The American approach to intelligence studies

James J. Wirtz

Introduction

Is there an American approach to the study of intelligence? The question calls to mind Russell Weigley’s *The American Way of War*, which suggested that Americans did in fact have a national “style” when it came to warfare. According to Weigley, Americans preferred to obliterate their opponents through attrition, not to use limited means for limited objectives. Although many have disputed Weigley’s characterization of the American way of warfare, his work renewed interest in the idea that the way officers and officials wage war is influenced by strategic culture, and this idea has been championed and contested by succeeding generations of strategic theorists. Yet, this debate about strategic military culture has not been mirrored by a similar discussion about the existence of a specific American approach to intelligence or intelligence studies.

Some might argue that it makes little sense to describe a national approach to intelligence or intelligence studies because any such characterization would have to reflect either unflattering stereotypes or overly generous depictions of a nation’s intelligence attributes or weaknesses. Moreover, it would be easy to think of an exception that disproves every observation about national style. For example, Americans are not particularly accomplished practitioners of denial and deception because they prefer to flaunt their superior military capabilities before potential opponents in the hope of getting them to comply with US demands without a fight. British officers and officials deserve the bulk of the credit for Allied deception operations during World War II. Analysts repeatedly warned about the effectiveness of Soviet *maskarova* (deception) during the Cold War, while noting that the United States lacked a similar capability. Yet, Barton Whaley, one of the greatest students of deception, is an American. Consequently, Whaley’s body of work could easily be used as a prima facie refutation of the idea that “Americans don’t do deception.”

National intelligence style also is a relative term. Americans’ apparent lack of interest in human intelligence (HUMINT) only becomes clear when one contemplates how Russian or Chinese intelligence agencies strive to cultivate networks of active agents and sleeper cells across the globe to seek out information of interest. Without a complete and consistent comparative framework for assessing intelligence culture, it will always be a simple matter to point out inconsistent, partial or biased characterizations of national intelligence efforts and scholarship. Additionally, by highlighting some scholarly efforts at the
expense of others, any attempt to identify a national approach to intelligence or intelligence studies will further downplay the part played by scholars, practitioners or literatures that are already in short supply in a given state.

With these caveats in mind, however, one may venture to characterize the American study of intelligence, which to some extent is also reflected in the actual conduct of foreign and domestic intelligence in the United States. Four factors shape the American approach to intelligence studies. First, Americans are relatively open even about their most secret intelligence organizations and practices. As a result of deliberate and inadvertent revelations about finished intelligence and the sources and methods employed in intelligence analysis, Americans periodically obtain accurate and important insights about the actual capabilities and state of affairs within the US intelligence community. Second, American intelligence professionals and scholars have embraced an intelligence paradigm that uses a combination of the scientific method and history to understand both intelligence pathologies and best practices. While some foreign intelligence agencies and scholars treat intelligence as a subject worthy of organized inquiry – here Israeli scholars and intelligence practitioners come to mind – most countries lack a scholarly community that addresses the subject of intelligence. Third, Americans focus on intelligence oversight and the issues raised by the presence of secret organizations within democracy. Indeed, concerns about the abuse of secrecy and surveillance have recently been exacerbated by intelligence activities undertaken on the domestic front in the Global War on Terror. Fourth, Americans have a strong bias towards technical intelligence. This emphasis on technical collection systems comes at the expense of HUMINT and better tradecraft, and creates an expectation that no area of the earth is beyond technical surveillance. Yet technical collection systems are not equally capable against all targets, and some opponents have become quite sophisticated in defeating “overhead surveillance” systems.

The chapter will unfold by discussing each of these traits that contribute to the American approach to intelligence. It will conclude by offering some observations about the ability of this style of intelligence study and practice to cope with today’s security challenges.

A culture of openness

The US intelligence community is made up of bureaucracies that work in secrecy and deal in secrets. Its personnel are screened through rigorous procedures to help prevent leaks of classified information and penetration by foreign intelligence agencies. Counterintelligence programs and hiring procedures also attempt to stop unstable people, who might have habits or weaknesses that make them vulnerable to blackmail, from ever getting on the intelligence payroll. Information also is restricted in terms of levels of secrecy and compartmentalization, i.e. regardless of one’s security clearance, access to information is granted on a “need to know” basis. In terms of day-to-day operations, the US intelligence community is set up to maintain the secrecy of its operations. Its output, finished intelligence, is intended for senior officials and officers. Most countries have intelligence organizations that would more or less match this description of the US intelligence community.

