



GUIDE TO THE STUDY OF INTELLIGENCE

Homeland Security and Intelligence

Fusing Sometimes Incompatible Missions

William C. Spracher, Ed.D.

One purpose of the *Guide to the Study of Intelligence* is to offer “suggestions for instructors teaching various topics for which intelligence is an important component.”¹ As a National Intelligence University faculty member, I can attest that many courses are taught on intelligence per se, and somewhat fewer on homeland security, the latter usually by rotating faculty “chairs” from the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), and the US Coast Guard (USCG).² At times, however, the students hailing from all the armed services and most of the civilian agencies of the Intelligence Community (IC) view these subjects as separate and distinct. One is outward-looking, focused primarily on what we used to carefully define as “foreign intelligence,” the other inward-looking, focused on “domestic intelligence.”

The multiple terrorist attacks of September 11, 2001 prompted a critical relook of the boundaries between foreign and domestic intelligence gathering as it became painfully obvious that threats are all around us and in our midst. The Homeland Security Act of 2002 created DHS, formally established March 1, 2003, combining assets from 22 different departments and agencies and more than 85,000 personnel previously performing related but separate duties.³ The USA PATRIOT Act of 2001 also changed the way intelligence and homeland security are viewed, as did

the Intelligence Reform and Terrorism Prevention Act of 2004, which in part mandated the establishment of the Office of the Director of National Intelligence (ODNI) and called for the creation of a National Intelligence University (NIU). Other key documents which influenced the development of the US national security establishment since then have included the 9/11 Commission Report and the WMD Commission Report.⁴

Several years ago, when NIU was operating under one of its previous names, the Joint Military Intelligence College (JMIC), I was asked to contribute an article on how homeland security relates to intelligence. The result was “Homeland Security and Intelligence: Can Oil Mix with Water in an Open Society?”⁵ In that piece, I argued that one of the most controversial aspects in the process of developing DHS, and refining the concept of homeland security overall, is the role of intelligence in gathering information on the terrorist threat and analyzing it for key decisionmakers.⁶ I explored the intelligence challenges for homeland security, to include the problems of merging disparate cultures – law enforcement versus intelligence; civilian actors versus military; federal efforts versus those at the state, local, and tribal levels; and a domestic focus versus the foreign perspective. At play is the traditional tradeoff between the rights of ordinary US citizens to their privacy and the national security imperatives of the country at large, a delicate balancing act that has taxed the patience and sensitivities of the American people, and the more time that has elapsed since a major attack inside the borders of the US the more outraged some people seem to become. Witness the huge reaction to revelations of domestic and diplomatic spying by the PFC Bradley Manning, “WikiLeaks,” and Edward Snowden sagas that still fill the headlines of our newspapers.⁷

“Homeland security” is a relatively new term in the American lexicon. We have long dealt with law enforcement, counterintelligence, and internal security (plus a term that Americans tend to recoil

4. The former, promulgated on July 22, 2004, is officially known as *The Final Report of the National Commission on Terrorist Attacks Upon the United States*; and the latter, promulgated on December 3, 2008, is officially known as *World at Risk: Commission on Prevention of Weapons of Mass Destruction, Proliferation, and Terrorism*.

5. William C. Spracher, “Homeland Security and Intelligence: Can Oil Mix with Water in an Open Society?” in *Learning with Professionals: Selected Works from the Joint Military Intelligence College* (Washington, DC: Joint Military Intelligence College, 2005), 139-140. Originally published in *Low Intensity Conflict & Law Enforcement* 11 (1), Spring 2002, 29-54.

6. *Ibid.*, 145.

7. Julie Tate, “Bradley Manning Sentenced to 35 Years in WikiLeaks Case,” *The Washington Post*, August 21, 2013; Barton Gellman, “Edward Snowden, after Months of NSA Revelations, Says His Mission’s Accomplished,” *The Washington Post*, December 23, 2013.

1. AFIO website, http://www.afio.com/40_guide.htm.

2. *Catalog, 2014-2015*, National Intelligence University, 4.

