CSI CENTER FOR THE STUDY OF INTELLIGENCE

Washington, DC 20505

EDITORIAL POLICY

Articles for *Studies in Intelligence* may be written on any historical, operational, doctrinal, or theoretical aspect of intelligence.

The final responsibility for accepting or rejecting an article rests with the Editorial Board.

The criterion for publication is whether, in the opinion of the board, the article makes a contribution to the literature of intelligence. The board comprises current and former members of the Intelligence Community.

EDITORIAL BOARD

Jozlyn Schroeder (Acting Chair)
Mozella Brown
Shannon Corless
Dawn Eilenberger
Brent Geary
Andrew Hayden
Martin Kindl
Maja Lehnus
Stacey Pollard
Mark Sheppard
Linda Weissgold

EDITORS

Andres Vaart (Editor)
Doris Serrano (Graphics Design)

STUDIES IN INTELLIGENCE

Contents

Vol. 70, No. 3 (Extracts, September 2026)

Counterterrorism and Homeland Security

Operation Goldenrod
The Capture of Terrorist Fawaz Yunis **1**
Adam and Vikki

The Mosaic of Homeland Security Intelligence **19**
COL. James Chastain, USA (Ret.)

Artificial Intelligence and Analytical Tradecraft

AI and Expertise: Intelligent Delegation for Intelligence Analysts **27**
William Martin

Judgment Under Tempo: Tradecraft in a Digital Intelligence Environment **33**
Justin K. Edmondson, PhD

Software-Defined Intelligence: Thinking About Tradecraft **39**
William Schlickenmaier

Analogical Reasoning in Intelligence Analysis **49**
Ryan Handy

Reflections on the Intelligence Profession

Secrets and Secrecy: The Case for a Practitioner's Dialogue **57**
Joseph Gartin and Timothy Schulz

Intelligence in Public Media

Agents of Change: The Women Who Transformed the CIA **69**
Reviewed by John M. Pulju

The Closing of the Russian Mind: How Putin's Ideology Took the Nation Hostage **71**
Reviewed by John Ehrman

(Continued on the following page.)

Intelligence in Public Media (Cont.)

At Sea Against the Soviet Fleet: The Evolution of U.S. Navy Operational Intelligence in the Cold War **75**
Reviewed by Scott A. Moseman, PhD

The Writer and the Traitor: Graham Greene, Kim Philby, and the Great Betrayal **79**
Reviewed by Ian B. Ericson

Ike and Winston: World War, Cold War, and an Extraordinary Friendship **81**
Reviewed JR Seeger

G.I. G-Men: The Untold Story of the FBI's Search for American Traitors, Collaborators, and Spies in World War II Europe **83**
Reviewed JR Seeger

John Ehrman's Summer Reads **85**
Cromwell's Spy: From the American Colonies to the English Civil War, the Life of George Downing
A Stranger in Corfu (a novel)
The Shame Archive (a novel) ■

Contributors

Article Contributors

Adam and Vikki (pen names) are retired officers of CIA's Counterterrorism Center.

COL. James Chastain has served nearly three decades in the US Army and IC. 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 NGA. He is a doctoral candidate at Vanderbilt University.

Justin K. Edmondson, PhD, is a senior analyst at the Farragut Technical Analysis Center, Office of Naval Intelligence.

Joseph Gartin is a retired CIA officer and past managing editor of Studies. ***Timothy Schulz*** is a program manager in the Center for the Study of Intelligence.

Ryan Handy **is** studying at the National Intelligence College of the NDU and a graduate of The Johns Hopkins School of Advanced International Studies. From 2022 to 2026, he led an analytic tradecraft evaluation program of the Office of Intelligence and Analysis of DHS. Before that, he was an analyst and liaison officer for DoD, serving in various overseas assignments and Washington, D.C.

William Martin is the pen name of a counterintelligence analyst.

William Schlickenmaier is a former CIA senior analyst.

Reviewers

John Ehrman is a retired CIA officer and a frequent contributor of reviews of intelligence literature, both fiction and non-fiction. His first review for *Studies* appeared in *Studies* in 2000.

Ian B. Erickson is the pen name of a CIA officer.

Scott A. Moseman is a retired Naval Intelligence officer, who is presently a member of the Department of Military History at the Command and General Staff College in Fort Leavenworth, Kansas.

John M. Pulju is a retired CIA officer and past chair of the *Studies* Editorial Board.

J. R. Seeger is a retired CIA officer. ■

Vice President George H.W. Bush (seated in the floral armchair in front of the group) hosts senior officials and members of the Operation Goldenrod team, including the co-authors of this article, at his Naval Observatory residence after the capture of terrorist Fawaz Yunis. CTC Director Dewey Clarridge is seated on the right, in the floral chair nearest the camera. (White House photo)

Operation Goldenrod

The Capture of Terrorist Fawaz Yunis

Vikki and Adam (pen names)

Vikki retired from CIA after 32 years of service, including as a founding member of the CIA Counterterrorist Center. Adam's career spanned more than 50 years, including service in the US Army, CIA, and State Department. Among other recognitions, he was awarded the Intelligence Star for Bravery. Adam and Vikki were leaders of the CIA "extraction" team in Operation Goldenrod.

Early on a cold, overcast morning on September 13, 1987, three people boarded a small fishing boat in Cyprus and headed into the Mediterranean Sea. The fog had not yet lifted. Operation Goldenrod was under way. The operation's aim was to arrest and transport a Lebanese terrorist, Fawas Yunis, to the United States to stand trial for acts of terrorism against US citizens. Operation Goldenrod was the first operation targeting a terrorist overseas undertaken by the recently created CIA Counterterrorist Center. Under the auspices of the White House and National Security Council, the operation fostered extensive, close planning, collaboration, and cooperation between federal law enforcement, diplomatic, intelligence, and military services. The operation had to be accomplished in such a way as to ensure it was legal under US and international law. Yunis would be tried, convicted, and sentenced to 30 years in prison in 1989.

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.

Terrorism in the 1970s and mid-1980s

Terrorism seldom has a clear beginning or a distinct ending. It has no shape, no structure and, in military parlance, no identifiable forward edge of battle (no front line). Terrorism changes; it evolves and transforms. Critical variations emerge; tactics change; new groups form, while some groups merge with existing groups or merely fade away. Technological innovations provide terrorists new capabilities in designing or undertaking attacks, which may have global impact. Terrorism was not a new phenomenon when discussions leading to Operation Goldenrod began in 1986.

By the 1970s, international terrorism had become rampant. Nationalist/separatist terror organizations, many with Marxist-Communist orientations, sought forms of self-determination or national liberation. Active in Europe, Asia, Africa, Middle East, South America, and the United States, these groups conducted attacks worldwide. Palestinian terror groups, some aligned with the Palestine Liberation Organization, sought the establishment of a Palestinian nation. Kidnappings, aircraft hijackings, bombings, and suicide operations were at the forefront of attacks, many gaining international media attention.

By the mid-1980s, a number of nationalist/separatist terror groups were no longer active or had merged with other terror groups. At the same time, new terror groups had emerged, such as Hizbollah and the Islamic Jihad Organization (IJO) in Lebanon. Amorphous terrorist groups also sprung up in Afghanistan after the Soviet occupation of that country in 1979. Nineteen-eighty-five was a violent year for terror attacks, including:

- January–June 1985: Four Americans were kidnapped in Beirut, Lebanon, and held captive by terrorists associated with the IJO.
- June 11–14: Royal Jordanian Alia Flight 402 en route from Rome to Athens was hijacked and its crew and passengers, including two Americans, held for four days in Beirut.
- June 14–30: Hizbollah terrorists hijacked TWA Flight 847 on the same day the Alia Flight 402 hijacking ended. The hijackers beat US Navy diver Robert Stetham to death and threw his body to the tarmac. Over two weeks, some passengers were released while others were removed from the aircraft, dispersed in small groups, and held under guard in Beirut's southern suburbs.
- September 16: Terrorists lobbed grenades into the Café de Paris restaurant in Rome, wounding 38, including nine US citizens.
- October 7–10: The cruise ship *Achille Lauro* was hijacked by Palestine Liberation Front (PLF) terrorists. US citizen Leon Klinghoffer was shot and tossed overboard while confined to his wheelchair.
- December 27: near-simultaneous machine gun and grenade attacks at airports in Rome and Vienna left more than 20 people dead, including five US citizens, and wounded 120.[1]

Moving Into Action

The series of terrorist attacks would lead to a whole-of-government response, beginning with White House authorization to engage CIA in counterterrorist operations abroad, with or without the approval of foreign governments.

Congress, too, came into play, months later enacting the Omnibus Diplomatic Security and Anti-Terrorism Act of 1986, which established extraterritorial jurisdiction over terrorist acts overseas against US persons or interests.[2] The act was a landmark law that, among its provisions, strengthened security for diplomatic personnel (and family members) and facilities, established a rewards program and expanded Federal jurisdiction to investigate terrorist acts against

US persons or properties overseas and to arrest those responsible.[3] Two years earlier, Congress had passed the Comprehensive Crime Control Act of 1984 which gave the FBI jurisdiction over terrorist acts in which Americans were taken hostage or injured, no matter where the act of terrorism had occurred.[4]

The 1986 act principally affected the State Department and diplomatic security, which defined terrorism as "premeditated, politically motivated violence perpetrated against noncombatant targets by sub-national groups or clandestine state agents, usually intended to influence an audience. International terrorism is terrorism involving citizens or territory of more than one country."[5]

CTC Established

At the same time, Director of Central Intelligence (DCI) William Casey had also recognized the need for stronger action against terror organizations and was prepared quickly to act on the White House authorization. In February 1986, he announced the creation of the DCI Counterterrorist Center (CTC) and placed its establishment and management under the CIA's Directorate of Operations (DO). Before CTC's creation, counterterrorism had been handled by the Counterterrorist Group of the DO, while the Directorate of Intelligence (DI) maintained its own office for counterterrorism analysis.

CTC would officially be established in April 1986 and placed under the leadership of Duane "Dewey" Clarridge. At the time, the center was unique in that it colocated CIA terrorism specialists from its then four directorates (the DO, DI, Science and Technology (D&T), and Support (DS) to counter and respond to terrorism. The center would also have substantial IC representation in its ranks. CTC was the first center of its kind in CIA.[a]

Under Clarridge's leadership, CTC implemented a proactive stance, going beyond just responding to terror attacks to implementing operations designed to prevent or thwart terror attacks. Simply stated, CTC's mission was to preempt, disrupt, and defeat terrorism. Senior officers in CTC and the FBI recognized that, at its core, a terror attack (or threat to conduct an attack) is a criminal act and, as such, terrorists must be prosecuted for their actions.

Before any prosecution, however, suspects must first be identified and arrested. CTC would work with other federal offices to identify and pursue terrorists responsible for attacks involving US citizens and ensure their arrest and prosecution in US courts. In September 1987, *Operation Goldenrod* did just that.

Selecting the Target

From mid-1986 into 1987, US law enforcement, intelligence, and military entities worked jointly under the auspices of the White House and the NSC to design, implement, and undertake an operation to 1) arrest any foreign terrorist involved in attacks against US citizens and interests overseas; 2) transport captives to the United States; and 3) arraign captive terrorists in a US federal court. Meetings were held to identify foreign terrorists who would meet the criteria and might be accessible for arrest.

In his memoir, *A Spy for All Seasons: My Life in the CIA*, Clarridge recalled some of the terrorists on CTC's radar at the time:

- Muhammad Rashid, a Jordanian linked to the Palestinian 15 May terror organization, for his role in placing an explosive device on Pan Am Flight 830, from Tokyo to Hawaii, in 1982. The device detonated over the Pacific Ocean, perforat-

a. In 2015, the center construct became the norm for CIA when, under the rubric of "modernization," an agency-wide reorganization created a fifth directorate, Digital Innovation, and ten integrated "mission centers," including CTC. The number and nature of the missions of centers would evolve until 2026; today, CIA has 11 mission centers, three of which did not exist in 2015 at the time of the reorganization.

Map of Cyprus. Operation Golden Rod activities were concentrated around Limassol and Larnaca on the southern coast.

ed the aircraft's cabin, killed a Japanese teen, and injured 16 other passengers.[6] (Husayn Muhammad al-Umari, aka Abu Ibrahim, remains on the FBI's Most Wanted Terrorist List for his role in this bombing.)

- Imad Mughniyah, associated with Hizbollah, for his role in the hijacking of TWA-847, which initially involved 153 passengers and crew (including many US citizens), and for his suspected involvement in the kidnapping and detention of US citizens in Lebanon.
- Fawaz Yunis, Lebanese Amal terrorist, as a hijacker of Royal Jordanian Alia 402 on which three US citizens were passengers, and his role in the detention of US citizens who had been passengers on TWA-847.

By February 1987, the focus of the investigation had turned to Fawaz Yunis.[a] One factor in the selection of Yunis—indeed, the pivotal one—was a DEA source, Jamal Hamdan, who had indicated to his DEA handlers that he had known Yunis since the early 1980s, when both lived in Beirut. After Hamdan relocated to Cyprus, the two remained in touch. According to Hamdan, Yunis needed money to support his wife and two children and might be interested in entering the lucrative drug business. According to Clarridge, the means to make Yunis "accessible" quickly became evident.[7] Operation Goldenrod was approved to arrest Yunis in an "extraction" operation, "as in the removal of a bad tooth."[8]

Operational Planning Begins in Washington…

DCI Casey oversaw the initial planning for Operation Goldenrod, while the principal responsibility for its execution fell to Clarridge

a. Fawaz Yunis's surname is often rendered in writings involving him, including FBI histories, as Younis. Court documents related to his trial during 1988–89 render the name as we do here.

and CTC.[9] In the NSC meetings, Casey, and later William Webster, represented the IC and CIA.[10] At the NSC Coordination Subgroup (CSG) meetings held at the White House, members became more focused as the operational plans developed and meetings increased as Operation Goldenrod drew nearer. In his autobiography, *A G-Man's Journal*, retired FBI Executive Associate Director Oliver "Buck" Revell noted the main participants at the NSC/CSG meetings were Amb. L. Paul Bremer (State Department), Richard Armitage (Defense Department), Lt. Gen. Tom Kelley (Joint Chiefs of Staff), Clarridge, Revell, and Charlie Allen (IC). Others also served on the NSC/CSG, but those listed above were the most essential members.[11]

In his memoir, Clarridge described how the Department of Justice (DOJ) set most of the ground rules. "CIA would run the extraction operation—up to a point." DEA would turn their source, Jamal Hamdan, over to the CIA for handling. Clarridge wrote: "We would dangle the bait, set the trap, and be sure that the target was delivered into the FBI's hands in international waters."[12]

CIA would be required to place "eyes on the target" at the start of the operation to confirm the person to be arrested was, in fact, the Fawaz Yunis who had participated in the Royal Alia hijacking. The FBI would then take custody, as CIA does not have authority to arrest individuals.[13]

Once FBI special agents took custody of Yunis, they would formally arrest him and accompany him to the United States. The US Navy would transport Yunis and the agents holding him to US soil on its ships and aircraft. Once there, DOJ would prosecute the case. To ensure a clean, unbroken line of jurisdiction, Yunis was to be "apprehended in international waters or airspace, remain solely in FBI custody, and avoid the territory of a sovereign nation."[14]

For his participation, Jamal Hamdan had a requirement: asylum for him and his entire family in the United States to protect them from retaliation after his role in delivering Yunis to the FBI became public. Enter the Department of State into the conversation. Because of Hamdan's record of drug dealing, "only after a great deal of discussion in Washington about this issue, was permission granted."[15]

Within CTC, Dewey relied on Howard, as chief of CTC's Special Operations Group (CTC/SOG), and Bruce, a branch chief, to develop and oversee the initial planning. Two CTC staff officers (the coauthors) became part of the extraction team: Adam, as team leader and Vikki as his deputy. Adam brought operational, intelligence, maritime and paramilitary skills to bear while Vikki had recent training in CTC operations and experience as an imagery analyst. Three other officers rounded out the team: Ed, a former Navy Seal, brought small-boat and navigation expertise; Denise had security and intelligence analysis experience; and Chris was a former police sniper.

In advance of the team's deployment to Cyprus, Howard met with Adam and Vikki to outline his and Dewey's expectations. At one point in the meeting, Howard referred to Vikki as a girl; she replied, "Call me what you want, but I'm not a girl." Shortly thereafter, while acknowledging "Vikki's" professionalism, Howard expressed regret to Adam for sending him out with a "feminist."

… and in the Field

With Yunis in Beirut and Hamdan in Cyprus, Beirut was ruled out for the extraction operation, in large part, because of the presence there of kidnapped US and other citizens being held for ransom by Hizbollah-associated groups. Plans instead focused on Cyprus. With Dewey at the helm in Washington, the senior on-site officer took the lead for the operational plans and decisions in the field.

With Cyprus confirmed as the jumping off point for the operation, extraction team members traveled separately to Nicosia as

individual tourists. Once on the island, team members toured cities along the country's southern coast evaluating them for their potential utility in the operation. "Beach duty," according to Vikki. Locales scouted included Ayia Napa, Coral Bay, Larnaca, Limassol, and Paphos.

After visiting various places, Vikki and Adam met with CIA's senior officer on Cyprus to recommend Limassol. It was the second largest urban area (after Nicosia), the most populated municipality in Cyprus, had a main seaport, and its many small coves operationally enhanced concealment of the true nature of the mission.[16] The senior officer concurred and forwarded the team's recommendation to CIA Headquarters. Limassol was selected.

Meeting with Hamdan, the senior officer instructed him to maintain contact with Yunis. The officer also worked with Hamdan's brother, Ahmad (a pseudonym), as he was known to and trusted by Yunis. As Clarridge noted, "We used Ahmad as a middleman in dealings with Yunis in Beirut and eventually he was brought to Cyprus to assist in the operation."[17] On instructions, Hamdan invited Yunis to visit him in Cyprus on at least three occasions. During one visit, Yunis bragged about the Jordanian hijacking and his involvement in guarding TWA-847 hostages, a boast that was recorded and passed to the FBI and DOJ, which had appealed for acquisition of solid evidence against Yunis.

According to Hamdan, Yunis was married with two young sons, was unemployed, and was in dire need of money.[18] Given Yunis' financial straits, Hamdan was provided with cash to throw around, telling Yunis he knew people in the drug trade and might be able to arrange an introduction with "Joseph," a big-time drug dealer (a fictional character created for the sting).[19] In one instance, having flashed a roll of money, Hamdan assured Yunis he could be rolling in cash if he was willing to work for Joseph.

Describing Joseph as extremely private, cautious, and guarded, Hamdan explained to Yunis that Joseph conducted his business from a luxury yacht, which his crew operated in international waters. Yunis expressed interest; he returned to Beirut to await a signal from Hamdan to return to Cyprus for the meeting with Joseph on his yacht just outside Cypriot territorial waters, where, instead of meeting Joseph, Yunis would encounter FBI special agents ready to take him into custody.[20]

It sounded simple, yet operations rarely are simple. How best to get a willing, unsuspecting Yunis to a yacht stationed at least 12 miles off shore had to be addressed. The team determined that the sole option was rental of small boats on Cyprus. In researching the prospects, the extraction team determined the majority of boat rentals came from local vendors who rented on an hourly basis and that the conditions of the boats were questionable at best.