Compared to other nations, however, Americans appear to be remarkably open about discussing policies, procedures, failures and even the tradecraft employed by their intelligence organizations. There are several traditions that create this culture of openness. First, in the aftermath of strategic surprise, official intelligence post-mortems, often conducted by blue-ribbon commissions or Congressional committees, collect the facts about the disaster that has recently transpired. These committees attempt to determine exactly what intelligence shortfalls
contributed to the calamity, and to suggest fixes to prevent future instances of strategic surprise. The most famous, or at least the longest-lived, intelligence inquiry involved the surprise attack suffered by the United States at Pearl Harbor, Oahu on December 7, 1941. To date, there have been ten official investigations of this incident. In fact, the last, official word on the attack was issued December 15, 1995 when Undersecretary of Defense Edwin Dorn rejected a plea to restore posthumously Rear Admiral Husband E. Kimmel, USN (who was the commander of the US Pacific Fleet in December 1941) and Major General Walter Short, USA (who was responsible for the defense of Hawaii in December 1941) to their highest wartime rank. Similarly, the Congressional Joint Inquiry into the September 11, 2001 terrorist attacks on the United States, chaired by Senator Bob Graham and Congressman Porter Goss, and the subsequent 9/11 Commission (the National Commission on Terror Attacks) issued significant reports on the events leading up to the al-Qaeda strikes against the World Trade Center and the Pentagon. Influenced by the Pearl Harbor inquiries, especially the way Roberta Wholstetter used the findings of the penultimate investigation of Pearl Harbor, the Joint Congressional Committee on the Investigation of the Pearl Harbor attack, to write her famous treatise on surprise, *Pearl Harbor Warning and Decision*, the 9/11 commissioners attempted to capture the context of the September 11, 2001 disaster. The Commissioners wanted to create an historical record that would be a launching point for future scholarship on the tragedy. In the aftermath of intelligence failure, the American intelligence community has been subjected to intense public and official scrutiny, which creates a treasure trove of information for scholars interested in intelligence.

Second, accusations of scandal or abuse of intelligence power often push aside the veil of secrecy surrounding intelligence organizations, providing scholars with additional insights into relationships between officials and intelligence professionals. These investigations not only reveal much about the sources and methods used to produce finished intelligence, but also information about covert intelligence operations. Investigations by the Pike and Church Committees in the 1970s, for example, produced a laundry list of questionable Central Intelligence Agency (CIA) operations, everything from experiments with LSD to various assassination attempts against Fidel Castro. In a political atmosphere dominated by the US defeat in Vietnam and revelations about the Watergate scandal, many Americans believed that the CIA was a “rogue elephant” that was beyond the control of elected officials and standard government regulation. More recently, Congressional scrutiny of the Iran-Contra scandal during the Reagan administration provided insights into the shadowy world of covert operations and diplomacy. The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction also offered insights into US collection and analytic capabilities following the failure to assess accurately the status of Iraq’s ability to manufacture and stockpile chemical, biological or nuclear weapons.

Third, elected officials sometimes deliberately reveal classified information in support of US foreign policy and diplomacy. These revelations not only divulge classified information, but they also disclose much about the sources and methods that go into intelligence production. Probably the most famous and dramatic use of intelligence to bolster US diplomacy was undertaken by the John F. Kennedy administration during the Cuban Missile Crisis. On October 25, 1962, Ambassador Adlai Stevenson’s use of photo reconnaissance pictures taken by U-2 spy planes and low-level surveillance aircraft in a presentation at a UN Security Council meeting convinced the world that the Soviets were deploying ballistic missiles in Cuba, while simultaneously highlighting US photoreconnaissance capabilities. In a speech delivered to the nation on September 5, 1983, President Ronald Reagan also provided insights into US Signals Intelligence (SIGINT) capabilities by playing a tape of conversations between Soviet ground
controllers and the pilots of Soviet interceptor aircraft as they zeroed in on Korean Airlines Flight 007. The decision to release intercepts of Soviet military communication helped gain international support for the idea that the Soviet government and military acted in a reckless fashion by shooting down a civilian airliner on September 1, 1983, but it also revealed much about US SIGINT capabilities. In fact, Secretary of State Colin Powell’s speech to the UN General Assembly on February 13, 2003 incorporated misleading SIGINT and photographic intelligence of Iraq’s alleged WMD capabilities. Powell, who described the speech as “the lowest point” in his life, provided a convincing demonstration of the limits of technical intelligence and the weaknesses of US analytical capabilities.8