3. DHS website, <http://www.dhs.gov/history>.

at hearing, but citizens of many other countries have routinely practiced – countersubversion), and we tend to separate those inward-looking exercises from the more outward-looking foreign intelligence. The FBI traditionally was responsible for counterintelligence (CI) within the borders of the US while the Central Intelligence Agency (CIA) had purview over CI overseas, and that is still the case, though the FBI maintains legal attachés overseas at a number of US embassies, in particular those in countries with a large number of US citizens. The armed forces, especially the US Army, got into a great deal of trouble in the late 1960s-early 1970s when they were pulled by various presidential administrations into collecting information on domestic actors, and particularly those assessed as somehow tied to communism and/or posing a threat to our national security.

Most of the existing intelligence oversight mechanisms the US utilizes today came about in the 1970s as a result of tightening controls against such abuses. We now have in Congress the Senate Select Committee on Intelligence (SSCI) and the House Permanent Select Committee on Intelligence (HPSCI), which oversee intelligence activities of the various components of the Executive Branch that formerly tended to get their guidance only from the President and the National Security Council. After 9/11, there were created a White House Homeland Security Council and Homeland Security Committees in both houses of Congress.⁸ Needless to say, some of the latter’s duties overlap with those of the intelligence select committees. Furthermore, DHS probably receives more oversight than any entity in the Executive Branch. I have seen mind-boggling charts showing how many different committees and subcommittees routinely oversee one function or another of the vast and complex Cabinet department known as DHS.⁹ To complicate matters even more, the Department of Defense (DOD) exercises a function known as “homeland defense.”¹⁰ There is an assistant secretary for homeland defense and Americas’ security affairs overseeing this function, and, of course, that senior official collaborates closely with the various

entities responsible for homeland security and also those responsible for intelligence.

At about the time the homeland security/homeland defense lash-up was being worked out institutionally and statutorily, an excellent article on this issue was published in the National Defense University’s premier publication, *Joint Force Quarterly*. Here is an excerpt from the article, titled “The DOD Role in Homeland Security”:

To date the Secretary of Defense has specifically referred to DOD involvement as homeland defense rather than homeland security – signifying more than a semantic difference. Defense implies deterrence and/or response whereas security is more comprehensive; defense is part of security but not the only part. This distinction avoids having the Pentagon become embroiled in an ill-defined mission as capstone agency for Federal, state, and local police and first-response agencies. The Department of Defense is not prepared, willing, or in some cases constitutionally permitted to play that role. Yet because agencies that must respond to the consequences of an attack using weapons of mass destruction need resources now instead of after another terrorist attack, the DOD mission must be expanded from just defending the homeland to supporting homeland security, especially since a future attack could inflict more casualties than were suffered on 9/11.¹¹

Another part of the Pentagon is also tied in closely with the intelligence organs, and that is under the control of the assistant secretary for special operations and low intensity conflict (ASD SO/LIC).¹²

The DHS is now a full-fledged member of the 16-agency IC through its Office of Intelligence and Analysis (I&A). Interestingly, when the department was first stood up, that entity was known as the Directorate of Information Analysis and Infrastructure Protection. However, growing pains and some confusion as to the scope of its mission soon led to splitting out the intelligence and infrastructure protection functions.¹³ There was a fairly rapid turnover of I&A directors too, as the department struggled to find its proper niche in the IC and sort out clearly defined roles and missions. The department still suffers from rapid turnover of key billets and slowness in recruiting

8. Mark M. Lowenthal, *Intelligence: From Secrets to Policy*, 5th ed. (Washington, DC: CQ Press, 2012), 31.

9. “Untangling the Web: Congressional Oversight and the Department of Homeland Security,” *CSIS Business Executives for National Security*, December 10, 2004, 6. It should be noted that the White House Homeland Security Council has now been folded into the National Security Council.

10. M. E. Krause, “Homeland Defense and Security,” *Joint Force Quarterly* 40, January 2006. See also “DOD Releases Strategy for Homeland Defense and Defense Support for Civil Authorities,” *DOD News Release* 172-13, March 22, 2013.