Additional hurdles included: local boats lacked basic instrumentation, and their fuel capacity was extremely limited, as tourists tended to rent boats for a one or two hour excursion, usually remaining within sight of shore. Another complication: neither Yunis nor Hamdan could swim, and neither had been in a small boat or knew how to navigate.

With Limassol selected as the departure site, acting as cost-conscious tourists, extraction team members set about renting small motorboats. Rentals would be for one to two hours at a time, two or three times a day, from different vendors over several weeks. As team members arrived at the various rental locations wearing shorts and bathing suits and carrying picnic supplies, the rental site owners began to extend the time and distance in which their small boats could be rented. The owners probably assumed team members were seeking private, secluded locations for parties.

Initially there was concern that the rental business owners would become suspicious of the team's repeated patronage. It became apparent, however, that team members were actually a lucrative source

of income, and the owners did not have a problem with repeat rentals. As a side note, because rental boats tended to be well used and sometimes in poor shape, a propeller and compass were purchased locally, mounted each day when out of sight of the rental shack, and removed before returning a boat.

Extraction Planning

As the extraction team continued renting small boats in the Limassol area, Adam returned to Washington. In meetings, he recommended that, to be successful, the CIA portion of the operation would require the rental locally of three boats on the day of the extraction; each had to be capable of making the round trip to a point 12-plus miles offshore and back without raising concerns or undue attention. A fourth vessel, acquired earlier, was to be the putative Joseph's luxury yacht on which FBI special agents would, in international waters, await the arrival of Yunis and Hamdan.

No member of the extraction team could be present at the arrest, so Ahmad, who had no experience in boating, would need to be trained to pilot one of the small boats. Tentatively, the plan was for Ahmad and Hamdan to bring Yunis out to the yacht where he was to meet Joseph.[21] Adam and the team proposed the following plan to officials in Washington:

> *The boats would, in effect, form a picket line from Limassol to the yacht. (See schematic.) First, was to be a 26-foot fishing boat to be crewed by Adam, Vikki, and Chris. Following at a good distance (and well out of sight) was a small boat, piloted by Ed and Denise. Ahmad, in the last boat, with Yunis and Hamdan, would follow until Ahmad saw the yacht. Planners in Washington approved the proposal.*

A joint CIA-FBI team met in the Mediterranean, and took charge of an 81-foot luxury yacht. They sailed to rendezvous with the USS Butte, a US Navy ammunition ship to which the captured Yunis would be taken. On reaching the Butte, the CIA officers went aboard, leaving the yacht in control of FBI special agents.[22]

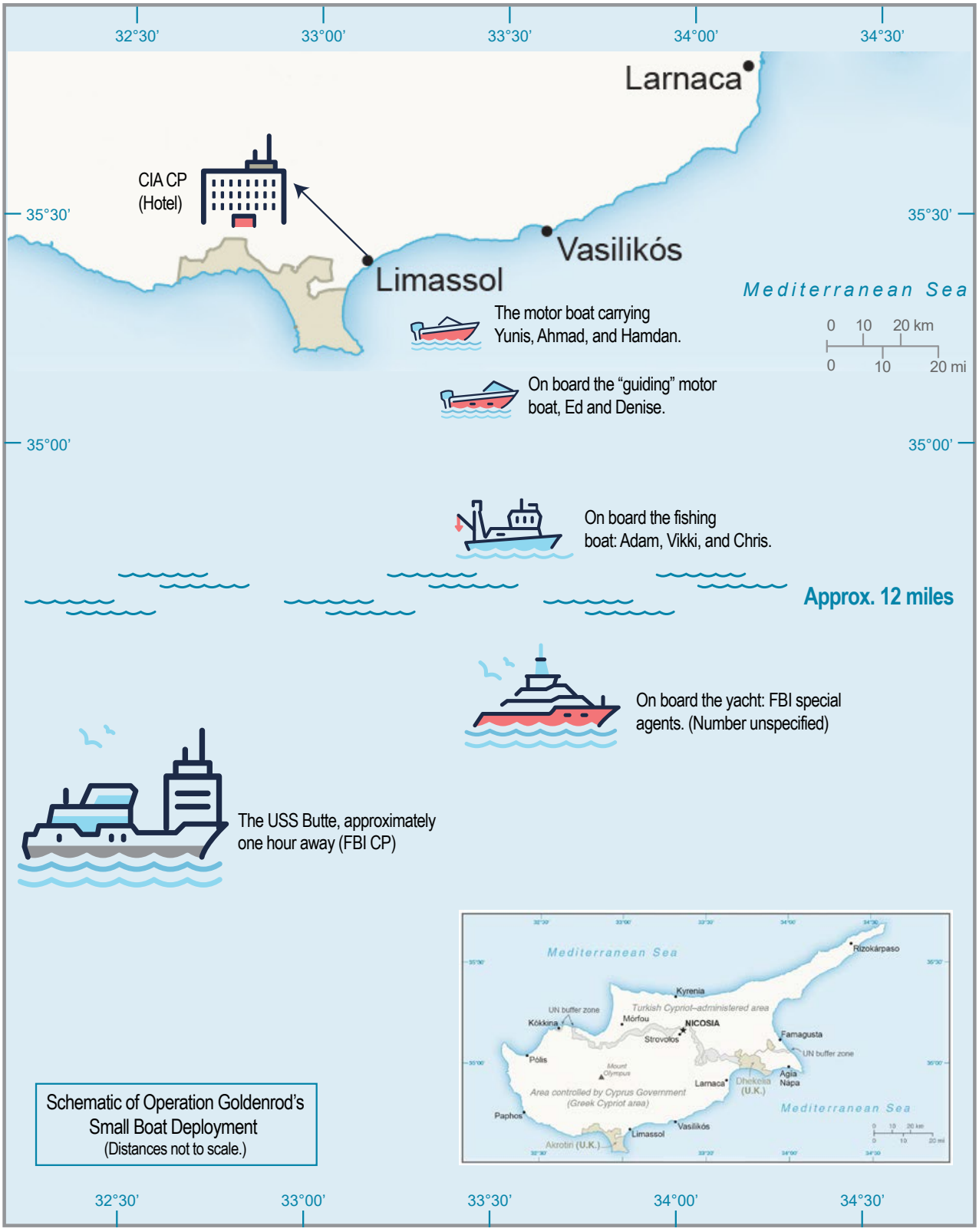
Ahmad's training was complicated by his lack of cover documents, which caused team members to decide he should not rent the boat he would operate. Moreover, the team worried that Ahmad could draw undue attention from Cypriot authorities if he was seen with a team member on a beach or while renting a boat. To work around these problems, the team rented a boat, then they met Ahmad at a location away from populated beaches.

The team knew Ahmad would need to learn how to navigate to a specific point under unknown weather conditions to locate and link up with Joseph's yacht (a yacht no team member had seen). All of Ahmad's training had to occur well beyond the shoreline. Ahmad proved to be a quick learner and, within weeks, had become familiar with basic navigation, docking, and trouble-shooting. Only on the morning of the operation did team members learn that Ahmad was exceptionally nervous because he, too, did not know how to swim.

As Ahmad's training continued, decisionmakers in Washington, DC, including Director of Operations Clair George and Clarridge, met and decided on September 13, 1987 as D-Day.

The Name of "Joseph's Yacht"

In his memoir, Clarridge asserted that the yacht's name was *Skunk Kilo*, "a name that seemed to suit a drug baron." Rather, the name was a matter of happenstance according to a senior CTC officer aboard the USS *Butte* explained to Adam that the US Navy maintained continual radar watch around it to identify and track vessels that could pose a hazard to navigation or a threat to the *Butte*. Until positively identified, tracked vessels would be listed as a "Skunk" and given an alphabetic designation in the order of their appearance on the radar screen. "Joseph's" yacht happened to be the 11th vessel tracked that day and thus was named *Skunk Kilo*. An observer on the *Butte* thought this was the actual name of the yacht and, since then, the yacht on which the FBI arrested Yunis has been refer red to as the *Skunk Kilo*.



Schematic of Operation Goldenrod's Small Boat Deployment
(Distances not to scale.)

Dewey further recalled: "On the way back to Headquarters following yet another interagency meeting, Clair turned to me and said, 'I think you better go and out run this one.'"[23] The FBI's "Buck" Revell supervised from aboard the Butte. In his memoir, Revell noted that, on September 7, while en route to National Airport, he received a call from Attorney General Edwin Meese. Revell recounted, "Meese told me that the President was enthusiastic about Operation Goldenrod and it was definitely a go."[24]

Dewey arrived in Limassol wearing a white safari suit, its pocket embroidered, as was his custom, with initials. He was accompanied by Howard and a communication specialist. Like the extraction team, they traveled as tourists. All three registered in the Sheraton Limassol, a luxury waterfront hotel that had recently opened, with some areas still under construction.[25] Dewey and the communications specialist were ensconced on the top floor in the hotel's largest suite. The suite filled with people and equipment including satellite communication (SATCOM) gear, whose antenna was directed—unobtrusively the team hoped—toward the living room window. Dewey recalled:

> *We had enciphered SATCOM links to CIA Headquarters in northern Virginia which, in turn, had a relay to the White House, FBI, and State Department. The US Military Command in Stuttgart, Germany, insisted on monitoring our communications because of its responsibility for the* USS Butte*, and, of course, we established communications with the Bureau's command center on the USS Butte, which had communications with the* Skunk Kilo*. We also had less powerful handheld radios for communications among the suite, small guide (picket) boat and the lead boat (fishing boat).*[26]

The hotel offered unique advantages and disadvantages. Typically, tourists to Cyprus arrive with a suitcase, camera, and sunscreen, not large aluminum boxes of telecommunications equipment (this was years before laptops and cell phones.) Being newly opened, the hotel had few guests and furnishings, and bulky objects were still being delivered to it, allowing Dewey to explain away the aluminum boxes as containers for photographic equipment.

One disadvantage was that the manager was so delighted to have a big spender from the United States renting his suite, that he kept sending gifts to the room. Each time a hotel employee came bearing food, drink, or flowers from the manager, people and gear had to be moved out of sight of the doorway. With the team meeting to review plans in Dewey's suite, Vikki solved the problem by donning one of the suite's bathrobes, strategically draping her clothes over furniture in such a way as to be obvious from the doorway, put a towel over her head as if just washed, and answered the door.

Vikki then left the suite for a short time to meet Ed, Denise, and Chris outside of the hotel to update them on the discussions with Dewey and group. On returning, she was instructed to put on a robe because she had been meeting the team members, another delivery was made and this time Dewey had to don a robe. Probably realizing he was interrupting a private party, the manager stopped sending gifts![27]

In contrast to Dewey's group, the team members continued to act as frugal tourists, moving several times from one small hotel to another. They dressed in beach garb and got around the island on motorcycles or jeeps. No luxury beachfront hotels for the extraction team**.**

Final Stages

Days before the operation was to commence, Dewey learned from the senior officer on Cyprus that Yunis had reached the island, but, because Cypriot authorities had him on a watch list, they were searching for him in hotels and other locations. The officer, then questioned whether it was prudent to go forward. It would be bad luck if Yunis were to be picked up

by the authorities; yet worse was the possibility the extraction team could be compromised. Traveling in Cyprus with no diplomatic immunity, the extraction team could find itself in an uncomfortable Cypriot jail if apprehended.

During a somber and tense meeting at an outdoor restaurant, Adam reported that Ahmad had become proficient enough to follow the guide boat, manned by Ed and Denise, to within sight of the yacht. Vikki assured Dewey the rental of the fishing boat had been secured and team members were ready. "Everything and everyone was in position."[28]

Later that day, Adam and Vikki rented a small boat and picked up Howard at the hotel's dock. While out on a general area familiarization for Howard and to discuss any issues he or Dewey might have away from potential eavesdroppers, Howard asked Vikki why she had taken offense at being called a girl. She informed Howard she was too old to be called a girl and that she would never think to refer to him or Adam as a boy. Howard chuckled, said he respected the answer, and would never call her a girl again. And he never did.

Dewey instructed the senior officer that Hamdan, Yunis, and Ahmad should move from the apartment where they were staying. Thus, on Friday, September 11, two days before the operation was to commence, the three of them checked into the same hotel in Limassol in which Dewey and his group were staying. "It was risky to have him check into a hotel, where his passport would be recorded," but by making the move at the start of a weekend, it was hoped no one would check passports in a high-priced tourist hotel until Monday—after Yunis had been arrested and was en route to the United States.[29]

On Saturday, Adam and Vikki were called to a meeting in Dewey's suite. Initially declining, citing security reasons, they were overruled. Hopping on a motorcycle, dressed in days-old beach wear, they entered the hotel. With Dewey taking the lead, the senior officer on Cyprus, Howard, Adam, Vikki, and the communication specialist focused on a final review of plans and a last chance to express concerns. There were none. Before leaving, Dewey wished Adam and Vikki good luck for the next day's operation. Vikki surprised all present by responding, "We don't need luck. This is going to work."

Howard accompanied Vikki and Adam downstairs and, while standing in the lobby, Yunis, Hamdan and Ahmad entered through the hotel's revolving door. Vikki pointed the three out to Howard and Adam, specifically identifying Yunis. Adam asked, "How do you know?" Vikki replied, "His photo has been on my desk for over a year." As the three CTC officers left the hotel through the same revolving door, they looked back into the lobby and saw Yunis and friends watching them!

Adam and Vikki then met with Ed, Denise, and Chris. Adam told the team that, based on his 25 or so years of experience, tomorrow's D-Day would be an opportunity the likes of which might never appear in most careers. Like a championship game, it would have a definite beginning and end, and there would be no do-overs. It would be our Super Bowl and, if we did not succeed, we would always look back and think of what we might have done differently. That evening, still acting their parts as tourists—at the same time, making an opportunity to check for surveillance—Adam and Vikki attended the Cyprus Wine Festival (and picked up shot glasses to prove it).

By September 12, the final stage of the operation brought encrypted communications to the forefront. The CIA command post in the Sheraton was led by Dewey and the senior officer in Cyprus. Revell's FBI command post, including a senior CTC officer, was in place on the *Butte*. FBI special agents were aboard the yacht, awaiting Yunis and Hamdan's arrival the next day, after which the yacht would sail to rendezvous with the *Butte* at a preaaranged location, about an hour's sail away.[30]

Meanwhile, DCI Webster was on an official visit to Israel. An encrypted satellite network allowed

Webster and the FBI's command post to establish direct contact with Dewey and enabled direct encrypted communications with Langley and the White House.

If all went as planned, it would be smooth sailing. What could go wrong? Well, there had been no opportunity for a dress rehearsal, much less to train together with FBI counterparts already on the yacht. Team members had trained Ahmad to pilot a small boat and conduct basic navigation, yet security concerns prevented Ahmad from practicing to dock his boat at the hotel's pier, much less with a yacht. Except for pre-paying the day before to rent the fishing boat, there was no way to know which small boats Ed or Denise could rent until the morning of the operation.

A further complication arose after someone in Washington determined the fishing boat, guide boat, yacht, and CIA command post did not need radio communications with each other. Fortunately, this changed after a last-minute meeting in Washington. Adam was given a pair of encrypted handheld radios—one for the fishing boat and one for the guide boat—that could link up with the yacht and the hotel's command center. These radios would prove critical.

September 13: Showtime!

D-Day for Operation Goldenrod arrived and brought with it less than ideal conditions, including heavy haze, mist, and overcast skies. Before sunrise, Adam, Vikki, and Chris arrived dockside to board the boat they had reserved and paid for the previous day. Wearing bathing suits covered by light shirts and carrying fishing gear as they boarded, they found an occupant asleep inside. They woke him by noisily bring their gear on board.

The three also brought on detailed navigation charts, the encrypted radio they had just received, binoculars and a rudimentary, locally purchased handheld radio-direction–finder.

Later that morning, Ed, the former Navy SEAL, rented a small speedboat and then picked up Ahmad at a prearranged spot on the shore, well beyond sight of the rental shack. They changed the propeller, brought onboard a portable gas tank, then piloted the boat within sight of the hotel. Ed jumped overboard and swam to the hotel, where he met Denise. Ahmad docked the boat at the hotel to wait for Yunis and Hamdan. Denise and Ed drove to a different rental shack and got the small boat they would use to guide Ahmad to the luxury yacht and piloted it to a location about five miles off shore, where it would be in line with the yacht's expected position.

At the hotel, Howard was seated in a chair near the boats, assuming the look of a proper tourist. As Yunis and Hamdan made their way to meet Ahmad at the pier, Howard positively identified Yunis and signaled the CIA command center, which in turn sent a message to all participants via SATCOM that the extraction was under way. The message, Dewey noted, "also asked CIA Headquarters to activate the complex plan to move Hamdan's extended family out of the Middle East to the United States. Tickets, funds, and necessary visas had been positioned for this moment."[31]

Twelve miles off shore is a long way for a small boat—well beyond sight of land—where even a luxury yacht looks tiny, if visible at all, from that distance on open water.[32] Moreover, the morning fog lingered. Dewey recalled the challenges in his memoir in this way:

> *Right away things started going awry. We had major problems with both navigation and communications. The picket* [fishing] *boat reported that it had been unable to find the* Skunk Kilo, *which had drifted off its designated longitude and latitude. Finally, sporadic communication was established between the yacht and the picket boat, and eventually the picket boat established a visual on the yacht.*
>
> *Meanwhile, the speedboat with Yunis was roaring out to sea,*

The authors reconnoitered the island using small rental boats. This photograph of the authors on a rented fishing boat was taken shortly after Yunis had been arrested. (Authors' collection)

following the lead boat with the couple aboard. Because the Skunk Kilo *was out of position, the picket boat was out of position. Thus the longitude and latitude that the lead boat was headed for to make the rendezvous was incorrect. Moreover, the picket boat, the lead boat, and the suite were experiencing intermittent communication blackouts with the handheld radios. The lead boat could not maintain communications with the picket boat long enough to get a fix on what its new course had to be to reach the yacht. Coupled with the extremely hazy conditions, which made visual navigation difficult, we had the makings of a major disaster.* [33]

To his credit, when plans were not going as designed, Dewey did not panic. While many of the participants asked for updates or progress reports, Dewey let the extraction team figure things out. Those on the fishing boat thought the lack of communication with the hotel/command post signaled Dewey's confidence in the team. It was not until his memoir was published in 1997 that team members would learn how often those in the command post had continually, yet unsuccessfully, attempted to communicate with the team. Howard later mentioned to Adam that, when communications were unsuccessful in reaching the fishing boat or guide boat, Dewey told those in their command post that "we will catch that guy if we had to go all the way to Beirut to do it, and we don't need advice from those not on the scene."

The wake of a passing Russian freighter that Adam presumed was en route to Limassol, gave Adam a data point that allowed him to reorient the team members. Having received no information, not even a photo, with which to identify the

Skunk Kilo, identification of the yacht was established using the hand-held radios. After spotting the yacht, one of several in the vicinity, Adam radioed to ask someone on the yacht to raise its sails. Up went the sails. Then he asked to have the sails lowered. Down they went. Identity confirmed**.**

Meanwhile, on the guide boat, Ed and Denise knew something was wrong—they were too far out to sea and had surely overshot the *Skunk Kilo* and the fishing boat. Ed took the initiative to turn back, with Ahmad following at a considerable distance.[34] On that boat, Yunis was getting nervous about being at sea for so long, with no sight of the yacht. After turning back, Ed reestablished radio contact with Adam on the fishing boat.

