an apparently minor encounter could be compared with national and international reporting.^b

The investigation of the Oklahoma City bombing provides the contrasting example of successful integration. Oklahoma Highway Patrol Trooper Charlie Hanger stopped McVeigh because his vehicle lacked a license plate and arrested him after discovering a weapons violation. The arrest took place 90 minutes after the bombing; the already imprisoned McVeigh was found two days later. Separately, federal investigators reconstructed the Ryder truck, traced its identifying number to a Kansas rental business, and used witness information to identify McVeigh. The traffic-stop record and federal investigation then converged. Of course, that success did not prevent the deaths of 168 people that April 19th morning in 1995, but it demonstrated the power of professional local policing, accurate records, private-sector cooperation, forensic expertise, and federal investigative reach.^c

The case embodies a central theme of both books: no one participant can possess the whole picture, but a connected system can transform fragments into actionable

a. National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States* (W.W. Norton & Company, 2004).

b. *The 9/11 Commission Report*.

c. That post-bombing investigation is detailed in the FBI's public website: <https://www.fbi.gov/history/cases-and-criminals/oklahoma-city-bombing>.

The Mosaic of Homeland Security Intelligence

knowledge. State and local officers see people and conduct in their jurisdictions. Federal investigators possess interstate authority, advanced forensic capabilities, national databases, and access to intelligence from across the country. International intelligence organizations can identify foreign networks, training locations, travel patterns, facilitators, and strategic intent. Security depends on combining these different forms of knowledge.

Enter DHS I&A

The post-September 11 response sought to build such a system before the next attack. The deeper problem was not merely a failure to “connect the dots,” but the absence of firmly assigned responsibility across the foreign-domestic divide and the difference between occasional cooperation and genuine joint action. The United States therefore strengthened strategic intelligence, networked information sharing, homeland defense, and management mechanisms capable of drawing information from across government and assigning responsibilities among agencies.

The Department of Homeland Security became a central institution in that evolving enterprise, and its Office of Intelligence and Analysis, commonly known as DHS I&A, occupies a particularly important position.^a I&A shares

intelligence and analysis with operators and decisionmakers so they can identify and mitigate threats to the homeland. It also helps integrate intelligence into operations across DHS components and serves as a bridge among the national Intelligence Community, DHS operational agencies, federal partners, and state, local, tribal, territorial, and private-sector organizations.

That bridging role is essential because national agencies and local governments see different portions of the threat. International and national intelligence organizations can identify hostile networks, overseas travel, communications, financing, cyber activity, terrorist tradecraft, and strategic intent. State and local officials encounter suspicious behavior, traffic stops, emergency calls, licensing records, infrastructure anomalies, community reporting, and the immediate consequences of violence or disaster.

The Mosaic Process

This integration reflects the mosaic intelligence process, through which separate and often inconclusive pieces of information are collected, compared, analyzed, and combined to reveal a threat that no single organization could identify independently. DHS I&A is positioned to help assemble this mosaic by working with DHS components that observe different parts of the threat environment.

- U.S. Customs and Border Protection may identify suspicious travel, border encounters, cargo movements, or document irregularities.
- U.S. Immigration and Customs Enforcement may uncover transnational criminal networks, smuggling activity, illicit finance, and immigration-related violations.
- U.S. Citizenship and Immigration Services may identify anomalies involving applications, identities, immigration benefits, or supporting documentation.
- The Transportation Security Administration may detect threats affecting aviation and surface transportation.
- The Cybersecurity and Infrastructure Security Agency may provide reporting on cyber threats and critical-infrastructure vulnerabilities.
- The United States Coast Guard may contribute maritime-domain awareness, port-security information, and observations involving vessels, waterways, and coastal activity.

DHS I&A must combine these component-level insights with intelligence from the FBI, CIA, National Counterterrorism Center, Department of Defense, Department of State, and other

a. DHS was established on November 25, 2002, with George W. Bush's signing of the Homeland Security Act of 2002. It began operation on March 1, 2003.

Federal partners, while also incorporating reporting and local context from state, local, tribal, and territorial governments and fusion centers.

Through these continuous exchanges, isolated fragments—such as suspicious travel, an immigration irregularity, a cyber intrusion, a local police encounter, unusual financial activity, or suspicious behavior near critical infrastructure—can become part of a larger warning picture. The mosaic process therefore depends not merely on collecting more information, but on ensuring that relevant information is lawfully shared, accurately analyzed, placed in context, and delivered promptly to officials with the authority and capability to prevent, disrupt, or respond to threats.

The mosaic concept also connects directly to the failures described by Toobin and Wright. McVeigh and Nichols generated fragments through travel, purchases, storage rentals, extremist associations, and logistical preparations, but those pieces were not assembled before the bombing. The September 11 hijackers generated fragments through foreign travel, terrorist associations, immigration violations, flight training, financial transactions, licensing activity, and encounters with local police, but those pieces remained divided among foreign intelligence agencies, federal departments, and state and local systems. DHS I&A's value lies in helping prevent such fragments from remaining isolated.

DHS I&A must help integrate these perspectives so the homeland-security enterprise can detect, warn, and deal with threats to the American people. Detection requires comparing national and international intelligence with behavior and vulnerabilities observed inside communities. Warning requires translating intelligence into timely, understandable, and appropriately classified information for officials who can act. Dealing with threats requires connecting analysis to prevention, investigation, disruption, infrastructure protection, emergency response, consequence management, and recovery.