11. Adrian A. Erckenbrack and Aaron Scholer, “The DOD Role in Homeland Security,” *Joint Force Quarterly* 35, Summer 2003, 1.

12. “Assistant Secretary for Special Operations/Low-Intensity Conflict,” Fact Sheet, undersecretary of defense for policy, undated, accessed at <http://policy.defense.gov/solic>, November 25, 2014.

13. Office of the Inspector General, Department of Homeland Security, *Survey of the Information Analysis and Infrastructure Protection Directorate*, undated. See also James Burch, “The Domestic Intelligence Gap: Progress Since 9/11?” in Proceedings of the 2008 Center Homeland Defense & Security Annual Conference, *Homeland Security Affairs*, online journal of the Center for Homeland Defense and Security, Naval Postgraduate School, 2008.

high-level talent, which even when found often takes months to get through the US Senate confirmation process.¹⁴ Protection of critical infrastructure is key in an era when the terrorist threat inside our national borders is palpable. Some would not define it as an intelligence mission per se, but cannot dispute that it is at least closely related to intelligence. For example, a few academic entities that look at these subjects – without inserting the word “intelligence” into their names – include the George Washington University Homeland Security Policy Institute, the Naval Postgraduate School Center for Homeland Defense and Security, the George Mason University (GMU) School of Law Center for Infrastructure Protection and Homeland Security, and the US Military Academy (USMA) Department of Social Sciences Combating Terrorism Center. The GMU center produces an excellent monthly CIP Report and the USMA center a monthly CTC Sentinel, which are highly commended to instructors looking for current teaching materials.

The CIP Report, produced digitally on a monthly basis, can be accessed at <http://cip.gmu.edu>. Each issue is introduced by the center director, a retired US Army lieutenant general whom this author knew when he was director of the Army Staff and later deputy under-secretary of the army for international affairs. The “Report” focuses on a different theme each month. For example, in July 2014, it was “State and Tribal”; in August 2014, “Water and Water Infrastructure”; in September 2014, “Risk and Risk Management”; and in October 2014, “Cybersecurity.” As the director points out in his cover introduction to the latest issue, partnerships are critical in the homeland security field – e.g., a cybersecurity research partnership among GMU, IBM Corporation, and the National Science Foundation.¹⁵ The center’s associate director served as a panelist during a one-day workshop this author organized in November 2012 with the theme “Intelligence Education and Training.”¹⁶ Many of these same issues are discussed via a LinkedIn group known as “The Intelligence and Homeland Security Alliance,” which interested parties can access through LinkedIn, the popular social media site used widely within the US Government and commercial entities.¹⁷ Another excel-

lent resource is a news compilation of articles dealing with homeland security and intelligence, known as the “CABLEGram,” disseminated to select members by the National Military Intelligence Association (NMIA).¹⁸

There is no shortage of books that deal with homeland security, and many of them examine the role of intelligence in generating information of value that assists our national, state, local, and tribal entities in keeping us safe. Michael Chertoff, DHS secretary in the George W. Bush administration and now head of his own influential consulting firm, The Chertoff Group, in 2009 published *Homeland Security: Assessing the First Five Years*. The foreword was penned by former Representative Lee H. Hamilton, who is now president of the Woodrow Wilson International Center for Scholars in Washington, DC. Hamilton stated that “both during and after my tenure as vice chairman of the 9/11 Commission, I witnessed striking changes, ranging from the restructuring of our intelligence agencies to the creation of the Department of Homeland Security. ... The FBI had made counterterrorism a top priority, fundamentally changing the law enforcement culture and direction of the Bureau. An integrated terrorist watch is now complete.”¹⁹ In other words, the FBI is one of those IC agencies where counterterrorism, intelligence, and homeland security all come together and are fused.

