Chapter 1
Introducing Security Analysis

Bottom Line Up Front (BLUF)

The need for security analysis stretches back thousands of years. Since humans first began organizing in groups, information has been sought on potential adversaries. During and after World War II, security analysis became even more in demand to support military operations in both the Atlantic and Pacific theaters, the later Cold War, and the now post-Cold War. The September 11, 2001, terrorist attacks on the United States exposed a dire need for both improved U.S. national security intelligence analysis and policy analysis; however, only the U.S. Intelligence Community took action to improve its analysis after this major national failure. Today, the need for security analysis is even more acute as the nation faces both external national security and internal homeland security threats.

Historical Summary of Security Analysis

Security analysis emerged eons ago as competing human groups (tribes, clans, etc.) sought to identify the strengths, locations, and intentions of both their enemies and friends. Chinese General Sun Tzu (544-496 BCE) discusses the use of military information in decision making throughout his treatise *The Art of War*, including dedicating the last chapter to "Employment of Secret Agents."[1] Seeking information to gain military advantage is also a frequent theme in Thucydides' *History of the Peloponnesian Wars* (431-404 BCE) waged between Sparta and its allies in the Peloponnesian League and Athens and its allies in the Delian League.[2] For centuries leaders have sent agents and envoys to foreign courts to assess their military capabilities and determine their intentions. One of the most noted

court advisers was Niccoló Machiavelli (1469-1527 CE), who was a diplomat and military strategist to waring principalities on what is today's Italian peninsula.[3] General George Washington was known for his spy networks that gathered information on British forces and their intentions in support of his decisions in the American Revolutionary War.[4] Security analysis to gain a decision advantage has a long history.

Modern U.S. security analysis began as the United States grew into a national security state with the start of World War II and during the following Cold War.[5] At the start of World War II, President Franklin D. Roosevelt (FDR) recognized the need for intelligence collection and analysis beyond those of the military services, Federal Bureau of Investigation (FBI), and State Department. Roosevelt called on William "Wild Bill" Donovan, a World War I Medal of Honor winner, civilian attorney, and politician, to become FDR's personal envoy in assessing the pre-war security conditions in Europe and the Mediterranean.[6] In 1941, FDR appointed Donovan to direct the civilian Office of the Coordinator of Information to produce strategic war analysis and report directly to the President and the Joint Chiefs of Staff. In 1942, with the addition of covert operations responsibilities, Donovan's new organization became the **Office of Strategic Services** (OSS) and supported the war effort until disbanded in 1945 at war's end by President Harry S. Truman.[7]

As the U.S. government adjusted to the end of World War II and the start of the Cold War against the Soviet Union and its allies, Truman signed the **1947 National Security Act** that formed a permanent **U.S. National Security Council** and **Joint Chiefs of Staff**, and created the Central Intelligence Agency (CIA), Department of Defense (DOD), and U.S. Air Force (from the U.S. Army Air Corps). CIA was given similar tasking to conduct analysis and covert operations as the wartime OSS and was envisioned as a national-level foreign intelligence agency reporting directly to the President and National Security Council. The CIA Director also was assigned the position of Director of Central Intelligence, responsible for coordinating the intelligence activities of the CIA, DOD, military services, FBI, and

State Department. As this new national security structure unfolded over the next several decades, the importance and size of the security analysis community grew by leaps and bounds. Since 2004, sixteen U.S. government intelligence agencies and offices support U.S. national security, homeland security, and law enforcement activities, making up the main structure of the **U.S. Intelligence Community** (IC) under the coordination, direction, and oversight of a new **Director of National Intelligence** (replacing the previous Director of Central Intelligence). Hundreds of state, local, and corporate intelligence entities also cooperate and are integral to the IC's missions.