Fourth, in the United States, intelligence commissions and blue ribbon panels often attempt to identify problems and make recommendations to improve intelligence procedures or organizations.9 Several of these studies provided recommendations that would have improved coordination between the Federal Bureau of Investigation (FBI) and the intelligence community, possibly eliminating the “seams” between US domestic and international intelligence and law enforcement activities and institutions that were exploited by al-Qaeda on September 11, 2001. A report issued in 2000 by the National Commission on Terrorism, which was headed by Ambassador Paul Bremmer, for example, called for a series of reforms that would have improved the ability of the US intelligence community to meet the terrorist threat. The Commission called for measures clarifying the FBI’s authority to investigate terrorist groups, eliminating CIA regulations that hindered the use of informants linked to terrorist organizations, placing terrorism high on the agendas of officials at the CIA, FBI and National Security Agency, and establishing new reporting procedures to deliver quickly information related to terrorism to all interested officials.10

Fifth, deliberate or inadvertent leaks of classified information are commonplace. Much to the chagrin of intelligence professionals, elected officials can and do reveal classified information when they believe that such information should be in the public realm or if disclosure becomes a convenient means to achieve a political end. Sometimes the disclosure of classified information is inadvertent. Sometimes it is undertaken because it is sensational or helps to undermine existing policies. Classified information that the intelligence community had monitored overseas calls made by US citizens, maintained prison facilities for terrorist suspects in foreign countries, or even monitored mosques in the United States for evidence of radioactive substances became public, despite the fact that these programs were considered important national security secrets. This unauthorized and illegal disclosure of classified information gives intelligence professionals fits,11 but as long as officials have an interest in providing this information to the press, “leaks” will remain commonplace.

When combined, intended and unintended disclosures of finished intelligence reports, information about intelligence operations, and insights into intelligence sources and methods provide scholars with large amounts of what was recently classified information from secret organizations. This information provides a sufficient historical record to support serious scholarship on intelligence matters in the United States. Few states generate as much documentary evidence about their intelligence activities as the US government, and this relative openness is a necessary condition for the American approach to intelligence.

The intelligence paradigm

The intelligence paradigm developed by the American scholarly community is an effort to apply analytic methodologies and insights drawn from the social sciences, to understand the
fundamental nature of intelligence, to explain the history of intelligence successes and failures, to understand intelligence organizations and processes, and to assess and improve upon the craft of analysis itself. While Israeli and British scholars have contributed greatly to this paradigm, other states and scholarly communities often fail to apply any sort of social science methodology to their study or production of intelligence. For instance, Soviet intelligence services, the KGB (Komityet Gosudarstvennoii Bezopasnosti) and the GRU (Glavnoe Rasvedyvatel'noe Upravlenie) relied on espionage or the open press for information and largely functioned as a clipping service for the Kremlin. During the Cuban Missile Crisis, Soviet Premier Nikita Khrushchev also served as his own intelligence analyst. Because many dictatorships have used intelligence agencies as instruments of domestic surveillance and terror, the “counterintelligence state,” in its many varieties, was never a safe subject for study by those subjected to its abuses.