Adam asked Ed if they had seen the Russian freighter. Indeed, they had. With the additional data point on the freighter's location, Adam was able to calibrate a new course to the yacht for the guide boat leading Ahmad. Thanks to some crude radio direction-finding using a wire coat hanger and ingenious piloting by Ed and Denise, Ahmad delivered Yunis and Hamdan to the yacht.

Upon arrival, they were welcomed, according to Dewey, by two bikini-clad women, frisked, and then "slammed" to the deck and formally arrested by FBI men. (CIA had recommended the FBI agents treat Hamdan and Yunis with equal severity so as to maintain Hamdan's cover.[35])

Aftermath

Initially, the Operations Center in the hotel was to be dismantled as Dewey's group checked out. Extraction team members would separate and catch various flights out of Cyprus and eventually reconnect in Washington, DC. Dewey had another plan, as he instructed the extraction team, via radio, to meet in the hotel parking lot before leaving Cyprus. "For security reasons, we could have only the briefest celebration, a handshake with the participants who had been operating outside of the hotel suite."[36] As Dewey handed out cigars to the men in the team, Vikki asked if she and Denise were to get cigars as well. Dewey replied "These are expensive ones. Are you really going to smoke it?" The ladies got their cigars.

At the airport, team members pretended not to know each other as they awaited flights to various European locations. As Murphy's Law would have it, Adam and Vikki ended up on the same flight (different rows) but could not relax until they were out of Cypriot airspace, a moment delayed by their aircraft's late departure. As a result, the two missed a connecting flight to the United States and ended up at an airport hotel in yet another European city. Because the earliest flight they could get to the United States did not leave until the next afternoon, Vikki shopped in the morning, while Adam enjoyed a true European breakfast.

Meanwhile, back in the Mediterranean Sea, after Yunis's capture, Revell had sped to the yacht on a launch from the *Butte*. Revell recounted, "I could see Yunis sitting on the deck handcuffed.... Once aboard, I could see it was him."[37] Yunis, Hamdan, Revell, and some of the FBI special agents boarded the launch for transfer to the *Butte*. Four days later, Yunis was transferred to the USS *Saratoga* aircraft carrier.[38] From the *Saratoga,* Yunis, an FBI special agent, and a physician were flown aboard a Navy aircraft to the United States. The 13-hour flight required two mid-air refuelings.[39]

Operation Goldenrod, although not its operational name, made the television evening news on three Washington, DC, channels shortly thereafter. The *Washington Post* published an article on September 18, 1987, entitled "FBI Dupes Terror Suspect, Brings Him to US for Trial."[40]

Days after Yunis's arrival in the United States, Vice President George H.W. Bush invited CIA and FBI participants to the vice president's home at the Naval Observatory for an after-action report and to thank those involved. "The only photograph that exists of the event shows just the backs of the heads of the participants, for

security reasons."[41] It was memorable when Barbara Bush came out to the porch, welcomed the arrivals (including Dewey by name), then took off jogging. After the meeting ended, Mrs. Bush rejoined the group and asked Adam, "How do you want your eggs cooked?"

Yunis was tried in federal court, found guilty in October 1989, and sentenced to 30 years in prison. He was released on February 18, 2005, after serving 16 years, and deported to Lebanon.[42]

Results

The arrest and prosecution of a foreign national terrorist was a priority for President Reagan and his administration. In announcing Yunis's arrest, then-Attorney General Edwin Meese called the arrest a unilateral action by the United States" and "an important step in our policy of bringing terrorists to justice."[43] Operation Goldenrod's success set a precedent for future operations against terrorists. It marked the first time the United States went outside its territory to arrest a known terrorist abroad, and it demonstrated the United States could undertake proactive, credible operations against terrorists overseas. Operation Goldenrod proved to terrorists and other nations that the United States could go it alone in devising and carrying out unilateral capture operations with no other nation's involvement. Writer Steven Emerson observed in a May 1989 *Penthouse* article on the operation's significance:

> *It is a story whose lessons have reverberated throughout the world, as terrorists have been put on notice that they are safe nowhere, that the long arm of the American law can and will reach them no matter where they are. As a result, U.S. intelligence officials say that several known international terrorists are now afraid to travel freely overseas and are keeping a lower profile. Equally important, the success of the operation demonstrated that the U.S. can mount an aggressive attack against terrorists, and that if no other country can be depended on to help the U.S., then American agents will go it alone.*[44]

Within the IC, Operation Goldenrod displayed unprecedented inter-agency collaboration. It demonstrated US intelligence, federal law enforcement, and defense entities under White House and National Security Council guidance could work jointly to confront foreign-based terrorism. While this article focuses on CIA's role in Operation Goldenrod, its ultimate success involved DoJ/DEA; DoJ/FBI, DoD/Navy; DoD/NSA (oversaw communication interactions), State Department, the Justice Department (in prosecuting Yunis in US Federal court) NSC and, ultimately, the White House for its approval to undertake the operation.

LESSONS LEARNED

Every plan has its snags; this operation was no exception. A few observations are offered as possible aids in planning future, unilateral (maritime) extractions.

Personnel

The extraction team had time to plan and rehearse its role in the operation. Team members were provided appropriate mission tasking and clear guidelines while, at the same time, they were encouraged to apply their own expertise to solve problems as they developed. Lines of responsibility among the team members were clearly delineated.

Operational Planning

The fast-breaking, sometimes changing, requirements; participation of several CIA components (CTC, maritime, communications); and, involvement of other federal government entities precluded working-level advance coordination for those actually participating in the rendezvous. The extraction team had no opportunity to plan and rehearse the most critical phase of the operation —to locate the yacht and deliver the terrorist to the FBI in international waters. Extraction team members had no opportunity to see the yacht before the operation, which would have

A patch commemorating the capture and delivery to justice of Fawaz Yunis. An image of the patch appears on the US Naval Institute's Instagram site with a brief account of the distance record-setting flight of a Navy S-3 Viking from the USS *Saratoga* to the United States.

assisted in its identification on the day of the operation.

Given that FBI personnel alone were required to make the arrest of Yunis, there nevertheless was no planning or rehearsals with the FBI yacht crew before the onset of the operation. It would also have been helpful to have available appropriate intelligence resources at CTC. Overhead photography of the beach areas, for example, would have allowed the extraction team to accurately plot locations of launch points.

On-Site Preparations

The necessity of training and rehearsals cannot be overstated. Each time extraction team members rented a small boat and trained away from the shore, new aspects were identified that could be applied in the final planning phase.

Team members planned and practiced to meet a number of contingencies that could arise during the locate-and-deliver phase of the operation as well as training Ahmad who piloted Yunis and Hamdan to the yacht.

On-site, planning was modified and refined several times to reflect changes of policy or refinement to the ground rules resulting from inter-agency discussions in Washington, DC. Because the mission required precise timing and coordination, various elements had to be locked in for early mobilization, thus denying last minute modifications of the scenario or equipment.

Communications

Extraction team members should have been involved in evaluating and selecting communication equipment because of the distance to be traveled from shoreline into international waters. Instead, they were given digital voice, privacy handheld radios just days before the operation.

Navigation

With the operation under way, CIA extraction team members realized that FBI agents on the yacht had only a hand-held radio with limited range with which to establish contact with CIA officers on the fishing and guide boats. A secure communication package could have facilitated contact between the yacht and the two boats. This is less an issue in today's world, given the availability of satellite links.

The boats used by the extraction team had no instruments beyond marine compasses, purchased locally. A hand-held radio-direction–finder (medium wave and beacon bands) could have helped team members fix positions between the fishing boat and guide boat relative to the coast by keying on the major beacons in the area while the operation was under way.

Additional Sources

The majority of public information on Operation Goldenrod focuses on the role of the FBI; little other than a chapter in Clarridge's memoir, *A Spy for All Seasons* (1997), has addressed the actions undertaken by CIA and CTC officers. Almost a year to the date after Operation Goldenrod, a *U.S. News & World Report* cover story—also written by Steven Emerson—entitled "The Capture of a Terrorist," discussed FBI and Navy participation. Emerson's May 1989 *Penthouse* magazine article, entitled "Operation Goldenrod,"provided similar information. Two years later, in April 1991, Emerson, writing for the *New York Times*, described the capture of Mohammed Rashid, mentioned early in this article.

The senior FBI special agent on the scene, Oliver "Buck" Revell, focused on Operation Goldenrod in his memoir, *A G-Man's Journal* (Chapter 15, "An Overseas Success and Trouble at Home").[45] Goldenrod was a feature story on the History Channel as well as the television series *F.B.I. Files* (season 6, episode 18) on the Discovery Channel—Clarridge offered his insights in that 50-minute film. Finally, the FBI's public website features Operation Goldenrod in its "Famous Cases and Criminals" section of its history. ■

Endnotes

1. U.S. Department of State, *Patterns of Global Terrorism: 1985* (October 1986), 11–20 and 33–40.
2. Duane Clarridge, *A Spy for All Seasons* (Scribner paperback edition, 2002; first published in 1997), 350. The chapter in Clarridge's memoir dealing with the operation, "Chapter 11: Bring 'Em Back Alive—or Not," runs from page 347 to 360; Exclusive Report, "The Capture of a Terrorist," and Steven Emerson with Richard Rothschild, "Taking on Terrorists," both in *U.S. News and World Report:* September 12, 1988.
3. PUBLIC LAW 99-399—99th Congress—AUG. 27, 1986, "CHAPTER 113A—EXTRATERRITORIAL JURISDICTION OVER TERRORIST ACTS ABROAD AGAINST UNITED STATES NATIONALS
4. https://www.fbi.gov/history/famous-cases/fawaz-younis; Wikipedia.org/wiki/Fawaz_Yunis.
5. U.S. Department of State, *Patterns of Global Terrorism: 1986* (October 1987), inside cover.
6. Mohammed Rashid's capture was discussed in detail in the *New York Times*: Steven Emerson, "Capture of a Terrorist": 21 April 1991.
7. Clarridge, 350–51.
8. Ibid., 351
9. Ibid., 351 and 347–60.
10. Director Casey suffered two seizures in December 1986 and never returned to his office. He died on May 6, 1987; William Webster, who had been serving as director of FBI (1978–May 25, 1987) was sworn in on May 26, 1987.
11. Oliver Revell and Dwight Williams, *A G-Man's Journal* (Atria, 1998), 266 and Claridge, 324.
12. Clarridge, 351.
13. Ibid.
14. Ibid.
15. Ibid., 351–52.
16. Wikipedia, Wikipedia.org/wiki/Limassol; U.S. News and World Report, 29; Clarridge, 350.
17. Clarridge, 353.
18. Ibid., 350.
19. Revel and Williams, 265–70; Clarridge, 352–53.
20. Revell and Williams, 269; Clarridge, 354.
21. Revel and Williams, 267; Clarridge, 353.
22. Clarridge, 353.
23. Ibid., 352.
24. Revell and Williams, 269.
25. Clarridge, 355
26. Ibid, 355–56.
27. Ibid., 356.
28. Ibid., 355.
29. Ibid.
30. Steven Emerson, "Operation Goldenrod," *Penthouse Magazine*, May 1989, 110.)
31. Clarridge, 356–57.
32. Ibid., 353.
33. Ibid., 357.
34. Ibid., 357–58.
35. Ibid., 358.
36. Ibid..
37. Revell and Williams, 272.
38. Revell and Williams, 272, and *U.S. News & World Report*, 34.
39. Revell and Williams, 275, and *U.S. News & World Report*, 34..
40. George Lardner, Jr. and Nancy Lewis, "FBI Dupes Terror Suspect, Brings Him to US for Trial," *Washington Post*, September 18, 1987.
41. Clarridge, 359, and Revell and Williams, 275–76.
42. Fawaz_Yunis: OPERATION GOLDENROD, at https://www.fbi.gov/history/famous-cases/fawaz-younis.
43. George Lardner, Jr. and Nancy Lewis, "FBI Dupes Terror Suspect, Brings Him to US for Trial," *Washington Post,* September 18, 1987.
44. Emerson, "Operation Goldenrod,"118.
45. Revell and Williams, 264–67.■

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 NGA. 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.

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;

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. ■

Grand Tetons, Wyoming (Wirestock)

AI and Expertise

Intelligent Delegation for Intelligence Analysts

William Martin
William Martin is the pen name of a counterintelligence analyst.

"How can you write or talk authoritatively about something if you haven't seen it?" David Love, American geologist (1913–2002)

Intelligence, at its most basic, is a delegation by decisionmakers of their senses and sense-making to an intelligence service in order to reduce uncertainty and deliver competitive advantage. It is the responsibility of intelligence officers to 1) collect information about (sense) the world and its dizzying array of potential partners and adversaries and 2) process that collection in ways that US policy, operational, and military customers do not have the capacity to do firsthand (sense-making). A US policymaker cannot personally be present for another country's foreign policy deliberations, a military planner cannot observe an enemy's missile systems firsthand, and law enforcement cannot be present with a terrorist group as they plot an attack. Instead, we deploy case officers to recruit sources who have access to foreign decisionmaking, we take satellite photos of missile placements, and we intercept the communications of attack plotters.

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.

As intelligence scholar Jennifer Sims has written, "Competitors choose to [delegate] because they want to gain better information on adversaries than their own faculties can provide, or than adversaries have on them. Most decisionmakers feel smart enough; they just abhor relative uncertainty."[1]

Intelligence analysis focuses on the sense-making part of this equation: turning collection into a coherent picture that ideally increases a decisionmaker's understanding, resolves decision dilemmas, and provides an edge over their adversaries. Good analysis requires working knowledge of the available sources of information, as well as expertise in the target itself, which helps sort fact from fiction, detect change, and spot opportunities for US decisionmakers. One of the surest ways to build true expertise in a subject matter is by removing as many layers between the analyst and the subject as possible.

The Intelligence Community tries to cultivate world-class expertise, often by providing opportunities to "sense" targets firsthand through experience overseas, academic learning, or language study. These investments remove the layers between analysts and their subject matters, and sometimes they help bypass the gates erected to keep information hidden by engaging directly with foreign counterparts. With deeper expertise, we can see more clearly through the dark glass of intelligence reporting.

And the glass, indeed, is dark. In general, the information analysts sift and interpret day-to-day is filtered through multiple layers. Consider a report based on human intelligence, say a diplomatic or attache contact: it is the end result of information transmitted through a set of mediators. The report reflects a collection management officer's refinement of a case officer's reflection of a meeting with a source, where the source reported their reflections of something that happened, sometimes reporting secondhand the reflections of sub-sources, and so on and so on. The value of the intelligence report—how diagnostic it is of foreign plans and intentions, or how reliably it reflects the issue we care about—increases in direct proportion to how close it is to the target of collection. Information from a source who participated in the plotting of a terrorist attack is more reliable and has a greater potential to reveal new opportunities than that from a source that only heard about that plot second or third hand.

LLMs Add Layers

Technological developments since late 2022 have introduced a tantalizing new potential enabler for the sense-making side of intelligence that is the bread-and-butter of intelligence analysts: artificial intelligence (AI), usually meaning large language models (LLMs) like ChatGPT or Claude, provides the promise of offloading some of the labor associated with the processing of intelligence collection. These models give the impression of being able to summarize large amounts of text and provide passable human-like narratives that can be tailored to look like intelligence analysis.

Articles in recent editions of this journal have argued from the premise that LLMs will play a larger and larger role in intelligence analysis. Grunspan, et al., for example, imagine a new form of intelligence called "emergent intelligence," where human roles "shift from manual data collection and processing to overseeing AI systems, verifying their outputs, and incorporating findings into strategic decisions."[2] Alison Melton envisions the creation of an entirely new cadre of intelligence officers responsible for providing quality assurance for AI-enabled capabilities in the defense intelligence enterprise, aimed at ensuring the reliability of the output, and accountability if something goes wrong.[3]

The incorporation of these tools, however, risks removing analysts further from the targets we are trying to comprehend. One way to understand the use of LLMs in intelligence analysis is a further delegation of sense-making. We could feed a large number of clandestine reports, signals intelligence publications, or press information into an LLM, and use a chat bot as an intermediary to ask questions of that body of text. This would, in

theory, speed the time it takes to answer some intelligence questions.

In many cases, however, the introduction of an additional layer between ourselves and information about our targets distorts our understanding and cripples our expertise, because the farther we are from the thing we are supposed to be experts on, the less we will understand it. We already sense the world through a plethora of layers. So, if we introduce an LLM as yet another intermediary—or the primary intermediary as some imagine the future of the discipline—we should ask ourselves whether that obscures or clarifies what we are trying to understand.

Recent research suggests that the real-world incorporation of AI tools in knowledge work often decreases productivity: the additional labor involved in refining prompts and the extra time it takes to remove errors from AI-generated output distracts professionals from the core tasks they are trying to undertake.[4] Indeed, if a suite of AI-powered IC tools meant to process abstracted data sets requires the creation of another bureaucracy staffed with quality control experts who themselves specialize in AI tools to verify the outputs, as some suggest, we should wonder what the gain of employing an AI-powered tool is in the first place, and at what cost?

Potential Expertise Erosion

Even if LLMs are refined, hallucinations rates are reduced, and true productivity gains emerge in some fields, the potential erosion of analyst expertise over time is an underappreciated cost of adopting reliance on these models on a large scale. Further distancing human analysts from "manual data collection and processing" as Grunspan envisions reduces opportunities for analysts to interact directly with the information that underpins assessments, makes them less fluent in foundational data, and less practiced at applying their own critical thinking and frameworks to the information. A restructuring of the intelligence cycle along these lines could create a cadre of analysts who are no longer experts in any particular subject matter, but instead spend time becoming adept at writing prompts for AI agents.

Empirical research so far indicates that diminished creativity and the atrophy of critical thinking skills are both predictable results of wide-scale adoption of LLMs. One study found that when creative writers used AI systems to generate prompts for short stories, the authors were anchored to the ideas proposed by the LLM, a dynamic that resulted in a more homogeneous set of ideas.[5] A separate 2025 study showed that knowledge workers who relied on AI tools were less likely to employ critical thinking in their work.[6] While the hope is that AI can produce high quality analysis at speed, the early research suggests that the more intelligence analysts delegate the retrieval and processing of information about their targets, the less expertise they will have, and therefore the less qualified they will be to evaluate the output of any given LLM. The loss of expertise will result in greater and greater reliance on AI tools that further upscale the all-too-human foibles central to most intelligence failures: anchoring bias, homogeneous views, and a lack of critical thinking.

The geologist David Love, whose quote introduces this article, provides one model for the kind of expertise intelligence analysts should strive to develop over time. Love's doctoral thesis, which he completed after personally "crawling up and over [the] steep-walled ridges and broad, windswept plateaus" of Wyoming, would revolutionize the discipline's understanding of the entire Tertiary geologic period.[7] Love was legendary for completing two full geological surveys of the state of Wyoming, in 1955 and again in 1985, both of which set the standard for the discipline in terms of detail, accuracy, and breadth. He did so by manually reviewing the state's geology firsthand on foot and horseback. As one commentator put it: "Dave has looked at all the rock. It's all in one mind.… When the solid foundations aren't there, geologists are talking complete mush. Dave is making sure the foundation is there." Love's career was ending in

the 1980s as newly available satellite-imaging techniques allowed geologists to survey from the comfort of their offices, with very little field work required. Love said he did not blame younger geologists for applying these new techniques, because "the money is in the black box."[8] But he rightly recognized that the opportunity to build expertise through more direct experience was lost in the prioritization of remote sensing techniques. Relying on those techniques without field-based verification could lead to gross misinterpretation.