Two early 21st Century cases were watershed events in U.S. security analysis. The first was the September 11, 2001, attacks on the United States by *al Qaeda* terrorists.[8] The second was in 2002, not long after the September 11 disasters, when the CIA's National Intelligence Council (NIC) published a later widely criticized National Intelligence Estimate (NIE) on Iraqi Weapons of Mass Destruction (WMD).[9] A number of investigations were commissioned to determine who in the U.S. security community was to "blame" for both the lack of warning about the September 11 attacks and the poor analysis in the Iraqi WMD NIE. Most of the published blame fell on the IC. The bi-partisan *9/11 Commission Report* found the IC failed to share information on the *al Qaeda* attackers and their plans, intelligence analysts were unable to "connect the dots" (in fact no single agency's analysts had all the known dots (facts) due to problems in sharing information), and the IC lacked "imagination," leading its analysts to discount a massive foreign terrorist attack on U.S. soil.[10] The Iraqi WMD NIE predicted inaccurately the existence of an Iraqi WMD capability, which was a major justification for the 2003 U.S. invasion of Iraq. Investigations found the NIE placed too much credence on one unreliable source, the analysis lacked robustness, and its findings were based on faulty assumptions.[11]

Although the IC received the bulk of the criticism over the September 11 disasters and the poor Iraqi WMD NIE, the security policy community was also at fault. When given pre-September 11 information on the threat of *al Qaeda*

attacks on U.S. soil—even though not specific in terms of the methods, places, or times of an attack—President George W. Bush and members of his National Security Council either disregarded the information or took no action.[12] There appeared little concern for finding out more about the threat or bringing together multiple intelligence agencies and national security policy planners to institute a domestic interagency counterterrorism effort. The early-Bush National Security Council saw Iraq and Russia as their main opponents and placed little priority on the threat from *al Qaeda*, who they perceived as a small, rag-tag terrorist group operating from caves in Afghanistan. The security policy community was also partly responsible for the poor quality of the Iraqi WMD NIE. The policy community pressured the NIC through a directed short deadline to publish the report. They also interfered as Bush administration policy staffers (including Vice President Richard B. Cheney) engaged directly with intelligence analysts to guide the NIE analysis to support a National Security Council decision already made to invade Iraq.[13]

Richards Heuer, a career CIA analyst and author of the landmark book *Psychology of Intelligence Analysis*,[14] characterized the IC political-military analysis at the beginning of the 21st Century as mainly **unaided judgment**.[15] He observed how the main analytic techniques in use included a combination of evidentiary reasoning, the historical method, case study analysis, and reasoning by analogy. These techniques usually followed the intuitive/inductive approach to analysis. Unaided judgment techniques can have serious limitations, but were the standard throughout the IC and no doubt also in the security policy community before the early-2000s.

> **Evidentiary reasoning** makes use of information (data, evidence, etc.), logic, and reasoning to reach a finding or conclusion. Evidentiary reasoning often lacks conceptual structures (models, theories) and can place too much analytic emphasis on the most recent evidence available. Some basic critical thinking was included with evidentiary reasoning, but this technique

was still embedded in the intuitive/inductive approach, which Appendix II details can inject significant bias in an analysis.

The **historical method** was an IC standard from World War II until the start of the 21st Century, as many OSS, CIA, and other IC analysts came from history and humanities departments in elite U.S. universities. This method included aspects of evidentiary reasoning and reasoning by analogy and was deeply embedded in IC analytic culture. The historical method excluded the more robust analytic techniques of **behaviorism** developed in the academic social sciences starting in the 1950s. Behaviorism, grounded in cognitive psychology and following the scientific method, became the main approach for academic social science analysis, but was little used in the IC steeped in the historical method. Behaviorism embraces both the application of the scientific method to human behavior and the ever-increasing capabilities of computers to quantitatively analyze large databases.

Case study analysis, when used with the intuitive/inductive approach, also has a long history in the analytic community. Case study analysis included aspects of evidentiary reasoning, historical method, and reasoning by analogy as it concentrated on one or two specific cases. Case study analysis can be severely flawed if the contexts of comparable cases are not thoroughly investigated and if there is not a conceptual model or theory to use in generating inferences.

The **reasoning by analogy** technique uses past behaviors to explain or predict future behaviors and can also lead to severe analytic problems. This technique often neglects historical background and context. Often used by experienced senior analysts, reasoning by analogy can be a positive factor in guiding intelligence analysis, if the historical background and context of a

situation are thoroughly considered; however, if this or other intuitive/inductive approaches are used mainly by experienced analysts, it could add significant bias to their findings.