In the intelligence business, we often say our job is to minimize uncertainty, though we cannot eliminate it entirely. Similarly, Chertoff observes that in the homeland security effort “it is neither possible nor desirable to pursue a risk elimination strategy.”²⁰ DHS does what it can to minimize risk, but it cannot eliminate it. Intelligence and homeland security share that dilemma, i.e., how to enhance security, knowing that the world is a dangerous place with countless bad actors wishing us harm, but without unduly stepping on the individual rights and liberties that our citizens are guaranteed by the US Constitution. It is a fragile balance, and one in which past misdeeds and overreaches have produced a plethora of scandals and legal battles.²¹

Former Secretary Chertoff insists, “We must use every tool in the security toolbox, and in the coming

14. Jerry Markon, “Top-Level Turnover Makes It Harder for DHS to Stay on Top of Evolving Threats,” *The Washington Post*, September 21, 2014, accessed September 30, 2014, at <http://www.washingtonpost.com/politics/top-level-turnover-makes-it-harder-for-dhs-to-stay>.

15. Mick Kicklighter, director, George Mason University School of Law CIP/HS, *The CIP Report* (13) (3), October 2014, 1.

16. William C. Spracher, “Editor’s Desk,” *American Intelligence Journal*, Vol. 31, No. 2, 2013, with theme “Intelligence Education and Training,” pp. 3-5.

17. “Intelligence and Homeland Security Alliance,” LinkedIn.

18. For more information see <http://www.nmia.org>.

19. Lee H. Hamilton, in Foreword to Michael Chertoff, *Homeland Security: Assessing the First Five Years* (Philadelphia: University of Pennsylvania Press, 2009), vii. See also *Today’s FBI: Facts & Figures, 2013-2014* (Washington, DC: US Department of Justice, 2014).

20. Chertoff, 6.

21. See, for example, discussion of the 1920 Palmer raids in David Major and Peter Oleson, “Espionage Against America,” in the *Guide to the Study of Intelligence*, at http://www.afio.com/40_guide.htm.

years we will have to invent a few tools that do not yet exist.”²² At the same time, he concedes, “Governments must continue to use old-fashioned counter-intelligence: working to prevent people from committing espionage, stealing data or passwords, or implementing trapdoors in systems.”²³ Cybersecurity seems to be the hot-button issue of the early 21st century, and cyber warfare has apparently supplanted conventional, much less nuclear, warfare as the method of choice for our wily adversaries. Both the intelligence and homeland security communities are heavily involved in the cyber effort. Witness the fact that the director of the National Security Agency (NSA), one of the largest, most expensive, and most secret of the IC, has been dual-hatted since 2010 as the commander of US Cyber Command, a subordinate element of US Strategic Command. For its part, DHS is responsible for coordinating cybersecurity with the non-governmental sector, to include private corporations. Intelligence and homeland security both are intricately intertwined with the cyber world. According to Chertoff, “In the wake of September 11, the United States moved decisively and effectively to create a new Department of Homeland Security, remove some of the barriers between intelligence agencies, hunt for Al Qaeda leaders overseas, and institute numerous measures to prevent or reduce our vulnerability to further attacks.”²⁴

Intelligence is even essential to some aspects of homeland security that may not be immediately obvious, such as public safety and public health. Chertoff suggests, “In a very real way, intelligence is a critical element in promoting public health in the twenty-first century. The value of this kind of intelligence was vividly demonstrated in London in spring 2008, and at the trial of those suspected of plotting to blow up transatlantic airliners in 2006. Based on diligent intelligence gathering, we learned about the elaborate efforts made to manufacture explosive devices concealed in sport drink bottles. There simply is no adequate substitute for good intelligence that can help us detect the initial emergence of dangerous biological pathogens or their appearance in our country.”²⁵ It is not surprising, then, that one of the increasingly important subordinate analytical production centers of the Defense Intelligence Agency (DIA) is the National Center for Medical Intelligence (NCMI), formerly known as the Armed Forces Medical Intelligence Center (AFMIC), located at