Intentional Delegation is Key

And yet, we live in a world of ever-increasing mountains of data that threaten to overload our ability to mentally process it in time for it to matter. We cannot look at all the rock. We never could. In such a world, is there a role for LLMs to add value in intelligence analysis? The answer, at least for now, lies in making very deliberate choices about what we want to delegate to an LLM. As a general rule, we should ask whether an LLM can help speed the process by which an analyst can more directly sense the target they are trying to understand. Under this criteria, the best current application of an LLM is in the processing of large sets of raw information, acquired through technical means. In such instances, there are initially fewer layers between the analyst and the underlying information, but it's not clear at the outset what information might help fill critical intelligence gaps. An LLM can quickly summarize documents, emails, or other human-generated text, and often help flag what might be relevant for an analyst faster than manual human review.

In this sense, an LLM can be used to eliminate layers between an analyst and important information about a target, ideally, speeding the process of filling intelligence gaps or uncovering new opportunities. However, such a delegation should only be the first step in an analyst's work generating new knowledge about a target: whatever an LLM might point an analyst to in a large dataset must still be reviewed by that analyst himself. An LLM should always be able to tie the summary to the original data. And, of course, the LLM cannot determine which target might hold the important secrets, or whether reliable answers can be found in the datasets that are currently available. Simply using an LLM to interact with the data adds an additional layer between the analyst and the target, decreasing the reliability of the information, and increasing the chances it will distort the sense-making so essential to good intelligence.

Working with a liaison service is a fitting analogy to using an LLM: an analytic exchange with a partner service, especially if our interests are generally aligned, can be enlightening: it can expand our knowledge, help fill our own intelligence gaps, or point us to new places to direct collection. However, the best exchanges with liaison require detailed discussions of the information that underlies that service's assessments, and (where trust is high) a discussion of what sources are providing that information and their reliability. But, as a general rule, relying on a liaison service without additional evaluation of the underlying information builds in the additional risk of manipulation, even if the intelligence gain seems to save us time and resources in the short term.

As Sims notes, liaison "which involves borrowing intelligence systems (platforms, sensors, processing, and exploitation), can dazzle the parties with cheap riches that mask their separate agendas and the benefits each party gains from the risks it is incurring."[9] Risks aside, if working with a liaison service helps bring us closer to the issue we are interested in understanding, the juice is worth the squeeze. The same should apply to the use of LLMs.

In 2019, Joseph Gartin posited in these pages that we face an inflection point in intelligence analysis,[10] but that shift may be more akin to that of geology in the 1980s than the Industrial Revolution or the invention of writing. Geologists, it turns out, never fully shifted to remote-sensing techniques. The new tools were useful, but still had to be employed

judiciously and combined with firsthand fieldwork to produce accurate assessments. Twenty years later, experienced geologists were writing about the potential compounding errors that over-reliance on remote-sensing techniques could produce.[11] Similarly, AI seems hot right now; it's certainly where the money is at. But it may be a mistake to follow that money and assume that the tools will revolutionize the core craft of intelligence analysis. A critical approach is necessary: we should recognize that the interests of the IC do not always overlap with those of AI companies. There are intense commercial incentives driving many of the claims about what AI can do, or will be able to do in the future. Private industry has invested trillions of dollars in the data centers and other infrastructure required to make AI widely available and ubiquitous in everyday life. That investment is, in effect, a bet that demand for the promised services will materialize, and such an extraordinary bet requires extraordinary claims to justify itself.[12] But it is our responsibility to determine for ourselves whether those tools bring us closer to—or push us farther from—the world we seek to understand. ■

Endnotes

1. Sims, Jennifer, Decision Advantage: Intelligence in International Politics from the Spanish Armada to Cyberwar (Oxford University Press, 2022), 17.
2. Rachel Grunspan, Jessica D. Smith, and Elizabeth VanderVeen, "Emergent Intelligence: Spycraft and Intelligence in the AI Era," *Studies in Intelligence* 69 No. 4 (December 2025).
3. Alison Melton, "Defense Intelligence Quality Assurance in the Age of AI," *Studies in Intelligence* 69 No. 4 (December 2025).
4. See Auste Siukte, Lev Tankelevitch, Viktor Kewenig, Ava Elizabeth Scott, Abigail Sellen, and Sean Rintel, "Ironies of Generative AI: Understanding and Mitigating Productivity Loss in Human-AI Interaction," *International Journal of Human-Computer Interaction*; October 15, 2024: https://doi.org/10.1080/1447318.2024.2405782 (accessed on February 22, 2026).
5. Anil R. Doshi and Oliver P. Hauser, "Generative AI enhances individual creativity but reduces the collective diversity of novel content," *Science Advances* 10, Issue 28, July 12, 2024; https://www.science.org/doi/10.1126/sciadv.adn5290 (accessed 21 February 2026).
6. Hao-Ping (Hank) Lee, Advait sarkar, Lev Tankelevitch, Ian Zachariah Drosos, Sean Rintel, Richard Banks, "The Impact of Generative AI on Critical Thinking: Self-Reported Reductions in Cognitive Effort and Confidence Effects From a Survey of Knowledge Workers," CHI Conference on Human Factors in Computing Systems, April 26, 2025; https://dl.acm.org/doi/10.1145/3706598.3713778 (accessed on February 21, 2026).
7. Susan Tweit, "For 60 years, J. David Love explored the West's geology," *High Country News*, November 1, 2002; https://www.hcn.org/wotr/for-60-years-j-david-love-explored-the-wests-geology/ (accessed February 22, 2026).
8. See John Mcphee, *Annals of the Former World* (Farrar, Strauss, and Giroux, 1981), 379–82.
9. Sims, 103.
10. Joseph W. Gartin, "The Future of Analysis," *Studies in Intelligence* 63, No. 2 (June 2019).
11. N. Horning and N. Dubroff, "Myths and misconceptions about remote sensing," American Museum of Natural History, Center for Biodiversity and Conservation, 2004; http://biodiversityinformatics.amnh.org/ (accessed on 21 February 2026).
12. A viral February 2026 blog post "Something Big Is Happening", from Matt Shumer, CEO of OthersideAI, is a good example of the kind of rhetoric that AI companies must employ to drive demand. Shumer predicts that AI will inevitably become "a general substitute for cognitive work" and he tells white collar workers that their only hope of surviving the coming revolution is to become early adopters and incorporate new AI models into their work: "Sign up for the paid version of Claude or ChatGPT. It's $20 a month." If it sounds like he is selling something, that's because he is. ■

Judgment Under Tempo

Tradecraft in a Digital Intelligence Environment

Justin K. Edmondson, PhD
The author is a senior analyst at the Farragut Technical Analysis Center, Office of Naval Intelligence.

Digital systems have transformed intelligence production, accelerating integration, synthesis, and presentation under operational tempo. Less visible is how this environment reshapes the formation of analytic judgment itself. Platforms that reward speed and legibility can gradually make deeper understanding and epistemic restraint harder to sustain. These pressures are structural rather than intentional, and they rarely manifest as immediate error. In this essay, I argue that modern tradecraft must account for the selection effects embedded in digital analytic environments. Making posture choice explicit strengthens professional discipline and reduces the risk of analytic failure before it emerges at scale.

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.

Intelligence in a Digital Habitat

Intelligence work now unfolds inside a dense digital ecosystem. Analytic platforms integrate sensor feeds across domains, automate portions of synthesis, and accelerate the path from collection to decision-maker. The enterprise is faster, more connected, and more capable than at any point in its history.

Less examined is how this environment shapes professional judgment. Digital systems do more than increase speed and coordination; they influence which analytic postures are rewarded, which forms of expertise remain visible, and which kinds of understanding become harder to sustain under tempo. These effects arise from structure rather than intent. Over time, they alter how judgment is formed.

This essay argues that contemporary intelligence practice must account for these environmental selection pressures as part of tradecraft itself. The goal is not to critique technology or propose reform, but to clarify the conditions under which professional judgment now operates. Making those conditions explicit strengthens discipline and reduces the risk that structural pressures are mistaken for personal or institutional failure.

From Tools to Environment

Intelligence professionals have always adapted to new tools. Signals intelligence, imagery analysis, and computational modeling each transformed the craft. The present moment differs in degree rather than kind, but the degree matters. Digital systems increasingly resemble an environment rather than an instrument. They create abundance, reduce friction, and accelerate coordination. Like any environment, they also apply selection pressures.

Those pressures are not imposed by intent or design. They arise from structure. Digital systems reward fluency across interfaces, responsiveness to cues, and the ability to integrate outputs quickly. Over time, these rewards shape practice. Certain postures thrive because they fit smoothly within the system's byproducts. This process is neither coercive nor adversarial. It is commensal, i.e., one element gains from another without causing harm or providing benefit. Recognizing this commensal nature is a prerequisite for disciplined professional judgment.

Abundance and Cost

One defining feature of the digital intelligence environment is that analytic production has become inexpensive. Collection, aggregation, synthesis, and presentation can be generated rapidly and at scale. This is a genuine operational advantage.

Other aspects of the work remain costly. Interpretation, validation, and judgment do not scale in the same way. In intelligence, correctness is rarely immediate or locally testable. Ground truth is delayed, incomplete, or never fully revealed. Errors propagate quietly. Plausible narratives can persist long after their assumptions have weakened.

This asymmetry is not new. What is new is the degree of abundance. As production accelerates, the effort required to understand and verify outputs becomes less visible by comparison. Institutions naturally emphasize what scales. This is adaptation as opposed to neglect. The challenge lies in recognizing how that adaptation reshapes professional posture.

Functional Postures in Intelligence Work

To describe these pressures more clearly, it is useful to name several functional postures that exist within intelligence work. These are not personality types, career tracks, or proxies for individuals. Every intelligence professional, team, and organization embodies all of them to varying degrees, often simultaneously.

These postures describe ways of working rather than kinds of

people. Their relative prominence shifts with context, tempo, and environment.

Orchestration: Integration Under Tempo

Orchestration is the posture most visibly amplified by digital systems. It involves integrating multiple streams of information, tasking collection assets, synthesizing outputs, and presenting coherent narratives under time pressure. Modern platforms are well suited to this work. They reward responsiveness, procedural fluency, and speed.

Orchestration is indispensable. In operational contexts where uncertainty is high and time is constrained, integration and decisiveness matter. Digital systems strengthen this posture for good reason. At the same time, orchestration necessarily rests on upstream assumptions. It inherits the limits of sensors, models, and abstractions that it cannot always interrogate in depth. This is not a deficiency of orchestration; it is inherent to the posture. Awareness of that dependency is part of professional discipline.

Building: Holding Internal Understanding

Building is the posture of internal comprehension. It is where the mechanics of collection systems, the assumptions embedded in models, and the limits of inference are understood and held. Builders recognize where abstractions simplify reality and where they distort it. They are often able to sense when a result feels plausible but fragile.

This posture is slower and less visible. Its outputs are harder to compress into briefings or metrics. Digital environments do not naturally foreground it, not because it lacks value, but because its value is difficult to surface. Yet without this posture, intelligence work becomes brittle. Understanding here is not procedural; it is conceptual. It anchors judgment.

Auditing and Governing: Discipline and Restraint

Auditing represents the posture of epistemic restraint. It includes red-teaming, second looks, boundary-setting, and the translation of past failures into present constraints. Auditors ask how conclusions were reached and under what conditions they might fail.

This posture introduces friction by design. It slows processes in order to preserve confidence in outcomes. Under pressure, that cost becomes more apparent. Strong intelligence organizations recognize this posture as ballast rather than obstruction. Discipline here is not procedural compliance; it is professional memory.

Exclusion as a Risk State. Exclusion is best understood not as a category of people, but as a risk state produced by defaults. When systems are complex, time is scarce, and understanding is costly, it becomes rational to follow procedures without fully grasping their internals.

This reflects adaptation to constraint rather than a lack of capability. If unmanaged, exclusion narrows the pool of professionals able to exercise independent judgment. It increases reliance on opaque processes and reduces resilience. Addressing this risk is an institutional responsibility rather than an individual indictment.

These postures are abstract. The following brief vignettes illustrate how they emerge in routine intelligence work as ways of operating under constraint.

Vignette 1 (High Confidence, Fragile Understanding)

A time-sensitive assessment draws on an automated system reporting high confidence in a developing situation. The team integrates the output quickly, operating in an orchestration posture shaped by tempo and decision demand. The result is coherent, plausible, and actionable.

Team members recognize that deeper interrogation of the system's assumptions would require shifting into a building posture, i.e., examining training data, edge cases,

and model sensitivities. Doing so would introduce delay and divert attention from coordination. Questions about failure modes are acknowledged but deferred.

The process reflects rational adaptation rather than neglect. The environment rewards timely synthesis and legibility. Understanding remains present but thin, and confidence rests on foundations narrower than they appear.

Vignette 2 (The Persistent, Plausible Narrative)

A digital dashboard aggregates complex operational data into a clean visual trend. The chart is intuitive, easily communicated, and quickly becomes a reference point across products and briefings. The narrative it supports is consistent and persuasive.

The team understands that the underlying data is more irregular. Cycles, gaps, and context-dependent variations exist beneath the aggregation. Surfacing those nuances would require a building posture, i.e., returning to raw inputs, unpacking assumptions, and complicating a story that has already achieved institutional traction.

Orchestration continues to dominate because alternatives are costly. Complication reduces clarity under tempo. Over time, however, the distinction between convenience and confidence becomes harder to see.

Quiet Drift

None of these dynamics produces immediate failure. They produce a quiet drift. As environments reward speed and integration, they favor confidence and plausibility. Over time, the balance among postures can shift. Orchestration becomes dominant. Building grows less visible. Auditing becomes harder to justify. Exclusion becomes normalized.

This drift is rational and gradual. It does not announce itself as error. When failures occur, they often occur at scale, and their origins can be difficult to trace. Recognizing this pattern is not an argument against digital systems. It is an argument for understanding the conditions they create. Countering this quiet drift requires tradeoff in time and effort. The following simple example illustrates this point.

Vignette 3 (Introducing Friction Deliberately)

A team leader notices that analytic work increasingly emphasizes integration and presentation, while opportunities to interrogate assumptions grow rarer. The work is efficient and responsive, but understanding is thinning by default.

Rather than slowing production wholesale, the leader introduces bounded friction. For selected briefs, responsibility rotates for articulating how an assessment could fail. The exercise is time-limited and preserves orchestration tempo while briefly shifting toward audit.

Preparation becomes marginally slower. Over time, however, analysts become more conscious of when they are orchestrating, building, or auditing. In the same environment, judgment becomes more deliberate because posture choice is visible again.

Implications for Professional Judgment

The value of this perspective is not operational. It is interpretive. Without a coherent way to understand the digital environment, many intelligence professionals experience modern work as a set of recurring tensions. Speed appears to outrun depth. Confidence is rewarded even when uncertainty remains. Verification becomes harder to justify under tempo. Some individuals seem to thrive without deep engagement with underlying systems. In the absence of an explanatory frame, these tensions are often attributed to leadership decisions, generational differences, cultural drift, or personal misalignment.

The environmental lens offers a different explanation. These tensions are predictable outcomes of operating inside a digital habitat

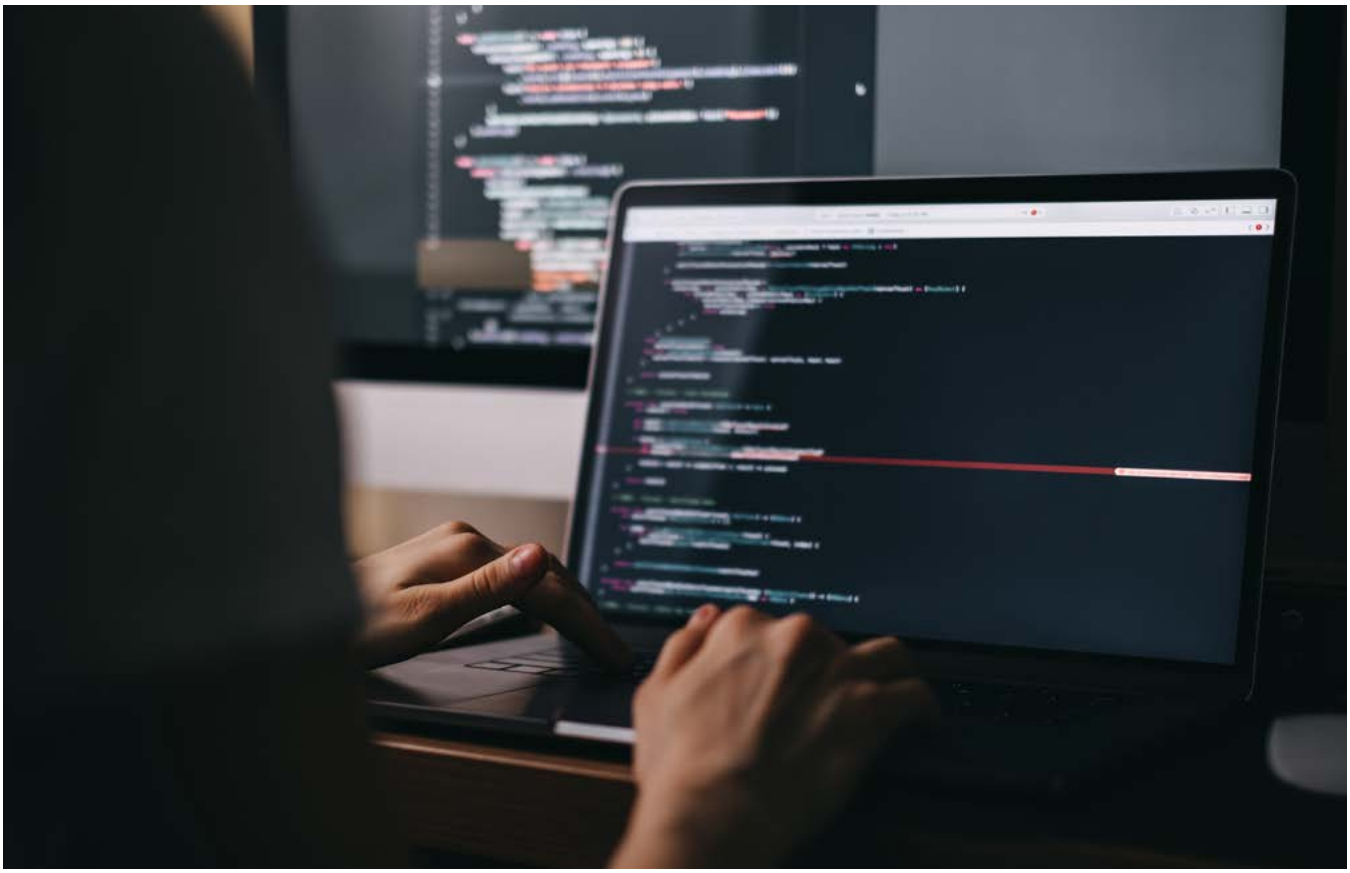
characterized by analytic abundance and uneven costs. Certain postures scale easily; others do not. Recognizing this does not excuse error or diminish standards. It clarifies why the pressures feel structural rather than personal. That clarity matters. It replaces cynicism with understanding.