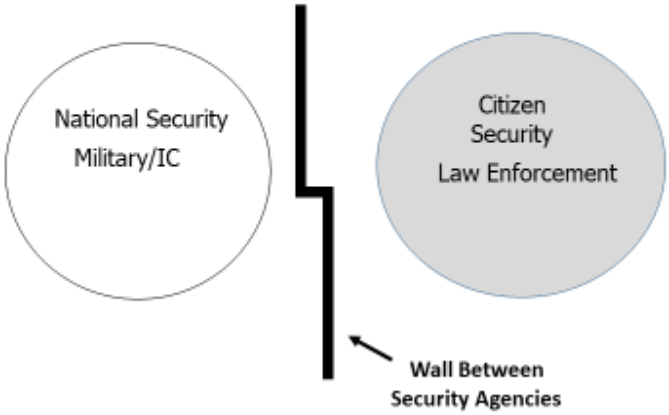
Heuer also highlighted how employing unaided judgment did not lead to a documented systematic analytic process. He explained how analytic procedures were usually not recorded and "remain[ed] largely in the mind of the individual analysts."[16] This lack of documentation limited the ability of other analysts to check the results for validity.

Reeling from the harsh critiques of the September 11 disasters and Iraqi WMD NIE investigations, in the 2000s, the IC initiated a two-pronged approach to improve its analysis. The first approach for improving analysis was the adoption of formal **critical-thinking** frameworks. DOD subordinate intelligence agencies (National Security Agency, Defense Intelligence Agency, National Geospatial Intelligence Agency, military service intelligence entities) led the charge in adopting a framework created by the California-based Foundation for Critical Thinking.[17] The second approach was the CIA and new National Counterterrorism Center's (NCTC) adoption of an emerging approach using both existing and newly created **structured analytic techniques** (SATs).[18] When the Office of the Director of National Intelligence (ODNI) formed after 2004, it mandated all IC analysts be taught and use the systematic methods of both critical thinking and SATs.[19] ODNI also published "Intelligence Community Directive 203, Analytic Standards,"[20] which was effectively a checklist or rubric (grading template) for evaluating analytic products prior to their publication. In the security policy community, there were no corresponding actions to improve security policy analysis. This book provides a foundational approach to using a combination of both critical thinking, SATs, and other analytic techniques and demonstrates their usefulness not only to intelligence analysis but also to the security policy community.

Conceptualizing Security

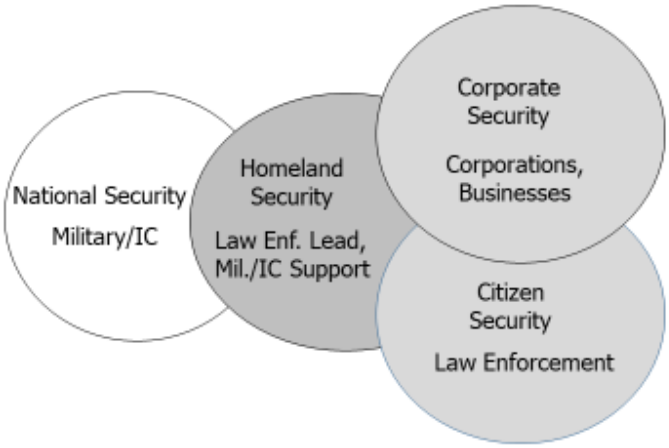
Security means different things to different people and the concept has changed over time. Prior to the 1980s, a model of U.S. security (depicted in Figure 1.1) could be described as non-overlapping circles for National Security and Citizen Security. The U.S. military and the IC were responsible for national security missions, i.e., protecting the United States from foreign aggression. Various federal, state, and local (tribal, county, city, town, etc.) law enforcement agencies were responsible for Citizen Security, i.e., protecting U.S. citizens from crime and violence. The few interactions between the Figure 1.1 National Security and Citizen Security communities included the areas of search & rescue, disaster response, major event security, and civil disturbance response. These limited-duration interactions were carried out under the legal authority of Title 10 U.S.C. and **Posse Comitatus.** Before the 1980s and continuing to today, U.S. government agencies complied with two primary existing federal laws defining the limits of U.S. military support to law enforcement agencies—10 U.S.C §271 - §284, Military Support for Civilian Law Enforcement Agencies, and 18 U.S.C §1385 "Posse Comitatus." In 10 U.S.C. are the details for how the military may legally provide information (intelligence), equipment, training, and maintenance support to civilian agencies. Posse Comitatus does not generally allow the U.S. military to become involved in civilian law enforcement searches, seizures, and arrests unless so directed by the Congress or President, which they have done almost 200 times since the late-1800s when Posse Comitatus was first enacted. Both 10 U.S.C. and Posse Comitatus support U.S. democratic governing tenets offering separation between the military and IC's foreign activities and U.S. domestic law enforcement. As a result of this separation, a "wall" developed between National Security and Citizen Security that severely restricted cooperation and information exchanges between these two key components of U.S. security.