Political scientists, historians, psychologists and practitioners have all played an important part in creating the intelligence paradigm. Those who work within this paradigm, unlike most other endeavors in the social sciences, share a general agreement about methodology, data, the issues to be addressed, and the problems that remain to be resolved. Most are concerned with exploring the intelligence cycle: setting intelligence requirements, collecting data, analyzing data, and disseminating finished intelligence. Alexander George, for example, has suggested that intelligence failure can occur at any point in the intelligence cycle, if intelligence professionals and policymakers fail to answer any one of six questions: (1) identifying the adversary (who?); (2) estimating the probability of attack (whether?); (3) determining the type of action involved (what?); (4) determining the location of the attack (where?); (5) estimating the timing of the action (when?); (6) determining the motivation behind the initiative (why?). This scholarship strives to understand why failures of intelligence occur and to devise best practices when it comes to analyzing and disseminating intelligence.

In their search for answers to the questions that frame the intelligence paradigm, scholars and practitioners focus on four levels of analysis: factors that are idiosyncratic to the production of finished intelligence; human cognition; organizational behavior; and the relationship between the intelligence community and policymakers. In terms of idiosyncratic factors, analysts often explore problems that complicate the intelligence cycle. The “Cry Wolf” syndrome, for example, occurs when analysts repeatedly sound false alarms that causes recipients to dismiss what eventually turns out to be a legitimate alert. The “Ultra” syndrome, named after the codeword given to Allied signals intelligence intercepts during World War II, occurs when analysts become overly reliant on an accurate and timely source of information. Although the information revolution has created many benefits and challenges for society, it also has introduced new intelligence pathologies. Observers ritualistically point out that analysts are constantly at risk of being overwhelmed by a deluge of information from both open and classified sources. Yet, the real danger may be the fact that, within this data stream, there is little valuable information about the highest priority targets and issues facing analysts. Additionally, the demand for current, original and even entertaining intelligence products is so great that the drumbeat of constant intelligence warning and analysis output may take on a life of its own, creating an impression of certainty, threat, and immediacy that is not justified by the contents and data used in the production of finished intelligence.

Scholars have turned to human cognition and psychology to understand both intelligence successes and failures. Scholars have identified several common cognitive biases that can impede analysis. Mirror imaging, the tendency to interpret another actor’s behavior using one’s beliefs, experiences, values, or standard operating procedures, can impede the creation of accurate estimates. Individuals also tend to see the behavior of other actors to be highly rational in the
sense that all policy and action is directed toward achieving specific objectives, even though similar behavior is beyond their own personal or even bureaucratic capacity. A host of these biases can bedevil analysts; practitioners have even devised methodologies to help analysts avoid common cognitive errors.

Today, many observers criticize analysts for a lack of imagination or a failure to “connect the dots” when it comes to anticipating the nefarious activities of terrorist syndicates or the next move made by the megalomaniacal leaders of kleptocracies. There is, in fact, a little recognized “rationality bias” inherent in official analysis, making it difficult to acknowledge truly irrational or maniacal behavior on the part of states, criminal syndicates or terrorist networks. Yet, what generally inhibits “imaginative” analysis is “the concept”: shared assumptions among analysts and policymakers of what constitutes rational behavior on the part of a potential opponent. Prior to the 1973 Yom Kippur War, for example, Israeli officials based their defense policy on three assumptions: Egypt would be at the center of any Arab coalition against Israel, Egypt would not undertake a significant attack without a strong prospect of victory, and, unless Egypt destroyed the Israeli Air Force, an Arab victory was not possible. Israeli officials also believed that their intelligence agencies would provide a “war warning” in time for them to mobilize their reserves or even launch a pre-emptive attack, actions that would produce an Arab rout. The effects of “the concept” on policymakers and analysts alike was staggering. Even though they were equipped with actual Syrian and Egyptian war plans, reconnaissance photographs showing unprecedented force deployments along the Suez Canal and Golan Heights, a warning from a credible and trusted spy within the inner circle of the Egyptian government, information that Soviet personnel and dependents were high-tailing it out of Cairo and Damascus, and signals intelligence suggesting that their opponents were about to strike, the Israelis never managed to act as if they were about to be hit by an all-out Arab assault. As a result, the outbreak of the 1973 Yom Kippur War was marked by one of the greatest intelligence-command failures in military history. The “concept” held sway, despite some unusually compelling contradictory evidence. Similarly, the idea that Saddam Hussein had used chemical weapons, had gone to great lengths to procure WMD, and appeared willing to bear enormous costs to hide his WMD infrastructure from the prying eyes of UNSCOM, was seen by US analysts as prima facie evidence that Iraq retained a WMD capability. Their concept of Iraqi behavior and intentions, not hard evidence, shaped analysts estimates of Iraq’s WMD capability.