This perspective also restores a measure of agency without pretending the environment may be controlled. Conversations about technology often collapse into false choices between embracing tools and resisting them. A more durable posture comes from understanding the environment well enough to choose how to operate within it. That choice involves self-knowledge and institutional self-knowledge. For a profession defined by judgment under constraint, this distinction is consequential.

Most importantly, this reframing speaks to professionalism itself. Professional intelligence has always included tradecraft, subject-matter expertise, and experience. It now also includes awareness of the selection pressures imposed by the digital environment. Knowing which postures are being rewarded, which are under strain, and when speed introduces epistemic risk has become part of the craft. The mission does not change. How one inhabits the mission does.

Judgment Remains the Mission

Intelligence has always been the practice of judgment under uncertainty. Tools change. Systems scale. The responsibility does not. Digital environments alter the conditions under which judgment is formed, but they do not alter its importance. Seeing those conditions clearly is now part of professional stewardship. This essay does not warn, predict collapse, argue for or against intelligence technologies, or propose tradecraft mandates. It offers a way of seeing the environment in which intelligence professionals now operate, so that discipline may be exercised deliberately rather than by default. Professional discipline in the digital era now includes recognizing which analytic postures are rewarded by default and which require deliberate protection. When posture choice becomes explicit rather than automatic, judgment becomes steadier under tempo and more resilient under uncertainty. ■



Significant improvements in generative AI are changing the nature of software in ways that demand a software-defined approach to intelligence. (AI-generated image of programmer working on a laptop, nickl-meel/Envato)

Software-Defined Intelligence

A New Way of Thinking About Tradecraft

William Schlickenmaier
The author is a former CIA Senior Analyst.

In the fall of 2023, I argued in these pages for rethinking intelligence analysis around the principles of software development.[1] I contended that Marc Andreesen's insight that "anything that can be software will be software" is as true for analytic production as for consumer applications.[2] I also made brief mention of emerging capabilities in generative artificial intelligence (GenAI) such as ChatGPT 4.0 that suggested this trend would continue if not intensify. Events since then have shown clearly that the accelerating pace of technological change are increasing the pressures for radical change in intelligence processes to meet customer demands.[3] In this article, I offer a new paradigm for thinking not only about analytic transformation, but about a broader change in our thinking about the craft of intelligence—the concept of "software-defined intelligence" based on prior work on software-defined warfare. I will outline six different forms or subcomponents of software-defined intelligence and propose a series of investments and policy changes to enable this change. Absent change, we risk having the IC find itself obsolete before it knows it.

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.

Defining Software-Defined Intelligence

In 2022, then-CIA Chief Technology Officer Nand Mulchandani and retired Air Force Lt. Gen. Jack Shanahan pioneered the concept of "software-defined warfare" in a paper for the Center for Strategic and International Studies.[4] In 2025, the Commission on Software-Defined Warfare defined the term as "a paradigm of the continuous integration and delivery of cutting-edge technology and leading interoperable software into legacy and future defense systems to drive a software-centric, hardware-enabled approach to warfighting."[5] As Mulchandani and Shanahan said in their 2022 report, "Software needs to be at the core of every business and operating model before any business can hope to gain an enduring advantage. The DOD is no different."

If the military is no different, the same can certainly be said of the Intelligence Community—indeed, even more so. Unlike the military services, which rely on advanced hardware (especially in the Navy and Air Force) to achieve their missions, the vast majority of the IC is in the information—thus the software—business.[6] All intelligence is information, and all information in the intelligence process is digitized at some point.[7] This means that a pivot away from manual processes and mindsets to one that embraces the digital is necessary to avoid obsolescence.

Software-defined intelligence is a mindset and a philosophy. It answers the question: How do we solve this intelligence problem with a software-first approach? It leans into automation, integration, and human-machine teaming to allow intelligence officers to excel at what humans excel at, not wasting their scarce time and expertise on arenas better served by computers.[8] It enables the continuous evolution of business processes by having rapidly scalable and changeable software at the core of all activities. To fully adopt software-defined intelligence, however, we have to go beyond legacy software processes.

Changing Nature of Software

Significant improvements in generative AI are changing the nature of software in ways that demand a software-defined approach to intelligence. In particular, the growth of agentic AI and "vibe coding" have so radically reduced the barriers to creating software that Andreessen's prediction of software eating the world may emerge sooner than expected. I did not foresee these developments in my 2023 essay, but if anything, two developing and overlapping trends—agentic artificial intelligence (AI) and so-called "vibe coding"—offer the prospect of deep transformation.

Agentic AI is the next generation of development beyond the large language models (LLMs) that reshaped the world with the release of ChatGPT 4. Unlike standard LLMs, which generate text, video, or visual representations based on a prompt, agents can be thought of as software that completes tasks.[9] While a year ago there was debate around the impact and prospects for agentic AI, the release of Claude's Mythos and Fable models and OpenAI's ChatGPT 5.6 model have laid those to rest, especially given their observed effects on both the private and public sectors.[10] Progress in capabilities fielded by the frontier labs just since the beginning of 2026 indicates progress is starting to grow at such a pace, particularly in software development, that it is having macroeconomic effects and reshaping the market for early-career coders.[11]

When fully scaled as currently imagined, agentic AI can complete—in some respects is already completing—complex tasks without human intervention. Focused on programming as opposed to human language, the agents can automate scripts, connect systems together, and perform other key functions. While the technology has yet to fully mature, it offers the prospect of significant gains for automation, particularly when paired with AI orchestration to combine agents.[12]

A subset of agentic AI has already caught the popular imagination. AI pioneer Andrej Karpathy

coined the term "vibe coding" in February 2025 to describe leveraging AI agents to write code for applications without any human programming.[13] Vibe coding radically reduces barriers to entry for bringing software to bear for any computer task—including the digital tasks all intelligence officers conduct.[14] While imperfect, being able to rapidly generate and execute code means that the "software-ization" of the digital world will accelerate.[15] We have seen this over the last year at speed and scale.

One example of this relevant to intelligence appeared at the June 2025 AI+ Expo, sponsored by the Special Competitive Studies Project. Anthropic, the frontier AI lab whose Claude Code software is the market leader, demonstrated the ability in less than 10 minutes to build a functional application displaying more than 3 million unstructured signals from ship beacons, including a geospatial layer and tracks over time.[16] How long would it take a team of IC officers using traditional tools to generate the same results? Since then, frontier lab capabilities have accelerated faster than anticipated and people are increasingly using these tools in day-to-day life.

In 2023, I argued that, at least for analysis, the time was ripe to imagine software as a model for delivering insight at speed. These developments transcend analysis—they will pervade every element of the intelligence process, and failure to grasp them and leverage them at scale will create systemic risks for the IC.

Building on Legacy Programs

Wholesale transformation of IC activities may feel impossible at first, particularly given budgetary and human capital constraints. The good news is that the move to a software-defined intelligence paradigm can build on investments over the last decade at multiple intelligence organizations that have blazed a path for progress.

The first is the IC's systemic investment in cloud computing, a necessary capability for any software-defined intelligence future.[17] Investments over the last decade in IC Gov Cloud and the IC Information Technology Enterprise (IC ITE) are fundamental and foundational to allow for the collaborative space demanded by software-defined intelligence.

The second is the paradigm shift toward object-based intelligence. Led by programs like NGA's Maven and DIA's Machine-Assisted Analytic Rapid-Repository System (MARS), object-based intelligence is the base layer for a significant amount of the processing needed for analytics at scale—the data software will need to compute for software-defined intelligence. Absent a properly structured base layer, the IC risks the classic statistical challenge of garbage in, garbage out.[18] MARS just reached initial operating capability in 2024, having launched in 2018, and is planned to reach full operating capability this year.[19] Maven transitioned from the Defense Department's Chief Digital and AI Office, where it began in 2017, to NGA in 2023.[20] Beyond that, the concept of object-based intelligence is increasingly prevalent in both defense and geospatial intelligence—but it needs to spread IC wide.[21]

At the same time, the vast majority of these have focused on analysis, as opposed to the full intelligence cycle. The software-defined intelligence paradigm requires that all components of intelligence, from collection to effects, be considered for disruption.

Six Elements of Software-Defined Intelligence

I argue that the paradigm of software-defined intelligence pervades all elements of the intelligence cycle and has implications for every component of and function in the IC. Six broad categories highlight this impact. In this introductory essay, I only briefly discuss each – follow-on assessments will explore implications and implementation of each.

Collection

We can imagine intelligence collection divided into digital-native and digital-enabled categories. Digital-native collection is technical collection (including open source) that collects digital information via machines. Digital-enabled collection is HUMINT that relies on digital capabilities to succeed for targeting and operational support.[a] The former is easier to imagine in a software-defined era, because agentic AI would enable everything from access development to defeating technical defenses.[22] On the latter side, software-defined collection would focus on identifying, mitigating, and eventually defeating the ubiquitous technical surveillance threat that holds espionage at risk.[23]

Processing, Exploitation, and Dissemination

Processing, exploitation, and dissemination (PED) is perhaps the most time-consuming aspect of the intelligence cycle and one where software-defined intelligence could yield the fastest and greatest advantages. All collection, whether digital-native or digital-enabled, goes from collectors to exploiters and analysts via software before being consumed by customers. Software therefore should radically speed the transmission of intelligence from the collection node to the sensemaking architecture (analysis). Especially in an era of ubiquitous data, edge processing will be increasingly necessary to distill valuable signal from noise before movement to data centers for machine exploitation.[24] Beyond that, exploitation and dissemination generated by agents in machine-native formats as opposed to natural language (or in addition to it) will be important for integration into object-based intelligence frameworks like MARS or NGA's Analytic Services Production Environment, as well as into application programming interfaces (APIs) for vibe-coded analytic and policy support applications.[25]

Analysis

Building on my prior "Agile Analysis" model, software-defined analysis would place machine intelligence at the heart of mapping pattern-of-life, a core requirement for any IC analytic account. To be clear, however, software-defined analysis is not outsourcing the analytic development process to machines—it enables humans to deliver more value-added work than the routine processes that take up significant bandwidth. Vibe coding makes possible the rapid fielding of analytics dashboards and custom applications that an analyst could tweak with the occasional advice of a supporting data scientist or programmer. It removes some of the human capital requirements of my original team approach to analysis and significantly speeds delivery.[26] Beyond that, agentic AI, combined with already existing LLMs, could transform the process of analytic editing and review, removing significant management overhead and speeding the delivery of insight to customers. These LLMs, when encoded with ICD 203, the CIA's style guide, and algorithms to detect bias and confidence levels, would significantly improve the quality and decrease potential politicization in analytic production when paired with agents to execute the quality control process.[27]

Defense and Security

As predatory adversarial capabilities spread and technology diffusion allows a greater number of actors to conduct counterintelligence activities, software-defined counterintelligence, cyber defense, supply chain risk management, and personnel and physical security measures will be critical to ensuring US decision advantage. The cybersecurity industry is already leaning heavily into AI-enabled defenses, and agentic AI is likely to speed these capabilities at the tactical edge.[28] ODNI has already implemented continuous evaluation as a framework for personnel security; agentic AI will be crucial to managing the spread and scope of this across the IC and with cleared private sector partners.[29] The Department of War is already exploring the use of AI for

a. Picking up a newspaper would be digital-enabled collection if the hardcopy paper were scanned and sent to someone. Downloading newspaper articles from a website would be digital-native collection.

supply chain risk management, a capability the IC could leverage at scale as well.[30] And as discussed above, agentic AI has applications not only for the detection and avoidance of ubiquitous technical surveillance, but can be harnessed at scale to detect foreign intelligence operations for both strategic defensive and offensive counterintelligence programs.[31]

Effects

Under Title 10 and Title 50 of the US Code, components of the IC are sometimes called upon not only to collect and analyze information but to conduct effects operations at the direction of the president or other senior leaders.[32] Software-defined effects go beyond cyber operations to also include how agentic AI and vibe coding, when paired with LLMs, can enable strategic and tactical precision effects. These include opportunities for wide-scale and precision messaging, potential disruption opportunities, and software enablement of other clandestine and covert activities.[33]

Infrastructure

The era of software-defined intelligence may have no more pervasive impact than on the enabling infrastructure and business systems that allow the IC to operate.[34] The private sector is already aggressively pursuing agentic AI for human resources, contract and budget, facilities, logistics, and other infrastructure requirements, as well as the business analytics that inform those infrastructure decisions.[35] As such, the IC can take advantage of private sector investments and rapidly scale efficiencies and effectiveness by harnessing these tools.

Enterprise Policy and Capability Requirements

Software-defined intelligence mandates enterprise architectures that can communicate with each other, and on which AI is pervasive. The answer cannot be a silo for an LLM with "normal software" elsewhere. Nor can it be an exclusive reliance on enterprise software solutions. Instead, IC architectures must enable coding at the edge—at the individual user level—with appropriate protections so that draft code does not spill into broader systems or yield systemic crashes. IC ITE is a strong starting point in this direction, but the fact that the IC still lacks an enterprise high-side system used by all members limits the interoperability that would be ideal for this approach.

Beyond technical capabilities—most of which are already feasible and available—the greater hurdle toward a software-defined intelligence approach is policy and regulations. A wide array of regulations and requirements govern the Authority To Operate (ATO) standard for secure computing at the Secret and Top Secret levels. As discussed below, risk management is integral to this approach—but not risk avoidance. Separate policies and regulations, such as Intelligence Community Directives (ICDs) that drive analysis and collection as well as department- and agency-specific regulations, do not embody this software-driven approach—but embedding these regulations within the software being fielded could yield further rewards.

Risk Management, Upskilling, and Software-Defined Intelligence

Risk management is the foundation of both the barriers to and the necessary conditions for software-defined intelligence. ICD 503, "Intelligence Community Information Environment Risk Management," is the standard for all software use in the IC and ATO accreditation.[36] Too often, risk management becomes risk avoidance because the consequences have typically been higher for acting and something going wrong than for not acting.[37] Technology is moving too fast to avoid action, but typical IC acquisition processes have relied on enterprise contracts with legacy vendors who provide individual software solutions. Agentic AI and vibe coding put these software solutions in the hands of individual officers, enabled by a back-end infrastructure and a level of trust and

empowerment that allows them to adapt at the tactical edge and the speed of mission.

At the same time, while agentic AI and vibe coding may appear to create a future where there is no need for software programmers, experts who have used these tools in the last year have actually reinforced that knowledge of coding and software development is still very valuable.[38] A conversational understanding of the nature of algorithms and some experience with hands-on coding is still a valuable skill, and indeed it may be more valuable than ever in this future where we expect individual intelligence officers to bring these capabilities to bear.

Next Steps

Software-defined intelligence is a framework. More than that, it is a mindset. This means that to bring it to fruition, those who agree with this perspective have to engage in the hard work of culture change. Advocates have already raised pieces of this, but more is needed—in particular, a mindset shift beyond the technologists to the mission users.

As a starting point, departments and agencies can look at their policies and regulations for those that either enable or hinder software-defined intelligence. At the IC level, a range of Intelligence Community Directives are a natural starting point. Beyond that, IC budgets and IT investments should further explore how to harness agentic AI at scale, and identify incubators or labs to prototype all six of the software-defined intelligence sectors discussed above. Failing to do so may well render the IC obsolete, faster than expected. ■

Endnotes

1. William Schlickenmaier, "Agile Analysis: Transforming Intelligence Production Through Lean Start-up Methods," *Studies in Intelligence* 67, no. 3 (2023): 15–22.
2. Marc Andreessen, "Why Software Is Eating the World," *Wall Street Journal*, August 20, 2011. https://www.wsj.com/articles/SB10001424053111903480904576512250915629460.
3. For the continuing dialogue on these questions in this journal, focused largely on analysis, see Dennis J. Gleeson, "Artificial Intelligence for Analysis: The Road Ahead," Studies in Intelligence 67, no. 4 (2023): 11–15; Zachery Tyson Brown, "'The Incalculable Element:' The Promise and Peril of Artificial Intelligence," *Studies in Intelligence* 68, no. 1 (2024): 1–7; Rachel Grunspan et al., "Emergent Intelligence: Spycraft and Intelligence in the AI Era," Studies in Intelligence 69, no. 4 (2025): 7–13; Andrea Brennan et al., "Snow Globe Multi-Player AI System: Lessons from Human-AI Teaming in War Games," *Studies in Intelligence* 69, no. 4 (2025): 15–21. For a more aggressive view, see Anthony Vinci, *The Fourth Intelligence Revolution: The Future of Espionage and the Battle to Save America* (Henry Holt and Company, 2025).
4. Nand Mulchandani and John N. T. Shanahan, *Software-Defined Warfare: Architecting the DOD's Transition to the Digital Age*, CSIS Strategic Technologies Program (Center for Strategic and International Studies, 2022). https://www.csis.org/analysis/software-defined-warfare-architecting-dods-transition-digital-age.
5. Whitney M. McNamara et al., *Commission on Software-Defined Warfare: Final Report*, Scowcroft Center for Strategy and Security (Atlantic Council of the United States, 2025). https://www.atlanticcouncil.org/in-depth-research-reports/report/atlantic-council-commission-on-software-defined-warfare/.
6. On how hardware intersects with organizational culture in the military services, see Carl Builder, *The Masks of War: American Military Styles in Strategy and Analysis* (Johns Hopkins University Press, 1989); S. Rebecca Zimmerman et al., *Movement and Maneuver: Culture and the Competition for Influence among the US Military Services* (RAND Corporation, 2019). It is true that significant components of the IC rely on hardware to collect intelligence; but the information itself, the value provided to the policy customer, is digital.