Figure 1.1 Conceptualizing Security (prior 1980s)



In the 1980s, the U.S. security posture began to change. On October 14, 1982, President Ronald Reagan declared illicit drugs a U.S. national security threat. By the late-1980s, the **War on Drugs** was further advanced as both the U.S. military and IC were tasked to directly support U.S. counterdrug operations with intelligence, operating units, and logistical support. Military deployments and IC activities supporting counterdrug operations were conducted for the first time on a continuing year-round basis and in some cases DOD and IC officials were in charge of key counterdrug agencies and programs. For example, CIA created the interagency Counternarcotics Center (CNC), and DOD formed joint military and interagency task forces to conduct maritime and airborne counterdrug detection and monitoring operations. The War on Drugs necessitated changes to the conceptual structure for U.S. security. As relationships grew among agencies of the military, IC, and law enforcement—plus the later formation of the U.S. Department of Homeland Security (DHS)—it created today's security structure seen in Figure 1.2.[21]

Figure 1.2 Conceptualizing Security (post 9/11)



DHS was formed with the passage of the **2002 Homeland Security Act**. Unlike with counterdrug relationships dating back to the 1980s, before 2002 coordination and planning among U.S. government agencies in the areas of counterterrorism, border security, and immigration control had few formalized structures. The September 11 disasters revealed a need to develop a specific government department for coordinating interagency responses to counterterrorism and other threats to the homeland that were not necessarily specific to the military; thus, the creation of DHS. Today, the military and IC have become more deeply involved in domestic counterterrorism, border control, and immigration enforcement operations. Common across these Homeland Security missions are threats to public security (terrorism, illicit drugs, human trafficking, smuggling, immigration violations, foreign criminal gangs) where existing law enforcement agencies are often overwhelmed and need assistance from the military and IC. As DHS formed, protecting the U.S. critical infrastructure also became a priority mission. With the vast majority of U.S. critical infrastructure owned by the private sector, corporate security also became a key component of the U.S. security structure. This is depicted by the Corporate Security circle in Figure 1.2, an area requiring coordination and support from both Homeland Security and Citizen Security (law enforcement) agencies. This new U.S. security

structure, with overlapping security responsibilities, reduced—but did not totally eliminate—the "wall" between security agencies.

For the purposes of this book, security analysis includes two key components: **intelligence analysis** and **policy analysis**. Both of these components provide support to security decision makers. Larger agencies likely will have dedicated intelligence support staffs tasked to deliver analytic reports on threats and opportunities to the policy analysts, or at times directly to decision makers. It is then up to the policy analysts and decision makers to combine the intelligence reports with other information sources; consider political and resource constraints; develop a list of potential policy alternatives; and finally, decide which alternatives are best to pursue. In smaller organizations, the policy analysts may not have dedicated intelligence support and will be required to also complete the intelligence threat and opportunity analyses themselves.

A major tenet of intelligence analysis is that the reports provided policy analysts and decision makers must *never* recommend policy or solutions to the problem. The intelligence products must be non-partisan and not be influenced by the politics of the situation.[22] Intelligence analysis mainly deals with threats and opportunities the IC has identified where decision makers need to be alerted and informed. It is perfectly acceptable; however, for policy analysts or decision makers to request an intelligence analysis of the implications or consequences of certain policy alternatives.

Herein the use of the terms "security analysis" or "analyst" will indicate applicability to both intelligence and policy analysis. When the material is specific to the process of intelligence analysis or security policy analysis, those designations will be used in the text. The book will primarily address national security and homeland security examples, but the analytic techniques covered in the book are equally applicable to law enforcement and corporate security analysis—both for practitioners and academics.