The Roles of Fusion Centers

State and major urban-area fusion centers are a principal instrument of this relationship. They serve as focal points for sharing threat-related information between the federal government and state, local, tribal, and territorial partners. Because they are owned and operated by state and local governments, they are not merely branch offices of a federal agency. I&A personnel and intelligence products can supply national context, while fusion-center analysts contribute local knowledge and return relevant reporting to federal partners.

This two-way relationship matters more than simply distributing additional reports. Intelligence must be timely, relevant, legally obtained, understandable to the intended recipient, and connected to someone

with the authority to act. State and local governments should not merely receive federal intelligence; they must help shape intelligence requirements by identifying local vulnerabilities, suspicious patterns, public-safety concerns, infrastructure dependencies, and emerging threats that may possess national significance.

FBI Joint Terrorism Task Forces

The FBI's Joint Terrorism Task Forces provide the investigative complement. JTTFs combine investigators, analysts, linguists, and specialists from federal, state, and local agencies to pursue leads, gather evidence, make arrests, share intelligence, and respond to threats. DHS I&A, fusion centers, and JTTFs should not duplicate one another. I&A and fusion centers strengthen analysis, warning, situational awareness, and information exchange; JTTFs convert credible terrorism leads into coordinated investigation and disruption. Their relationships must be habitual before a crisis rather than improvised afterward.

The Need for Continuous Learning

Much has been learned since DHS began operating. Watchlisting and information-sharing mechanisms are stronger; federal personnel work more routinely with state and local partners; terrorism investigations are more joint;

The Mosaic of Homeland Security Intelligence

immigration and border information is more closely connected to national security; and homeland-security intelligence now encompasses cyber threats, critical infrastructure, transnational crime, foreign influence, natural hazards, and other risks. State, local, tribal, and territorial law-enforcement partners are now more fully recognized as essential to domestic defense. These advances make the country better able to detect patterns that previously would have remained divided among agencies.

Yet much remains to be done. More information can create overload rather than insight. Classification may keep intelligence from officials who can use it, while indiscriminate collection can violate privacy, produce false leads, and weaken public trust. Small jurisdictions, tribal nations, and territories may lack analysts, secure communications, cybersecurity capacity, or sustained access to federal expertise. Databases can contain errors, names vary across documents, and agency incentives can recreate the silos that reorganization was intended to remove. *And yet to be determined is the impact for good or ill of the artificial intelligence revolution.*

The continuing mission is therefore one of organizational learning. DHS I&A and its partners must test whether warnings actually reach decisionmakers, exercise joint procedures, measure the usefulness of intelligence products, correct information-sharing gaps, provide

intelligence training to state and local entities, and adapt to technologies and tactics that did not exist in 1995 or 2001. Integration cannot be judged by the number of reports distributed or meetings held. It must be judged by whether the enterprise produces improved understanding and timely action.

Both authors also invite caution. Toobin's effort to connect McVeigh to later political extremism is provocative, but intelligence professionals should avoid forcing every threat into a partisan narrative. Wright's focus on O'Neill and CIA-FBI conflict makes bureaucracy dramatically understandable, yet personalities alone do not explain September 11. Law, resources, technology, leadership, analytic assumptions, and organizational design also mattered.

In Sum

The books are strongest when thought about together in the context of our intelligence missions. One shows domestic radicalization becoming operational; the other shows foreign direction entering the homeland. Both demonstrate that ideology matters, but preparatory behavior, enabling relationships, travel, logistics, and institutional seams often provide more actionable warnings and opportunities to detect at the local level.

Security is inseparable from American prosperity. Safe

transportation, reliable infrastructure, lawful international travel, resilient communities, functioning markets, and public confidence allow economic and civic life to flourish. The goal is not maximum surveillance or the elimination of all risk. It is a disciplined system that concentrates on threats and behavior, protects constitutional liberties, shares intelligence according to legitimate need, and enables government and private institutions to continue operating during disruption.

Homegrown and *The Looming Tower* ultimately describe the human cost of fragmented knowledge. The Oklahoma City and September 11 attackers were not entirely invisible; they traveled, purchased, trained, communicated, violated rules, interacted with institutions, and left records. What failed before the attacks was the conversion of scattered information into integrated warning and coordinated response.

The enduring responsibility of DHS I&A is to help connect international intelligence, national capabilities, DHS operations, and state and local knowledge so that officials can detect danger early, warn those at risk, and deal with threats before they become catastrophes. *Much has been learned, but the final lesson of both books is that integration is never finished.* It must be continuously trained, practiced, evaluated, and renewed to protect the American people, their freedoms, and the

prosperity those freedoms make possible.

These historical intelligence gaps fiercely highlight that we still need further integration of federal, state, local, territorial, and tribal (SLTT) information as a core component of homeland security. Today and in the future, protecting the American people requires a unified operational picture to combat evolving threats, particularly Chinese malign influence and extraterritorial actions within US borders. State-sponsored

actors frequently operate at the local level, engaging in transnational repression, intellectual property theft, economic espionage, and the operation of undeclared overseas police outposts.

Just as local traffic cops were on the front lines of encountering the 9/11 hijackers, local law enforcement and state officials are often the first to receive reports of foreign harassment of dissidents, cyber intrusions against municipal infrastructure, or suspicious local

corporate investments. Without seamless, secure data sharing across all jurisdictions, these isolated local incidents will fail to trigger federal counterintelligence alarms. A true whole-of-government approach ensures that an intelligence analyst in Washington and a patrol officer in the field are connected, closing the gaps that hostile nations and terrorist organizations alike seek to exploit. ■