Scholars also have turned to organizational behavior for insights into the production of finished intelligence. Compartmentalizaton, for example, is endemic in intelligence production because the “need to know” principle governs individual analysts’ access to information. But organizations are jealous guardians of information and bureaucratic rivalry or differences in standard operating procedures can slow the flow of information within organizations or across the intelligence community to a trickle. Bureaucratic rivalry also can take on a life of its own; the quest to trump analysts from other organizations can take precedence over the effort to serve the needs of policymakers. Small-group dynamics can also shape intelligence estimates: the well-known phenomenon of “group think” can emerge among small teams of analysts and intelligence managers. Institutional affiliation also tends to color one’s perceptions and prescriptions, and it is a rare analyst or manager who will advance a position that is at odds with the interests of his or her home organization or career interests. Bureaucracy itself – hierarchy, specialization, centralization, routine, and secrecy – and the need to continuously justify budgets and priorities, which creates an endless reporting requirements and innovative “metrics,” all work to impede creative thinking and effective analysis.

The fourth level of analysis, the intelligence–policy nexus, focuses on how relations between intelligence professionals and policymakers shape the dissemination and
intelligence and warning. A variety of problems can emerge to bedevil relations between the intelligence and policymaking communities. The best-known pathology, politicization, emerges when policymakers place overt or subtle pressure on intelligence analysts and managers to produce intelligence estimates that support current political preferences or policies. Although there is no consensus about what constitutes best practices when it comes to intelligence–policy interaction, two schools compete as a guide to relations between policymakers and the intelligence community. One school of thought, most closely associated with the work of Sherman Kent, focuses on ensuring the independence of intelligence analysts. Kent’s thinking, which shaped the evolution of the US intelligence community, identifies the importance of political and policy detachment in producing finished intelligence. The other school, most closely associated with the reforms instituted in the mid-1980s by then Director of Central Intelligence Robert M. Gates, focuses on producing “actionable” intelligence, information of immediate and direct use to policymakers. To produce actionable intelligence, analysts have to maintain close working relationships with policymakers, literally looking into the policymakers’ inboxes to make sure finished intelligence addresses important policy issues of the day.

Scholars also are beginning to explore new developments in the intelligence–policy nexus. The information revolution is creating new points of friction as intelligence analysts and policymakers interact using less formal channels of communication, producing new challenges for those charged with monitoring the contents of finished intelligence – formal written reports that reflect a deliberate judgment made by analysts and backed by the intelligence community. Other scholars are focusing on the political costs of responding to surprise. In contrast to the tentative estimates often offered by the intelligence community, the costs of responding to possible threats are clear, which makes elected officials leery of responding to warnings that might turn out to be false alarms. To overcome this reluctance to act on all but the most compelling warning, new ways to undertake limited alerts of military and police forces have to be devised, eliminating the need to place an entire city on a “war footing” in response to uncertain threat assessments.

**Intelligence oversight**

Students of public policy and government also have contributed to the American approach to intelligence studies by undertaking an open and evolving project dealing with the oversight of secret organizations within a democracy. The United States is based upon the idea of limited government: intelligence operations and intelligence agencies are subjected to uneven government oversight. During the Cold War, many elected officials believed that the intelligence community needed to be given free rein, at least overseas, in fighting the militarily powerful Soviet Union and the ideological menace posed by communism. In the aftermath of the Vietnam War, however, this attitude changed and during a series of hearings in 1975, Congressional committees heard about a variety of misdeeds perpetrated by the intelligence community: plots to assassinate foreign leaders, wiretaps, drug experiments and plans to conduct surveillance against US citizens who chose to express their right to protest government policies. In response to these revelations of misconduct, improved Congressional and executive branch oversight was launched: the Senate Select Committee on Intelligence, the White House Intelligence Oversight Board, and a House Permanent Select Committee on Intelligence were all created during the 1970s.