Key Concepts

1947 National Security Act
2002 Homeland Security Act
Analyst
Behaviorism
Case Study Analysis
Critical Thinking
Director of National Intelligence
Evidentiary Reasoning
Historical Method
Intelligence Analysis
Joint Chiefs of Staff
Policy Analysis
Posse Comitatus
Office of Strategic Services
Reasoning by Analogy
Security Analysis
Structured Analytic Techniques
Unaided Judgment
U.S. Intelligence Community
U.S. National Security Council
War on Drugs

Discussion Points

1. Why did the United States not have an equivalent of the Office of Strategic Services or Central Intelligence Agency before World War II?
2. Why was the U.S. IC after the 1950s resistant to using behaviorism as a key analytic method?
3. Why did the U.S. security *policy community* (policy analysts and decision makers) not take action to improve its analysis and decision-making after the September 11, 2001, disasters and Iraqi WMD NIE failure?
4. Are there (or should there be) limits on the security support the U.S. military may provide to U.S. law enforcement under 10 U.S.C. and Posse Comitatus?

Notes

[1] Sun Tzu, *The Art of War*, trans. Samuel B Griffith (London: Oxford University Press, 1963).

[2] Thucydides, *History of the Peloponnesian War*, trans. Rex Warner (New York: Penguin Classics, 1954).

[3] Niccolò Machiavelli, *The Prince*, trans. Harvey C. Mansfield, Jr. (Chicago: The University of Chicago Press, 1985).

[4] Thomas B. Allen, *George Washington, Spymaster, How the Americans Outspied the British and Won the Revolutionary War* (Washington, DC: National Geographic, 2004).

[5] John H. Hedley, "The Evolution of Intelligence Analysis in the US Intelligence Community," in *Analyzing Intelligence, National Security Practitioners' Perspectives*, 2nd ed., ed. Roger Z. George and James B. Bruce (Washington, DC: Georgetown University Press, 2014), 23.

[6] Ibid, 23-24.

[7] Ibid, 24.

[8] Ibid, 33-35.

[9] US National Intelligence Council, "National Intelligence Estimate: Iraq's Continuing Programs for Weapons of Mass Destruction" (Washington, DC: Central Intelligence Agency, October 2002).

[10] National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report* (New York: W.W. Norton, 2004), https://www.9-11commission.gov/report/911Report.pdf (accessed June 25, 2018).

[11] "Report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction," March 2005, http://www.dtic.mil/dtic/tr/fulltext/u2/a441144.pdf (accessed June 25, 2018).

[12] Erik J. Dahl, *Intelligence and Surprise Attack, Failure and Success from Pearl Harbor to 9/11 and Beyond* (Washington, DC: Georgetown University Press, 2013), 128-159.

[13] Bryan Burrough et al., "The Path to War," *Vanity Fair*, December 19, 2008, https://www.vanityfair.com/news/2004/05/path-to-war200405 (accessed July 8, 2018).

[14] Richards J. Heuer, Jr., *Psychology of Intelligence Analysis* (Washington, DC: Central Intelligence Agency, Center for the Study of Intelligence, 1999).

[15] Richards J. Heuer, Jr., "Taxonomy of Structured Analytic Techniques," (paper presented at the annual meeting of the International Studies Association, San Francisco, CA, March 26-29, 2008), 3-4.

[16] Ibid, 4.

[17] See David T. Moore, *Critical Thinking and Intelligence Analysis* (Washington, DC: National Defense Intelligence College Press, 2009).

[18] See U.S. Government, "A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis," March 2009, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/Tradecraft%20Primer-apr09.pdf (accessed July 1, 2018). This publication demonstrates early work on structured analytic techniques.

[19] Office of the Director of National Intelligence, "Analytic Transformation, Unleashing the Potential of a Community of Analysts," (Washington, DC: September 2008), 17.

[20] Office of the Director of National Intelligence, "Intelligence Community Directive 203: Analytic Standards," (Washington, DC: January 2015), https://www.dni.gov/files/documents/ICD/ICD%20203%20Analytic%20Standards.pdf (accessed June 24, 2018).

[21] Figure 1.2 modified from A. Douglas Kincaid and Eduardo A. Gamarra, "Disorderly Democracy: Redefining Public Security in Latin America," in *Latin America in the World Economy*, ed. Roberto Patricio Korzeniewicz and William C. Smith (Westport, CT: Praeger, 1996), 211-228.

[22] Mark M. Lowenthal, *Intelligence, From Secrets to Policy*, 7th ed. (Thousand Oaks, CA: SAGE/CQ Press, 2017), 4-5.