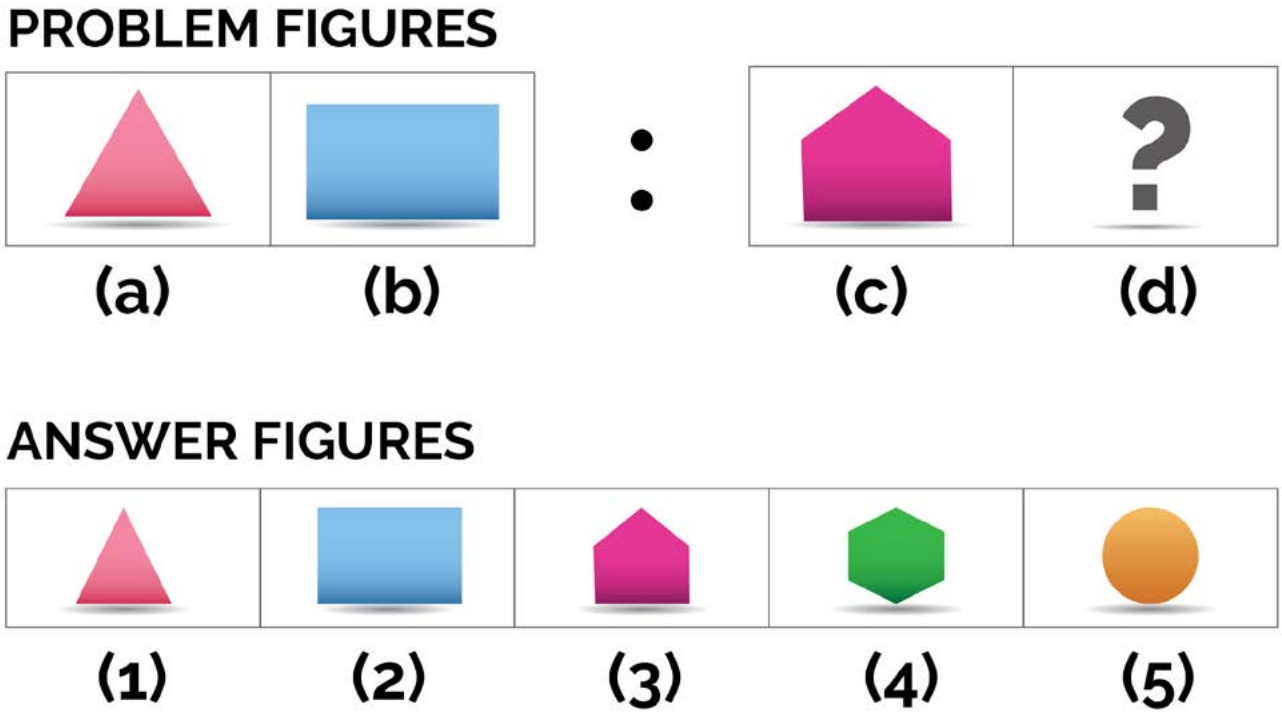
7. The only imaginable way in which intelligence information would wholly avoid digitization would be if a HUMINT source spoke to a case officer who took hardcopy notes or recorded them on an analog tape recorder, typed those notes on a manual typewriter, pouched those notes to the US via courier, and the US-based intelligence organization transferred those notes–again, either handwritten or manual typed–onto paper delivered in hardcopy to customers. Today's intelligence process renders that scenario implausible for all but the most restricted and limited-dissemination information.
8. On the concept of human-machine teaming, which has been discussed in national security circles for over a decade, see Robert O. Work, "Reagan Defense Forum: The Third Offset Strategy," Speech, Reagan Defense Forum, Reagan Presidential Library, Simi Valley, CA, November 7, 2015, https://www.war.gov/News/Speeches/Speech/Article/628246/reagan-defense-forum-the-third-offset-strategy/; Garry Kasparov, *Deep Thinking: Where Machine Intelligence Ends and Human Creativity Begins*, Reprint (PublicAffairs, 2018).
9. Cole Stryker, "What Is Agentic AI?," *IBM Think*, n.d., accessed October 16, 2025. https://www.ibm.com/think/topics/agentic-ai; Teaganne Finn and Amanda Downie, "Agentic AI vs. Generative AI," *IBM Think*, n.d., accessed October 16, 2025. https://www.ibm.com/think/topics/agentic-ai-vs-generative-ai.
10. Paul Mozur and Adam Satariano, "Anthropic's New A.I. Model Sets Off Global Alarms," *The New York Times:* April 22, 2026; Zvi Mowshowitz, "Claude Fable 5 and Mythos 5: Capabilities," Don't Worry About the Vase, June 19, 2026, available at https://thezvi.substack.com/; Zvi Mowshowitz "GPT-5.6: The System Card," Don't Worry About the Vase, June 28, 2026, available at https://thezvi.substack.com/
11. Rya Jetha, "AI Writes the Code Now. What's Left for Software Engineers?," *The San Francisco Standard* (San Francisco, CA), February 19, 2026. https://sfstandard.com/2026/02/19/ai-writes-code-now-s-left-software-engineers/; Noah Smith, "Superintelligence Is Already Here, Today," Substack, *Noahpinion*, March 2, 2026. https://www.noahpinion.blog/p/superintelligence-is-already-here; James Wang, "White-Collar Apocalypse Isn't Around the Corner—But AI Has Already Fundamentally Changed the Economy," Substack, *Weighty Thoughts*, February 19, 2026. https://weightythoughts.com/p/white-collar-apocalypse-isnt-around; Ryan Fedasiuk, "The Arrival of Strong AI," Substack, *Choosing Victory*, March 5, 2026, https://www.choosingvictory.com/p/the-arrival-of-strong-ai; Dean W. Ball, "On Recursive Self-Improvement," Substack, *Hyperdimensional*, February 5, 2026. https://www.hyperdimensional.co/p/on-recursive-self-improvement-part.
12. Erin Griffith, "A.I. Isn't Magic, but Can It Be 'Agentic'?" *New York Times*, September 8, 2024. On orchestration, see Ivan Belcic and Cole Stryker, "What Is AI Orchestration?," *IBM Think*, n.d., accessed October 16, 2025, https://www.ibm.com/think/topics/ai-orchestration.
13. https://x.com/karpathy/status/1886192184808149383 It is noteworthy that Karpathy is the same researcher who expressed skepticism about the status of agentic AI discussed earlier.
14. Kevin Roose describes this as "software for one—small, bespoke apps that solve specific problems in my life… [not] the kinds of tools a big tech company would build." Kevin Roose, "Not a Coder? With A.I., Just Having an Idea Can Be Enough.," B, *New York Times*, March 4, 2025. Tarun Chhabra, head of National Security at Anthropic, said in an interview that he imagined capabilities like vibe coding would lead to the "re-engineering" of much government business. Jordan Schneider, *Tarun Chhabra on the Stakes of AI Competition*, ChinaTalk, October 16, 2025, 19:15, 67 minutes, https://podcasts.apple.com/us/podcast/chinatalk/id1289062927?i=1000732041970.
15. Rhiannon Williams, "What Is Vibe Coding, Exactly?," *MIT Technology Review*, April 16, 2025, https://www.technologyreview.com/2025/04/16/1115135/what-is-vibe-coding-exactly/.
16. This presentation was specifically on June 3 at a joint presentation between Anthropic and Palantir. https://expo.scsp.ai/about/2024-recap/ For more on the Anthropic-Palantir relationship, see "Anthropic and the Department of Defense to Advance Responsible AI in Defense Operations," *Anthropic*, July 14, 2025, https://www.anthropic.com/news/anthropic-and-the-department-of-defense-to-advance-responsible-ai-in-defense-operations. I do not comment here on the current controversy over Anthropic's designation by the Department of War as a supply chain risk, but use this as an illustrative example of what is available from the range of frontier labs.
17. *The IC Data Strategy 2023-2025* (Office of the Director of National Intelligence, 2023), https://www.dni.gov/files/ODNI/documents/IC-Data-Strategy-2023-2025.pdf; *Strategic Plan to Advance Cloud Computing in the Intelligence Community* (Office of the Director of National Intelligence, 2019), https://www.dni.gov/files/documents/CIO/Cloud_Computing_Strategy.pdf.
18. L. Todd Rose and Kurt W. Fischer, "Garbage In, Garbage Out: Having Useful Data Is Everything," *Measurement: Interdisciplinary Research and Perspectives* 9, no. 4 (2011): 222–26.
19. George I. Seffers, "DIA Developing Order of Battle Capability for Space," *SIGNAL*, December 2, 2024, https://www.afcea.org/signal-media/dia-developing-order-battle-capability-space; Lauren C. Williams, "DIA's AI-Powered Intel Repository Will Be Fully Operational about a Year Late," *Defense One*, October 10, 2024, https://www.defenseone.com/defense-systems/2024/10/new-ai-powered-intel-repository-will-be-fully-operational-about-year-late/400188/.
20. "GEOINT Artificial Intelligence," *National Geospatial Intelligence Agency*, n.d., accessed October 22, 2025, https://www.nga.mil/news/GEOINT_Artificial_Intelligence_.html; "Palantir Expands Maven Smart System AI/ML Capabilities to

Military Services," Palantir Investor Relations, September 20, 2024, https://investors.palantir.com/news-details/2024/Palantir-Expands-Maven-Smart-System-AIML-Capabilities-to-Military-Services/. Maven more recently received significant press coverage because of its role in support of US military operations in Venezuela and Iran. See Tara Copp, et al., "Anthropic's AI Tool Claude Central to U.S. Campaign in Iran, amid a Bitter Feud," *The Washington Post* (Washington, DC), March 4, 2026, https://www.washingtonpost.com/technology/2026/03/04/anthropic-ai-iran-campaign/; Elizabeth Dwoskin et al., "In Trump's Washington, Palantir Is Winning Big," *The Washington Post* (Washington, DC), August 1, 2025, https://www.washingtonpost.com/technology/2025/08/01/palantir-trump-defense-tech-ai-software/.

21. Catherine Johnston et al., "Transforming Defense Analysis," *Joint Force Quarterly* 79 (October 2015): 12–18; Todd S. Bacastow et al., "From Layers to Objects: Evolving the GEOINT Analytic Tradecraft," in *The State and Future of GEOINT 2017* (US Geospatial Intelligence Foundation, 2017), https://usgif.org/wp-content/uploads/2024/06/2017_SoG.pdf; Patrick Biltgen et al., "Activity-Based Intelligence: Understanding Patterns-of-Life," in *The State and Future of GEOINT 2017* (US Geospatial Intelligence Foundation, 2017), https://usgif.org/wp-content/uploads/2024/06/2017_SoG.pdf; Brian Flanagan et al., *Intelligence After Next: Rethinking Collection Management to Better Track Mobile Targets*, nos. 23–4349, Intelligence After Next (MITRE Corporation, 2023), https://www.mitre.org/news-insights/publication/intelligence-after-next-collection-management-track-mobile-targets.
22. Schneider, *Tarun Chhabra on the Stakes of AI Competition*, 10:40.
23. Shawn Benson, *Intelligence After Next: Deciphering Ubiquitous Technical Surveillance with Data-Driven Analytics and Artificial Intelligence*, 24 1387, Intelligence After Next (MITRE Corporation, 2024), https://www.mitre.org/news-insights/publication/deciphering-ubiquitous-technical-surveillance; Warren P. Strobel and Ellen Nakashima, "CIA Chief Faces Stiff Test in Bid to Revitalize Human Spying," *The Washington Post*, May 28, 2025, https://www.washingtonpost.com/national-security/2025/05/28/cia-spy-china-russia-ratcliffe/; David Ignatius, "A Band of Innovators Reimagines the Spy Game for a World with No Cover," *The Washington Post* (Washington, DC), July 10, 2025, https://www.washingtonpost.com/opinions/interactive/2025/cia-ai-technology-spies/.
24. Brian Katz, *The Collection Edge: Harnessing Emerging Technologies for Intelligence Collection*, CSIS Briefs (Center for Strategic and International Studies, 2020), https://www.csis.org/analysis/collection-edge-harnessing-emerging-technologies-intelligence-collection.
25. Kimberly Underwood, "Greater Emphasis on AI at NGA," *SIGNAL*, March 11, 2025, https://www.afcea.org/signal-media/defense-operations/greater-emphasis-ai-nga.
26. Schlickenmaier, "Agile Analysis: Transforming Intelligence Production Through Lean Start-up Methods," 17–18.
27. *Intelligence Community Directive 203: Analytic Standards*, Intelligence Community Directive (ICD) 203, version 2023 TA, Office of the Director of National Intelligence, Active June 12, 2023, https://www.dni.gov/files/documents/ICD/ICD-203.pdf. Vico, an AI startup that launched in early 2026, has developed algorithmic capabilities to detect bias in production as well as model confidence levels. Insights provided by Vico's founder, Anthony Vinci, to the author. For more on Vico, see https://www.vico.io
28. Kevin Townsend, "Cyber Insights 2025: Artificial Intelligence," *SecurityWeek*, n.d., accessed October 23, 2025, https://www.securityweek.com/cyber-insights-2025-artificial-intelligence/; "Agentic AI in Cybersecurity: The Next Frontier for Human-Centric Defense," Cybersecurity, *Keepnet Labs*, March 14, 2025, https://keepnetlabs.com/blog/agentic-ai-in-cybersecurity-the-next-frontier-for-human-centric-defense.Security week and agentic ai
29. *Security Executive Agent Directive 6: Continuous Evaluation*, SEAD 6, version 1, Office of the Director of National Intelligence, January 12, 2018, https://www.dni.gov/files/NCSC/documents/Regulations/SEAD-6-continuous%20evaluation-U.pdf.
30. Adarryl Roberts, "Utilization of Artificial Intelligence (AI) to Illuminate Supply Chain Risk," *Defense Logistics Agency News*, May 1, 2025, https://www.dla.mil/About-DLA/News/News-Article-View/Article/4186367/utilization-of-artificial-intelligence-ai-to-illuminate-supply-chain-risk/#:~:text=Specifically%2C%20AI%20can%20assist%20with,pre%2Dqualified%20suppliers%20during%20disruptions.; "LMI Wins DOD Supply Chain Risk Evaluation Environment Contract," *WashingtonExec*, August 22, 2024, https://washingtonexec.com/2024/08/lmi-wins-dod-supply-chain-risk-evaluation-environment-contract/.
31. *Intelligence Community Directive 750: Counterintelligence Programs*, Intelligence Community Directive (ICD) 750, version 1, Office of the Director of National Intelligence, Active July 5, 2013, https://www.dni.gov/files/documents/ICD/ICD-750.pdf.
32. Authorities Concerning Military Cyber Operations, Pub. L. No. 115, 394 10 2123 (2018), https://www.govinfo.gov/content/pkg/STATUTE-132/pdf/STATUTE-132-Pg1636.pdf#page=488; Matters Related to Irregular Warfare, Pub. L. No. S.2226, 543 (2023), https://www.govinfo.gov/content/pkg/BILLS-118s2226pap/pdf/BILLS-118s2226pap.pdf; Presidential Approval and Reporting of Covert Actions, 3093 50, accessed October 23, 2025, https://www.law.cornell.edu/uscode/text/50/3093.
33. On precision messaging in particular, see Hui Bai et al., "LLM-Generated Messages Can Persuade Humans on Policy Issues," *Nature Communications* 16 (June 2025): 1–12, https://doi.org/10.1038/s41467-025-61345-5; "AI's Powers of

Political Persuasion," *Stanford University Human-Centered Artificial Intelligence*, February 27, 2023, https://hai.stanford.edu/news/ais-powers-political-persuasion.

34. For a view on the future digital requirements, see Randy Howard and Geralyn Blossom, *Intelligence After Next: Creating Interoperable And Antifragile Digital Platforms: A New Paradigm For Sensemaking*, 24 2265, Intelligence After Next (MITRE Corporation, 2024), https://www.mitre.org/news-insights/publication/intelligence-after-next-creating-interoperable-and-antifragile-digital.
35. Jill Barth, "What Is Agentic AI in HR? A Simple Explainer for People Leaders," *HR Executive*, May 19, 2025, https://hrexecutive.com/what-is-agentic-ai-in-hr-a-simple-explainer-for-people-leaders/; "How to Use AI Agents for Accurate Budget Tracking & Automation," *Datagrid*, April 8, 2025, https://www.datagrid.com/blog/ai-agent-budget-tracking; Andrew Renzella, "Agentic AI in Financial Services: The Future of Autonomous Finance Solutions," *AWS Marketplace*, September 8, 2025, https://aws.amazon.com/blogs/awsmarketplace/agentic-ai-solutions-in-financial-services/; Toby Yu and Annie McMillan, *Evolving CLM with Agentic AI: A Human-Centered Approach* (KPMG, 2025), https://kpmg.com/us/en/articles/2025/agentic-ai-in-clm-balancing-human-and-machine-expertise.html; Ryan Aytay, "Agentic Analytics: A New Paradigm for Business Intelligence," *Tableau*, April 15, 2025, https://www.tableau.com/blog/agentic-analytics-new-paradigm-for-business-intelligence#:~:text=Meet%20the%20world's%20first%20agentic,to%20swivel%2Dchair%20between%20platforms.; Ruben Phukan, "How AI Agents Can Transform Facilities Management into a Data-Driven Process," *Facilities Management Advisor*, May 23, 2025, https://facilitiesmanagementadvisor.com/maintenance-and-operations/how-ai-agents-can-transform-facilities-management-into-a-data-driven-process/.
36. *Intelligence Community Directive 503: Intelligence Community Information Environment Risk Management*, Intelligence Community Directive (ICD) 503, version 1, Office of the Director of National Intelligence, Active October 25, 2024, https://www.dni.gov/files/documents/ICD/ICD-503.pdf.
37. For a perspective on the importance of risk management and AI adoption for the IC, see Corin R. Stone, "Artificial Intelligence in the Intelligence Community: Know Risk, Know Reward," *Just Security*, October 19, 2021, https://www.justsecurity.org/78641/artificial-intelligence-in-the-intelligence-community-know-risk-know-reward/.
38. Josh Brake, "Live By The Vibe, Die By The Vibe," Substack, *The Absent-Minded Professor*, October 21, 2025, https://joshbrake.substack.com/p/live-by-the-vibe-die-by-the-vibe. ■



Humans have evolved an exceptional cognitive ability to prioritize structural relationships over surface-level features. Analogical thinking, the basis of human intelligence and creativity, allows people to map complex patterns from a known scenario to a new, unfamiliar scenario. (The solution to this example of a nonverbal analogy test is on the following page.)

Analogical Reasoning in Intelligence Analysis

Desk-side Evaluation Methods

Ryan Handy

The author is an MS candidate at the National Intelligence College of the National Defense University and a graduate of the Johns Hopkins School of Advanced International Studies. From 2022 to 2026, he ran an analytical tradecraft evaluation program of the Office of Intelligence and Analysis of DHS. Before that, he was an analyst and liaison officer for DoD, serving in various overseas assignments and Washington, DC.

Analogical reasoning is a pervasive heuristic tool we use to make sense of complex and ambiguous situations, reduce uncertainty, and aid decisionmaking. In the Intelligence Community, analysts often use analogical reasoning to make inferences, explain situations and their implications for US interests, or probe for clues to the future. Selecting analogies that best explain a current scenario—the issue under examination—is essential for supporting national security customers and maintaining analytic credibility. Yet experience tells us this selection process is fraught. In this article, I offer a method to improve it.

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.

Although humans use analogical reasoning daily, we can still use it improperly and fall into cognitive traps.[a] A common pitfall is vividness bias. It occurs when an observer is disproportionately influenced by information that is vivid, most readily accessible, or emotionally charged, even if the information in question is less credible. The focus on a vivid past situation may exclude other potentially stronger ones that would provide better insights for analysts and decisionmakers alike. The late CIA methodologist Richards Heuer noted:

> Frequently … a historical precedent may be so vivid and powerful that it imposes itself upon a person's thinking from the outset, conditioning them to perceive the present primarily in terms of its similarity to the past.[1]

Research indicates even highly experienced decisionmakers use analogical reasoning poorly, resulting in weak or fallacious arguments.[2] Further, Yuen Foong Khong's study on US decisionmakers' use of analogical reasoning suggests vividness and other biases are pervasive in the decisionmaking realm.[3] After North Korea's invasion of South Korea in June 1950, President Truman turned to events in the run-up to World War II to frame the situation and understand Washington's predicament. He viewed Japan's invasion of Manchuria (1931), Italy's invasion of Ethiopia (1935), and Hitler's annexation of Austria (1938) as analogues demonstrating that inaction in the face of aggression resulted in broader catastrophe, while leaving out other less vivid but credible precedents.[4]

As US involvement in Vietnam increased in the mid-1960s, the Korean War itself became a vivid but faulty analogy for President Johnson and several of his advisors. Khong reveals the extent to which the Johnson administration used Korea as a guiding precedent:

> [The] Korean analogy was used in private to define the nature of the problem in Vietnam, to assess the stakes of the problem, to prescribe possible responses, and to indicate the morality of those prescriptions.[5]

We can draw upon case studies and refine methods identified by academics to mitigate bias and other pitfalls that create defective analogies. In this article, I discuss some methods and offer a new one for consideration.