Fort Detrick in Frederick, Maryland.²⁶ With the Ebola epidemic sweeping through west Africa in 2014, and people worldwide frightened that it will spread, US homeland security has a new threat to deal with, and the President has involved US military forces in helping to contain the situation. Though the bulk of them are performing logistical tasks not in the immediate vicinity of infected patients, it would not be surprising if some of them are working in intelligence specialties. Speaking of DIA, it maintains close coordination with DHS. For example, as previously mentioned, there is a DHS chair on the NIU faculty. In addition, a member of the DIA senior executive service is presently serving on a joint duty assignment with DHS as chief, cyber intelligence integration.²⁷

A couple of other books come to mind that in part examine the overlap of homeland security and intelligence. Looking at the former in an international context, and how it affects alliances and partnerships, is *North American Homeland Security: Back to Bilateralism?* by three authors who insist DHS was established as “the central agency in the largest overhaul since World War II to keep not only the United States safe, but also revive a wider security community.”²⁸ The book focuses on the three North American nations of the United States, Canada, and Mexico, and evaluates how well each can protect its citizens while dealing bilaterally and trilaterally with its neighbors. Looking at “trilateralism” and “intelligence instincts” after 9/11, the authors observe, “Intelligence becomes meaningless in a vacuum or if tardy.... Forging partnerships may be useful, as between Canada and the United States, but integrating the disparate agencies demands more attention and resources than any of the countries can offer, or show interest in.”²⁹ As the continuing debate in the US on immigration reform demonstrates, not only is unilateral action by one branch of one government of concern, but unilateral action by one nation without coordination or consultation with neighboring nations can lead to problematic spillover effects and unintended consequences. Just as intelligence sharing and collaboration are challenges for international relations, homeland security must take into consideration differing “homelands,” perspectives on how to protect them, and legal frameworks that often clash.

26. See Jonathan D. Clemente, MD, “Medical Intelligence,” *The Intelligencer* 21 (1), Fall/Winter 2013, http://www.afio.com/40_guide.htm.

27. DIA internal communications on personnel assignments.

28. Imtiaz Hussain, Satya R. Pattayak, and Anil Hira, Preface, *North American Homeland Security: Back to Bilateralism?* (Westport, CT: Praeger Security International, 2008), vi.

29. Ibid, 236-237.

22. Ibid, 54.

23. Ibid, 100-101.

24. Ibid, 125.

25. Ibid, p. 137.

Finally, Jonathan White's book, *Defending the Homeland: Domestic Intelligence, Law Enforcement, and Security*, though now a bit dated, is well worth examining. The author opines that "organizational conflict between the intelligence and law enforcement communities is a managerial issue, but it also impacts the Constitution."³⁰ He quotes from *The National Strategy for Homeland Security*, which calls for increased information sharing among law enforcement agencies.³¹ Similarly, there is a *National Intelligence Strategy*, promulgated by the DNI, most recently in 2014. In that document, Director James Clapper lists the IC's "Mission Objectives" as strategic intelligence, anticipatory intelligence, current operations, cyber intelligence, counterterrorism, counterproliferation, and counterintelligence.³² These very same objectives translate nicely to areas the homeland security community must be concerned about. In a section of his book titled "The Inevitable Failure of Intelligence," White confesses that "despite the best intentions and the creation of better systems, intelligence will fail at certain points," a fact that has been examined in the past by such eminent scholars as Richard Betts of Columbia University.³³ "Intelligence is competitive, and our enemies are trying to beat us. Terrorists only need to be successful one time. ... The best system cannot stop every attack. When prevention and interdiction can do no more, state and local law enforcement will be called to the scene to manage a crisis. In terms of homeland security, the mission will shift from offense to defense."³⁴

It is often argued that one of the main reasons intelligence and law enforcement cannot be compatible is the differing goals of the two. While law enforcement aims to arrest perpetrators of a crime (a retrospective focus) and obtain a conviction, intelligence (with a prospective focus) often prefers to gain information about trends and patterns without rolling up the sources of that information too soon. To do this, sometimes a low-level perpetrator of a crime, or an enemy combatant, will be monitored but not apprehended for a time in the interest of finding the high-level orchestrator of the crime or the military action planned. In other words, short-term, tactical

success might be sacrificed for long-term, strategic success. In the latter case, the overall threat is what counts, not individual actors doing malicious things.