The academic question at the heart of intelligence oversight has been stated succinctly by
Marvin Ott: “Can a democracy maintain an effective, capable intelligence service without doing violence to the norms, processes and institutions of democracy itself?”

Thus, the debate about intelligence oversight is generally between those who want more Congressional effort to monitor intelligence activities and to protect civil liberties, and those who believe that too much oversight can hamper the intelligence community, especially in its conduct of covert operations overseas and domestic intelligence-gathering. In the American context, democracy usually trumps the needs of secret organizations: Congress, an institution based on the open, public debate of policy issues, has responsibility for oversight of the intelligence community. But the proper balance between secrecy and openness, between the needs of national security and civil liberties, at least from a political perspective, reflects threat perceptions. When threats are high, most observers seem willing to give the intelligence community more leeway. When threats are reduced – a time when past “intelligence abuses” often become public – most observers clamor for greater intelligence oversight.

The September 11, 2001 attacks revealed that terrorist cells had indeed penetrated the United States and that al-Qaeda was committed to killing Americans. Events overseas – the bombings in 2004 of Madrid trains, of Bali tourists in 2002 and 2005, of the Marriott Hotel in Jakarta in 2003, and in 2005 of the London Underground and Amman hotel – continue to highlight the fact that al-Qaeda and its sympathizers are hell bent on creating death and destruction. To many observers, this ongoing threat is evidence of a need to strengthen US foreign and domestic intelligence and police efforts. Debate about these efforts, and the renewal by Congress of the USA Patriot Act of 2001, are just the latest chapters of the ongoing debate about the role of secret organizations and surveillance in democracy. This dialogue is likely to continue indefinitely because scholars, and the American public, want both civil liberties and a shield against foreign threats. As Loch Johnson has recently noted, both scholars and intelligence practitioners alike will continue to “search…to find the right formula for power sharing in this most difficult of government domains – knowing full well that no formula exists, only the hope that in the spirit of comity, the Congress, the executive, and the courts will carry on the quest for a modus vivendi that takes into account liberty and security.”

The American technological bias

Americans have an obsession with technology, which is reflected in their approach to intelligence. US HUMINT efforts are relatively undeveloped. Intelligence managers are limited in their ability to traffic with the kinds of unsavory characters who are able to penetrate terrorist or criminal networks. Gaining access to agents in “denied areas,” a significant problem during the Cold War, still hamstrings HUMINT operations today. Targets of greatest interest – North Korea comes to mind – are probably the most closed and tightly policed societies in the world. Intelligence managers and analysts increasingly turn to open-source intelligence (OSINT) to make up shortfalls in HUMINT, but they apparently have a bias against over-reliance on sources readily available to the public. If the Internet is all that is required to stay informed, then who would need special organizations with access to secret information?

Since the early 1960s, analysts have come to rely increasingly on technical collection methods to access denied areas of interest or for general surveillance. Some of these systems are ground-based or rely on aerial reconnaissance, but most of them are deployed in space and are dependent on satellite access to low-earth or geo-synchronous orbit. The best-known technical collection systems rely on satellite photography (imagery) or IMINT. Originally based on technology requiring the physical retrieval of exposed film, which parachuted to earth
in a capsule, today’s IMINT satellites can provide digital high-resolution images in real time. SIGINT, or signals intelligence, is eavesdropping on all sorts of communication and often provides insights by listening into unencrypted conversations. Over time, even encrypted transmissions can be made to reveal important information. By undertaking analysis of encrypted communications, command relationships as well as patterns and levels of activity can be discerned. The movements of specific individuals can be tracked, especially if they use cellular or satellite telephones to communicate. Measurement and Signatures Intelligence (MASINT) is the collection of information about the capabilities and location of an opponent’s electronic systems or even industrial processes. For instance, waste plumes emanating from smokestacks can be monitored to detect the presence of trace elements associated with the manufacture of chemical weapons.