Identifying Fundamentals

Identifying the fundamental elements or issues of a current scenario is an important first step for establishing parameters. This helps us to avoid wasting time on irrelevant information or superficial commonalities that lead to poor analogical reasoning. William Flanik illuminates this pitfall in his study of the use of analogies and metaphors in foreign policymaking:

> The main pitfall of comparative reasoning is that surface-level similarities between target and source domains often overshadow more fundamental differences.[6]

Neustadt and May propose that we should first group elements into "Known," "Unclear," and "Presumed" buckets to establish our understanding of an issue. This focuses our minds on evidence and presumptions, helping to understand the information base, what is truly relevant, and any associated uncertainties. This step should improve the framing of analogical reasoning and subsequent steps by distilling the issues, reducing the potential for anchoring on misleading surface-level similarities.[7]

The Neustadt-May method should also help fix a scenario in time to prevent the creation of

a. The solution to the puzzle on the preceding page is answer 4: a triangle (three sides) is to a rectangle (four sides) as a pentagon (five sides) is to a hexagon (six sides).

overly broad or general analogies. Many intelligence questions are complex and protracted issues that may drive analysts to rely on hazardous mental shortcuts, increasing an analyst's susceptibility to cognitive traps. Individuals may focus on a less relevant point of time or the wrong driver in the base scenario, leading to faulty conclusions and time-wasting miscommunication. A correspondent for the Economist highlights this framing problem by invoking their effort to understand a new development within a major foreign policy issue that involves many actors and vivid events:

> When America started bombing the Houthis on March 15th [2025], your correspondent messaged a diplomat: Was this déjà vu or something new? The group, a Shia militia in Yemen, has been bombed so many times by so many people that the diplomat needed clarification. Déjà vu from when Joe Biden bombed them last year? From when Israel did so months later? Or from when a Saudi-led coalition began bombing almost a decade earlier?[8]

Vietnam's turbulent and complicated history probably produced a similar dynamic for the Johnson administration. In 1965, National Security Advisor McGeorge Bundy provided President Johnson a memo on the "Americanization" of the Vietnam conflict that compared the United States' situation to France's own experience in Vietnam. Bundy sought to challenge a more credible France-Vietnam analogy championed by Undersecretary of State George Ball but anchored his own analogy on France's defeat in 1954 at Dien Bien Phu and the subsequent withdrawal of French forces. This revealed limited similarities to the US position in 1965, when Washington was much less militarily committed in Vietnam.[9] Ball, on the other hand, looked to 1950–51 to invoke France's own pained decisionmaking for increasing force levels and the initially higher levels of French public support for war. Ball's framing enabled him to anticipate some of the critical challenges the United States would face.[10]

Similarities-Differences Analysis

Similarities-Differences analysis can help us further evaluate and eliminate presumed analogues. This technique provides a quick, economical structure for testing the strength of prospective analogies. Users list known critical elements to identify and weigh the similarities and differences between the current situation and past scenario, revealing the appropriateness of the past event for providing potential insights into the future. Users need only to create a table with paper, whiteboard, or software applications (e.g., Word, PowerPoint).

To illustrate this method (Figure 1, next page), I replicate some elements from a 1964 memo Ball sent to Johnson and other senior officials questioning the suitability of the Korean War analogy for debating greater US military involvement in Vietnam.[11] These scenarios occupy the first and second columns; the third is for evaluating the suitability of the elements and assigning a value: weak, moderate, strong, or not analogous or possibly ambiguous/unclear. (Analysts should use other terms that make sense given the nature of the assembled information).

The conspicuous lack of critical analogous elements should rule out the use of the Korean War as an instructive analogue for considering US commitments to Vietnam. The salient differences—as captured by Ball—indicate the burden could be higher for the US than it was in Korea, demonstrating that similarities-differences analyses can provide valuable insights even when they fail to validate scenarios as having credible analogous attributes.

Reflection-Mapping: A New Approach

I offer this method (Figure 2, page 31) for evaluating the suitability of proposed analogues and for extracting maximum insights from the analogues under examination. I call it "reflection-mapping" because the method compares two

Korea 1950	Vietnam 1964	Qualification Explicit or Implicit
Political Legitimacy: US involvement under clear UN mandate, conferring clear international legitimacy; Korea sought US support	Presence in South Vietnam "depends on the continuing request of the [government of South Vietnam] (and a SEATO protocol)."	Weak/Not analogous
Political Legitimacy/Host Government Stability: South Korean government stable, general support, limited factional jockeying for power	"In South [Vietnam] we face governmental chaos"	Not analogous
Allied Military Commitment: UN forces provide 53,000 (non-US and non-South Korean) personnel	In Vietnam we are "alone with no substantial help from any other country"	Not analogous
Resolve: Korea had been independent for two years before North Korea invaded the South; South Koreans fighting	People of Vietnam have been fighting for almost 20 years; "all evidence points to the fact they are tired of conflict"	Not analogous Perceived war fatigue suggests US may shoulder greater combat/military burden
War Context: The North invaded–crossing a sovereign border with 100,000 troops–resulting in UN support for intervention on behalf of South Korea	There has been no invasion, "only slow infiltration"; Viet Cong has strong indigenous support; that Hanoi is directing Viet Cong operations is not so clear to outside world	Not analogous Vietnam conflict is far more ambiguous; Viet Cong and weakness of Saigon may incline observers to perceive conflict as an "internal rebellion"

Figure 1. Analogical elements derived from a memo written by Undersecretary of State George Ball in 1964. Adapted from Yuen Foong Khong, *Analogies at War: Korea, Munich, Dien Bien Phu, and the Vietnam Decisions of 1965* (Princeton University Press, 1992).

scenarios by organizing critical information across a horizontal meridian.

Reflection-mapping builds on similarities-differences analysis by providing space for deeper comparisons of evidence, critical forces or factors while showing how these elements interact. If anything, this technique can help analysts organize their thoughts; observers will notice this method has similarities to argument mapping and, depending on your approach, back-casting.

Technology or Capabilities Development

Reflection-mapping can help us understand the implications of emerging technologies or capabilities, including their significance in other fields, domains, or scenarios. Analysts can use it to

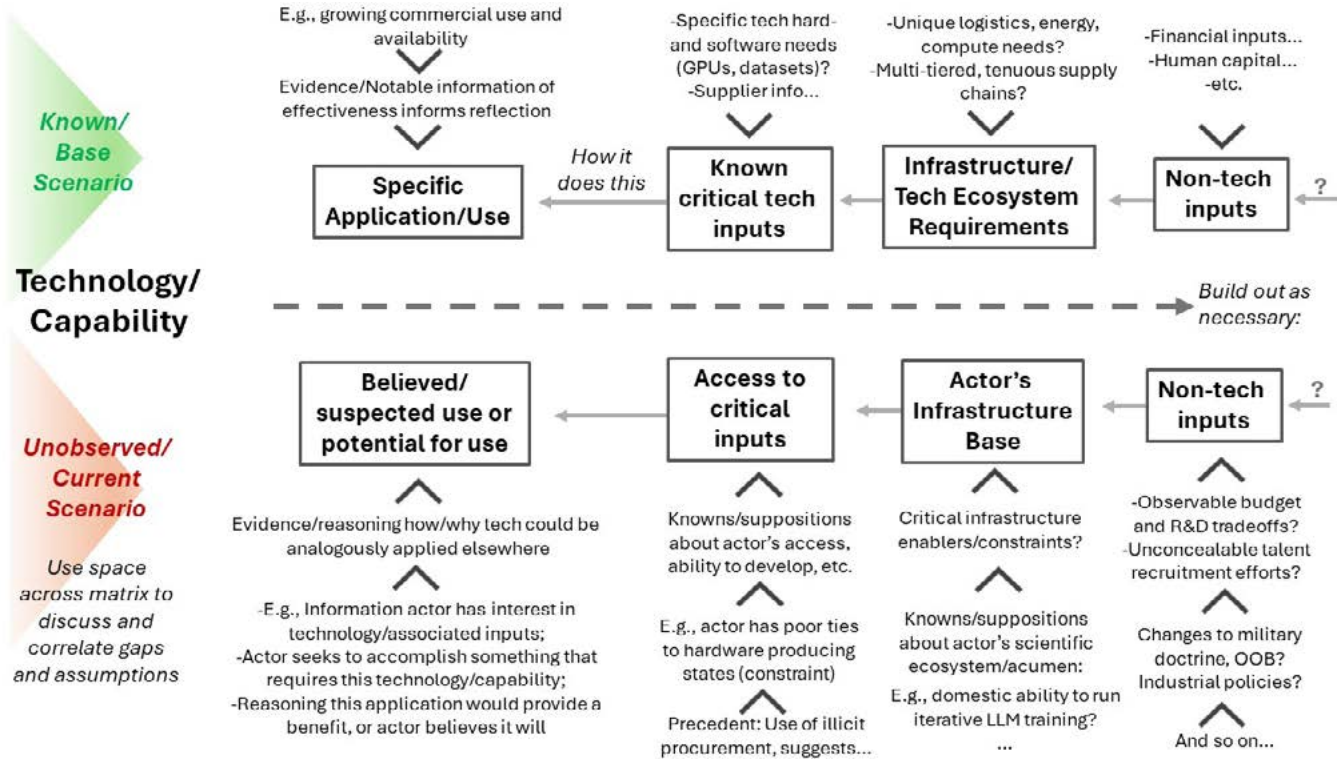


Figure 2, Reflection Mapping template for technology or capability: Integrate the Neustadt-May methods across the map to vet your suspected analogy, hone your reasoning, and identify potential indicators and opportunities for US action.

identify processes, inputs, skill-sets, and chokepoints that may affect an actor's ability to develop a specific capability. Reflection-mapping may also help practitioners identify, develop, or refine indicators for warning.

To start, place the meridian higher on the medium (paper, PowerPoint, etc.) to provide more space for the Unobserved/ Undetected section, the target domain (current scenario). This creates space to discuss reasoning and the fragmentary evidence, gaps, and assumptions. Above the meridian, identify the base technology or capability (base scenario); clearly describe its function and demonstrated use. Then identify the underlying technology enablers.

Use the space radiating out from the meridian to organize and explore evidence, inferences, critical assumptions, and intelligence gaps that affect these other elements of analysis. The meridian can be expanded to the right to accommodate sub-elements, factors or forces relevant to the technology in question or any actors pursuing it.

In the following demonstration (Figure 3, next page), I use reflection-mapping to glean insights into a fictitious country's ability to use computer vision for specific military ends. Computer vision has broad applications, but it is used by some countries to monitor individuals in the name of public safety. This application is our base scenario (also known as source domain). For the sake of demonstration, I posit the current scenario is an undemonstrated or unobserved application of computer vision to the military domain. I use analogical reasoning to assess computer vision's ability to improve offensive targeting because I suspect the underlying technology function—identifying and distinguishing objects—has transferable attributes to the military domain.

My map is bounded by the finite space provided in this article, but there is nothing to keep analysts from building more expansive maps.

As I will demonstrate, reflection-mapping can refine our thinking and assessments by helping to identify the breadth of the requisite input, supporting technologies,

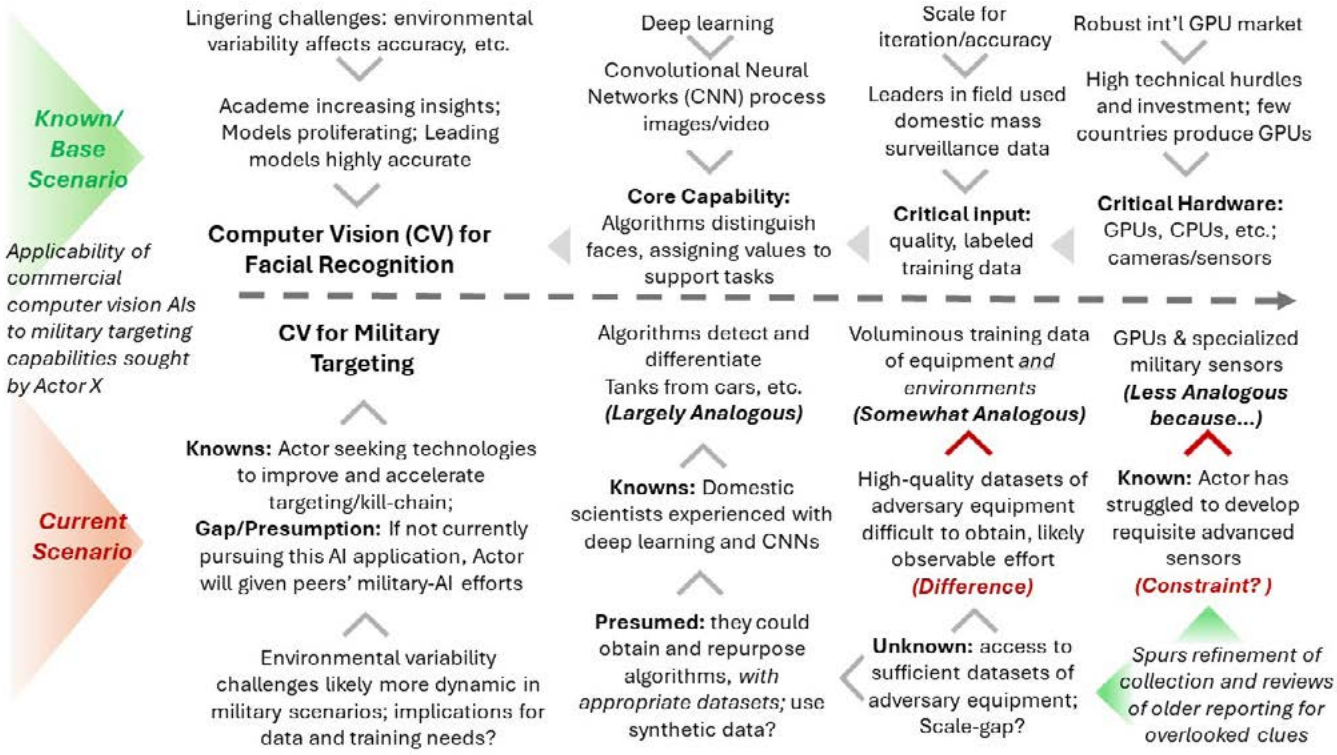


Figure 3, Technology Example for Actor X: Our map helped us to understand the strengths and limits of the analogy and the challenges the actor may face in pursuing this technology. The method can support actor-agnostic analogy vetting depending on the framing of the intelligence question.

processes, and skill-sets—factors we may easily overlook. The technique can support exploratory analysis in other areas, like the potential for nefarious actors to use AI intended for drug discovery and synthesis for developing novel narcotics or deadly toxins. What does researchers' work say about operational milestones and computing power requirements? This information may help contextualize any observed activity or fragmentary information in evidence bullets.

As analysts map scenarios, this method may also help them consider alternative explanations for ambiguous reporting, the significance of individual elements, or biases or analytic leaps: are those aluminum tubes for centrifuges or an Italian rocket system the Iraqi military wanted to reproduce?[12]

Historical Analogues

Reflection-mapping can help anticipate the potential trajectory or implications of complex issues such as unexpected conflicts or the decisionmaking of foreign actors. For example, it could help one probe whether an actor might use an unscheduled military exercise as cover to invade a neighbor or a cartel's recent actions can be explained by those of other cartels, illuminating future developments and their implications for US interests. Depending on how one frames the intelligence question and map, they can reveal forces at work and patterns that can aid warning and generate additional indicators.

The mapping structure for these scenarios largely resembles Figure 3, except our base scenario (located above the meridian) is a past event and we organize themes like analysis, collection/knowns, and other analytic elements and other tradecraft processes.

For this demonstration (Figure 4, above), we've generated a fictitious crisis for our current scenario: the autocratic monarch of Eastland

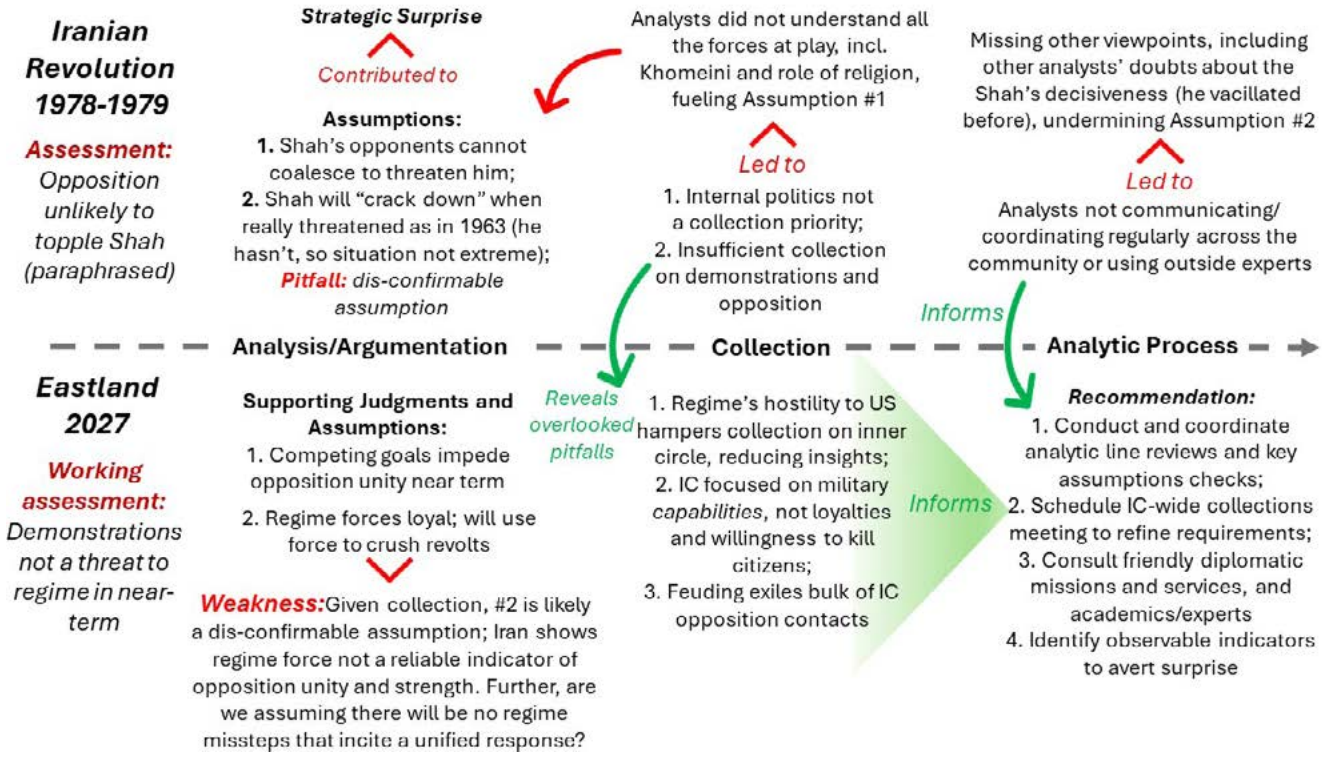


Figure 4. The use of intelligence case studies as potential analogies enables us to perform a form of pre-production diagnostic analytic line review, providing insights for avoiding analytic traps and potentially strategic surprise.

is facing growing popular opposition but is firmly in control of his security forces. Several vivid similarities lead us to recall the Iranian Revolution as a potential analogue that could reveal important insights into Eastlandic internal dynamics and our own analytic process, reducing the potential for strategic surprise. For example, are we repeating the errors of past Iran analysts by relying on unconfirmable assumptions about the monarch's willingness to crush his opposition when seriously threatened?[13] Are we mistakenly relying on regime reactions to draw conclusions about the opposition's strength?[14]

This process may help analysts determine the existence of commonalities relevant to the reader's needs for digestible context and warning. For our fictitious current scenario, it could look like this:

> The religious opposition is increasingly invoking nationalist narratives to challenge the Eastlandic regime, a development likely to draw strength from competing secular opposition groups. During the Iranian Revolution, Ayatollah Khomeini invoked nationalist narratives to gain support from the Shah's secular opponents and increase pressure on the monarch, a dynamic that was underestimated at the time.