As just one example, a Department of Justice (DOJ) Drug Enforcement Administration (DEA) agent or a DHS Immigration and Customs Enforcement (ICE) agent may desire to make an arrest, yet the intelligence information utilized has to be managed in such a way that it can be used as evidence in a trial. This often runs counter to what an intelligence officer's aims are, which are more likely to develop comprehensive, confirmed information to support a policymaker, combatant commander, or decisionmaker of some sort. The type of information needed to accomplish that objective – and how it is protected, exploited, and released – may be radically different. Still, in the high-threat environment of the present century post-9/11, where transnational actors often are not sponsored by states and pay no attention to borders, international law, or the norms of human decency, intelligence agencies and law enforcement/homeland security agencies must work together. Elements from both play a key role in keeping our citizens safe and our governments at all levels functioning effectively for the well-being of all.

READINGS FOR INSTRUCTORS

- Chertoff, Michael. *Homeland Security: Assessing the First Five Years* (Philadelphia: University of Pennsylvania Press, 2009).
- Hussain, Imtiaz, Satya R. Pattanayak, and Anil Hira. *North American Homeland Security: Back to Bilateralism?* (Westport, CT: Praeger Security International, 2008).
- Logan, Keith G. *Homeland Security and Intelligence* (Westport, CT: Praeger), 2010.
- Lowenthal, Mark M. *Intelligence: From Secrets to Policy*. 5th ed. (Washington, DC: CQ Press, 2012).
- Spracher, William C. "Homeland Security and Intelligence: Can Oil Mix with Water in an Open Society?" *Learning with Professionals: Selected Works from the Joint Military Intelligence College* (Washington, DC: Joint Military Intelligence College, 2005).
- US Army War College. "Homeland Security: A Selected Bibliography." Carlisle, PA: US Army War College Library, April 2011.
- US Department of Justice Federal Bureau of Investigation. *Today's FBI: Facts & Figures, 2013-2014* (Washington, DC: Government Printing Office, 2014).
- US Office of the Director of National Intelligence. *The National Intelligence Strategy of the United States of America* (Washington, DC: Government Printing Office, 2014).
- White, Jonathan. *Defending the Homeland: Domestic Intelligence, Law Enforcement, and Security* (Belmont, CA: Wadsworth,

30. Jonathan White, *Defending the Homeland: Domestic Intelligence, Law Enforcement, and Security* (Belmont, CA: Wadsworth, Cengage Learning, 2004), 19.

31. *Ibid.*, 74.

32. *The National Intelligence Strategy of the United States of America* (Washington, DC, 2014), 2.

33. Richard K. Betts, "Analysis, War, and Decision: Why Intelligence Failures Are Inevitable," in *World Politics* 31 (1), October 1978, 61-89, <http://www.jstor.org/stable/2009967>.

34. White, *op. cit.*, 76.

Cengage Learning, 2004).

William C. Spracher is a contracted faculty member at the National Intelligence University, teaching courses on social analysis, globalization, peacekeeping & stability operations, and Latin America. He is a retired US Army colonel who served for over 30 years in armor, military intelligence, and the Foreign Area Officer program. He was Army attaché to Peru and defense attaché to Colombia prior to his final assignment as military professor at the National Defense University Center for Hemispheric Defense Studies. Earlier, he taught political science at the US Military Academy, from which he graduated in 1970. He has a master's degree in international relations from Yale University, a master's in political-military studies from the US Army Command & General Staff College, and a doctorate in education from George Washington University. He serves on the boards of directors of the International Association for Intelligence Education (IAFIE) and the National Military Intelligence Association (NMIA); for the latter, he is editor of its principal publication, the *American Intelligence Journal*.



**WITHOUT AN EMERGENCY PLAN
YOUR BUSINESS CAN END UP HERE.**

Ready.gov/business

Up to 40% of businesses never recover after experiencing a major disaster. Do you have a plan to keep your business running if disaster strikes? For a free online tool that helps you develop an emergency plan, visit Ready.gov/business.

   