Although the American fascination with and reliance on technical collection systems has yielded enormous benefits, these systems also create costs. There is a tendency, for example, to believe that they have increased international transparency and that virtually nothing is beyond their reach. In reality, technical collection systems are best at monitoring significant industrial processes and manufacturing operations, large military units, and crew-served weapons. Small manufacturing operations and micro-scale industry are difficult to identify. Individuals or small units can blend into the background of everyday activities, making them difficult to detect or monitor. Some opponents also are aware of US surveillance capabilities and can take rudimentary measures that significantly degrade the ability of US systems to monitor their activities.30 The emphasis on technical collection systems also draws interest and attention away from HUMINT and efforts to improve tradecraft. Technical collection is important, but it must be incorporated into an effective analytical process to yield real benefits.

In lieu of conclusions

Is there an American approach to intelligence studies that differs from other national styles? This chapter suggests that the American approach to intelligence and intelligence studies shares several characteristics that support this idea. Americans live in an open society and are kept relatively well informed through a variety of inadvertent and deliberate revelations about the intelligence community. American scholars also combine history and an approximation of the scientific method to study intelligence pathologies and best practices. Indeed, the intelligence paradigm emerged nearly twenty years ago and continues to produce a coherent research agenda. American scholars and practitioners also devote much attention to understanding the role of secret organizations within democracy and devising the proper balance between effectiveness and restraint when it comes to intelligence organizations. The American fascination with technology also influences the US approach to intelligence collection: practitioners and scholars alike are preoccupied with technical collection systems at the expense of other methods for collecting information.

American and non-American participants in the intelligence paradigm exhibit a vitality not present among other scholarly communities. Unlike other countries, where the study of intelligence might be underdeveloped or even taboo outside of official circles, intelligence studies are considered to be a legitimate academic field within the United States. Scholars continue to address new problems uncovered by the latest intelligence fiasco or to devise better methods of intelligence oversight. In a negative sense, a preoccupation with technology threatens the American analytic tradition as both scholars and practitioners mistakenly seek technical solutions for problems rooted in the limits of human cognition or bureaucracy. Yet, as
long as a spirit of inquiry animates the American study of intelligence, scholars will continue to search for best practices and to understand how new security threats create unique intelligence challenges. The American approach to intelligence studies has no ready response to these challenges, but it does have a community of scholars who are willing to address the issues confronting not only the intelligence communities, but the societies in which they are embedded.

Notes

3 Walter Jajko makes the point well: “The United States armed forces, despite the revolutionary rhetoric of the National Military Strategy concerning the information dominance of the battle-space, are predisposed to attack an enemy’s capabilities, not an enemy’s strategy. Systematic shaping of an enemy’s strategy and attacking an enemy’s intentions through deception in peacetime are unusual undertakings.” See “Commentary,” in Roy Godson and James J. Wirtz (eds.), Strategic Denial and Deception: The Twenty-First Century Challenge (New Brunswick, NJ: Transaction Publishers, 2002), pp. 115–122.
13 For example, see Ephraim Kam, Surprise Attack: The Victim’s Perspective (Cambridge, MA: Harvard University Press, 1988); and Ariel Levite, Intelligence and Strategic Surprises (New York: Columbia University Press, 1987).
16 Thomas C. Bruneau, “Controlling Intelligence in New Democracies,” International Journal of Intelligence and Counterintelligence Vol. 14 (Fall 2001), pp. 323–341. The term “counterintelligence state” was coined by John Dziak to describe the Soviet Union, a state where the domestic police/ intelligence function was synonymous with the dominant governing body of the state. See John


18 Kam, *Surprise Attack*, pp. 42, 64, 186.

19 *Report to the President of the United States*, pp. 12–14.


21 Richards J. Heuer, Jr., *Psychology of Intelligence Analysis* (CIA: Center for the Study of Intelligence, 1999).

22 “The concept” was the term originally coined by the Agranat Commission Investigation into the failure of Israeli intelligence prior to the Yom Kippur War; see Ephraim Kahana, “Early Warning Versus the Concept: The Case of the Yom Kippur War 1973,” *Intelligence and National Security* Vol. 17 (Summer 2002), pp. 81–104.


29 Johnson, *Bombs, Bugs, Drugs and Thugs*, p. 222.