The implication and policy prescription are such: as in Iran in 1979, things could unravel quickly; pay closer attention to the opposition.

This example shows how this form of mapping may produce more insightful analogical reasoning that aids processes like important reappraisals of collection strategies or assumptions based on other analogies. According to a study conducted by the late academic Robert Jervis for the CIA, some analysts believed the

Shah would "crack down" on the opposition when seriously threatened because he had in 1963, though there was some evidence that he may have been hesitant to use massive force; this assumption could be instructive to Eastland analysts. Analysts also may have overestimated the sufficiency of the US government's information base, reducing the impetus to alter collection. Reflection mapping-style processes can help expose what Jervis described as hazardous "circularity" wherein collection on an issue is poor because analysts believe a situation is stable.[15]

Conclusion

Flanik writes "analogies seem most prevalent and influential in security decision making," suggesting intelligence analysts have an even greater obligation to use analogical reasoning carefully and to consider diverse methods for developing credible analogies.[16] Members of the Intelligence Community and the curious public will undoubtedly develop better and more user-friendly techniques that can benefit our craft. I hope this article inspires further debate.■

Endnotes

1. Richards J. Heuer, *Psychology of Intelligence Analysis* (Center for the Study of Intelligence, CIA, 1999), 38.
2. Sjoerd Keulen, "Historical Analogies: Functions, Limitations and the Correct Use of Historical Analogies in Applied History," *Journal of Applied History 5*(2) (2023): 111–31. See also Yuen Foong Khong, *Analogies at War: Korea, Munich, Dien Bien Phu, and the Vietnam Decisions of 1965* (Princeton University Press, 1992), 13.
3. Khong, *Analogies at War*.
4. Richard E. Neustadt and Ernest R. May, *Thinking in Time: The Uses of History for Decision-Makers* (Free Press, 1986), 34–36.
5. Khong, *Analogies at War*,117.
6. William M. Flanik, "Analogies and Metaphors and Foreign Policy Decision-making," in T. Cameron G. (Ed.), *The Oxford Encyclopedia of Foreign Policy Analysis* (1 ed., Vol. 1 of 2 ,) (Oxford University Press, 2018), 128.
7. Neustadt and May, *Thinking in Time*, 89–90.
8. *Economist*, "Many bombs, little thought," April 5, 2025, 35.
9. Neustadt and May, *Thinking in Time,* 81–85, and Khong, *Analogies at War*,154–55.
10. Khong, pages 104-110, 150-153.
11. "How Valid Are the Assumptions Underlying our Vietnam Policies?" See Khong, 106–11.
12. Robert Jervis, *Why Intelligence Fails: Lessons from the Iranian Revolution and the Iraq War* (Cornell University Press, 2010), 127–28, 142–43, 213.
13. Jervis, *Why Intelligence Fails*, 69–71.
14. Jervis, *Why Intelligence Fails,* Chapter 2.
15. Jervis, *Why Intelligence Fails,* 4, 17–18, 41–42, 69–75.
16. Flanik, "Analogies and Metaphors and Foreign Policy Decision-making," 8. ■

Secrets and Secrecy

The Case for a Practitioner's Dialogue

Joseph Gartin and Timothy Schulz

Joseph Gartin is a retired CIA officer and past managing editor of *Studies*. Timothy Schulz is a program manager in the Center for the Study of Intelligence.

"Tell me the secret that you possess."

"I will not, for this is in my power."

Epictetus, *Discourses*

Writing about government secrets and secrecy is irresistible, judging from the many books, scholarly articles, industry publications, and commentaries that now treat the US Intelligence Community. With varying degrees of accuracy and thoughtfulness, many of these works make broadly similar arguments: The US government over-classifies information (Hathaway, Lebovic, Maret); It relies too much on secrecy and secrets in the conduct of national security decisionmaking and actions (Brown, Connelly, Monyihan); and publicly available information increasingly supplants secrets (Zegart). More advice comes from prominent think tanks, which argue the IC needs to step out from behind the wall of official secrecy and embrace new, more open ways of doing business (Weinbaum, et al.). A small but important body of academic work in recent years has tackled the thorny ethical considerations around state secrecy (Fabre, Ben Jafel, Pozen), building in part on foundational scholarship (Sissel, Shils, Bok), and wrestled with epistemological questions applied to intelligence analysis (Whitesmith).

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 authors' views.

This list is hardly exhaustive, as the explosive growth in intelligence literature in the past two decades shows (Coulthart, Rorissa), but it represents the broad contours of mainstream, English-language discourse about secrets and secrecy in the IC. Although one can point to flaws in some of the arguments for and against secrecy in intelligence, taken together they highlight an opportunity for practitioners.

In this essay, we argue secrets and secrecy are naturally integral to intelligence, and yet neither is subject to rigorous evaluation by those who create and value them most. We explore the reasons behind this gap, examine the carrying and epistemic costs of secrecy, contest arguments against government secrecy, explore potential analogs that could help inform the IC's relationship to secrets and secrecy, and suggest areas of further research.

Before proceeding, it is useful to define some terms. Secrets are bits of information that are willfully withheld. As we will discuss in detail, secrets are not fixed things; they shift in response to changes in perceived value of openness versus privacy. The reader does not know what we had for breakfast. That is not a secret, because there is no perceived value in concealing or revealing the information. On the other hand, if readers wanted to poison our breakfast because they are our mortal enemies, they would conceal their intention and capability; if we knew either bit of information, we would conceal our dining habits.

Turning to secrecy, we observe at least three senses of the word and their relationships to one another. The first is the willed act of nondisclosure: to make, hold, or selectively share a secret is to engage in secrecy. We call this base definition act-secrecy. This is the everyday sense of the word. A person or group decides not to let someone know a piece of information.

Secrecy also points to a normative system prescribing, regulating, or often dominating a member's disclosive or non-disclosive calculus. This system-secrecy appears as an epistemic and social arrangement. The system must judge the default status of information: What newborn information can pass into discourse, what falls secret, and who decides?

But secrecy can also refer to something much larger than mere secret-keeping. Secrecy also points to a type of normative system. It is normative because it prescribes or regulates information disclosure and non-disclosure, circumscribes the individuals or types of people who can be admitted into the system and occupy roles within it, and describes the sanction regime for violations. Unlike act-secrecy, system-secrecy is an epistemic and social arrangement. One of its main epistemic tasks is determining the default status of newborn information. That is, what can pass into discourse, what falls secret, and what must be adjudicated one way or the other. The system must also decide the individuals or sorts of individuals who have the power to modify and regulate the system of secrets—this is a political and social decision as much as a counterintelligence or bureaucratic concern.

A third sense of secrecy is constitutive-secrecy, i.e., an organization's attempt to constitute itself in the larger political sphere. The "Glomar response"—neither confirm nor deny—is emblematic of this constitutive-secrecy.[a] Glomar is not in the first instance about information nor about a system aimed at handling secrets. It is an organization's attempt to define itself by its secrecy. If one were to ask the tax agency for another's tax records, the agency would simply say "no." If one were to ask an intelligence organization for secret records, the Glomar response conveys to the requester that the IC is not the sort of place that discloses its business. Glomar does not keep a secret so much as foreclose inquiry into the possibility of a secret.

a. The term is taken from revelations of Project AZORIAN, in which the Hughes *Glomar Explorer* was used in a covert, CIA-led attempt to recover a sunken Soviet submarine in 1974.

Dominating Characteristic

Secrets and secrecy are as necessary to protect political communities as they are to protect individual liberty. Unlike some outside the IC, we do not assert *a priori* that the IC abuses secrecy, and we reject as indefensible the premise that secrecy is unnecessary in today's global information environment or that secrecy is incompatible with liberal democracy. Essential functions of government, including but not limited to the national defense (for example, setting interest rates or negotiating contracts), would be impossible without the capacity to keep some secrets. That said, the weight of secrecy is heavy.

Reviewing Sissela Bok's *Secrets: On the Ethics of Concealment and Revelation* in these pages in 1984, John Harington observes that secrecy is "the dominating characteristic of intelligence work, whether it is a question of the safeguarding or compromise of one's own secrets or the acquisition by stealth of another."[a] Of course, governments are not alone in keeping or seeking secrets. Secrets and secrecy, Bok argued, are essential for individuals and the state alike. They preserve the physical, emotional, and temporal space necessary to make decisions and safeguard the privacy and intimacy needed for human coexistence.

Forty-plus years on, however, we would argue secrecy is not only the how of intelligence, as Harington observed, but the what. Like the old saw about one young fish asking another as they swim along—"What is water?"—today's intelligence practitioners are so immersed in secrets that they cannot readily distinguish between secrecy as an act, culture, process, or outcome. Prying these differences apart would enable a constructive dialogue owned by practitioners.

Secrets of the State

For centuries, *arcana imperii*—the mystery of rule—meant state secrecy was largely immune to checks and balances, and the arguments against openness redound across epochs, regions, or polities. Leaders of every stripe have assiduously held to the principle that secrecy is essential to the exercise of executive power, that total transparency is impossible given human nature, and that the sovereign alone can determine what is and is not secret. We need look no further than the Founders' defense of secrecy during the American Revolution. George Washington argued, "All that remains for me to add is, that you keep the whole matter as secret as possible. For upon Secrecy, success depends in most Enterprises of the kind, & for want of it, they are generally defeated, however well planned." (Quoted in Lathrop)

Despite the continuity of this logic across history and forms of government, some political communities have gradually if grudgingly imposed limits on state secrecy. Within the United States, for example, construction of these guardrails began in earnest in the 1970s, driven by a changing media environment, abuses of executive power, revelations of unlawful intelligence and police activities, and evolving norms for legislative oversight. Since then, successive cycles of revelation and response in the late 20th and early 21st centuries ushered in a complex array of laws, policies, and procedures that partially constrain intelligence agencies' inherent capacity to abuse secrecy.

We stress inherent, because what is remarkable about secrecy in the US Intelligence Community is the extent to which it is not abused, given its enormous capacity and capability. (To be sure, ours is a contested viewpoint.) We emphasize partially because this state of restraint is entropic; history shows that maintaining the status quo depends on norms and behaviors that can change, often suddenly, under external or internal influences.

Habits of Secrecy

The place to begin this examination is with secrecy itself. Individuals and groups of all kinds—families, social networks, private societies, cults, congregations, corporations, and governments—keep secrets. For

a. John Harington, review of Sissela Bok, *Secrets: On the Ethics of Concealment and Revelation* (Pantheon Books, 1982), *Studies in Intelligence* 28, No. 2 (Summer, 1984).

individuals, habits of secrecy are learned at a very young age, as centuries of fiction have explored: secret powers, friends, languages, forests, labyrinths, and portals, to name a few. Imagine *The Lion, the Witch, and the Wardrobe* without a secret doorway to Narnia, *Harry Potter* without his invisibility cloak to move secretly through the corridors of Hogwarts, or *Harriet the Spy* without her secret notebook filled with information about her classmates and neighbors. Scholars have further observed that, for children, secrets and the physical or mental spaces they create offer power in the face of omnipresent vulnerability. (Sturm, Bosman, and Lambert)

Indeed, power and vulnerability are at the very heart of act-, system-, and constitutive-secrecy. Bok observed, "Some capacity for keeping secrets and for choosing when to reveal them, and some access to the underlying experience of secrecy and depth, are indispensable for an enduring sense of identity, for the ability to plan and to act, and for essential belongings. With no control over secrecy and openness, human beings could not remain either sane or free." This is true, we would argue, whether the secrets belong to a child or a government.

Secrecy exists in every level and every role of government decisionmaking, but it naturally has an outsized role in national security enterprises, where power is concentrated in the executives. We need not look very hard to find examples from history:

- During the Warring States (403–221 BCE) period in China, strategist Lu Shang advises, "In employing the army, nothing is more important than obscurity and silence. In planning, nothing is more important than not being knowable. The greatest affairs are not discussed, while the employment of troops is not spoken about."[a]
- In his history of Rome's tumultuous Year of the Four Emperors (69 CE), Tacitus recounts how the short-lived emperor Marcus Otho Caesar Augustus rebuked his soldiers: "We are preparing for war. Do you imagine that we could publish all our dispatches, and discuss our plans in the presence of the whole army, when we have to devise a systematic campaign and keep up with the rapid changes of the situation? There are things a soldier ought to know, but there is much of which he must be ignorant."[b]
- Fifteen hundred years later, Giovanni Botero, the great sixteenth-century adviser to Italian courts, observes, "Secrecy is also of great importance to a prince; not only does it make him like God, but men, ignorant of his intentions, are kept in suspense about his schemes."[c]

Pathologies

If secrets and secrecy are endemic to governments and essential to freedom of action, they are also at the heart of every kind of institutional scandal: torture of prisoners, polluted drinking water in poor neighborhoods, medical experimentation on the unwitting, abuse of children, and so on. Unifying these disparate attacks on human dignity, which disproportionately affect the weakest among us, are the mutually reinforcing pathologies of unchecked secrecy in powerful institutions:

- Absolute executive authority over secrecy, whether by decree, assent, or tradition.
- Expansive scope and depth of what institutions might consider secret, including membership, rites, knowl-

a. Cited in Ralph D. Sawyer, "Traditional Chinese Conceptions and approaches to Secrecy, Denial, and Obfuscation," *Studies in Intelligence* 64, No. 1 (March 2020).
b. Tacitus, *Histories*, Loeb Classical Library (1925). www.penelope.uchicago.edu/Thayer/E/Roman/Text/Tacitus/Histories/2A*.html.
c. Giovanni Botero, *The Reason of State,* trans. Peter Joseph Waley and Daniel Philip Waley (Yale University, 1956), 56.

edge, ignorance, capabilities, and intentions.

- Absence or impotence of channels for appeal or arbitration.
- Weakness or complicity of counterbalancing institutions, like the police, civil society, press, or courts.
- Wide-ranging, often lifelong, strictures against revealing secrets.
- Coercive tools to enforce secrecy, including censorship, banishment, garnishment, imprisonment, torture, and death.

Hesitancy among practitioners to critically examine secrecy is driven by three broad factors. First, intelligence services worldwide generally see secrecy through the lenses of security, compliance, and authority. Bok observed that "keepers of secrets can experience the powerful, the forbidden, and the sacred with the same awareness that outsiders have of such secrets as both endangered by and dangerous for those who come too near or who expose them." This esoteric relationship with secrecy, she argued, "inheres in the sense of sacredness that people can have with respect to themselves, their families, their professions, their nations. It serves as an indispensable function in protecting these, but it can also deflect moral inquiry."[a]

Within secret organizations, the esoterica of system-secrecy manifests in multiple ways: extensive barriers to entry, such as testing, vetting, and training; ritualized introductions to secrecy through ceremonies, oaths, and documents; the adoption of new identities; messaging that equates employer to family; rigid, vertical lines of authority over what is and is not secret; arcane segmentation of the population into in and out groups; and isolation from the public common.

These combine, intentionally or not, to stifle vigorous debate, and this is acutely so within intelligence services. The immutable connection between intelligence (the what) and secrecy (the how) leaves the practitioner with little intellectual space to evaluate its impact or to offer alternatives. At best, such efforts look quixotic; at worst, they may be perceived as professionally fraught.

Secrecy Besieged?

Second, intelligence practitioners are naturally inclined to dismiss calls for less secrecy and more openness as risky, impracticable, or even malicious. As a result, IC insiders have largely ceded the intellectual conversation to non-practitioners in media and academia. This is not to devalue those perspectives, as our bibliography indicates, but rather to observe that intelligence officers often reflexively reject challenges to secrecy. Writing in 2011, for example, Bowman Miller calls WikiLeaks "an aberrant manifestation of transparency advocacy" that had turned "the whole notion of operational security and protection of sensitive sources" on its head. Miller doubles down, arguing that the ability to keep secrets is endangered.[b]

Miller's claim conflates act-secrecy (creating a secret) with system-secrecy (keeping a secret), and in either case it is contradicted by the explosion in intelligence collection 15 years on. However prevalent the view of secrecy as besieged, the simple fact is that worldwide, intelligence agencies are keeping vastly more secrets, not fewer, and nothing has slowed the growth.

The principal challenge today is not that states cannot keep secrets, rather that governments must collect, store, and safeguard exponentially greater numbers of secrets. The accumulation occurs as both an intentional outcome (e.g., disseminated analysis) and as a waste product, in the same way that mining a small amount of gold results in vastly disproportionate amounts of worthless, toxic tailings that must be retained for

a. Bok, *Secrets*, 39.
b. Bowman H. Miller, "The Death of Secrecy: Need to Know…With Whom to Share," *Studies in Intelligence* 55, No. 3 (September 2011).

generations. Every new seam of secret information adds to the pile.

Disparate Obligations

Finally, the third factor is the traditional separation (at least in the US system) between the provider and consumer. We mean more than the generally accepted divisions of labor for reasons of efficiency, expertise, and security, or the divide between policymaker and analyst to safeguard objectivity. Instead, we emphasize the gap in ethical duty. The IC is left to ensure that the acquisition of the secret meets the ethical tests—do we really need it or will it answer a question we have?—along with any legal requirements for lawful collection. In contrast, consumers of intelligence need only to concern themselves with reliability and utility.

Truth to Power

A further challenge in fostering a conversation about secrecy is IC messaging and lore, which tend to equate secrecy with truth. We need look no further than the inscription from John 8:32 inside the entrance to CIA's headquarters: "And ye shall know the truth, and the truth shall set you free." (The critical context is missing: Jesus was disclosing His divine nature.) Similarly, every IC officer knows the mantra that the community should "speak truth to power," echoing an eponymously titled Quaker pacifist treatise published in March 1955. And yet, the IC does not possess the truth. It works to build understanding and to deny the same to others. Secrecy enables and hinders those goals.

A deep dive into theories of truth is well beyond the scope of this essay. It is sufficient to observe that there is a difference between truth as a comprehensive understanding of the world and facts as the basic units of truth that the IC collects, assesses, and uses to promulgate contingent knowledge. Perfect collection would yield all the secrets, but we might still lack all the relevant facts and the understanding formed by their correct ordering. This is because secrets are not facts; they might not even be true, but rather falsehoods, half-truths, and outright deceptions (like Curveball's fabricated reporting on Iraqi weapons of mass destruction).

For intelligence practitioners, the truth-to-power expression embodies truths in the furtherance of a state's interests. Scholars have emphasized that objectivity in intelligence is inherently elusive because no intelligence officer approaches the task without significant cognitive biases. (Marrin) In the United States specifically, these biases reflect a general if sometimes uneasy elite consensus formed and refined in the mid-to-late 20th century and further adapted to the post-9/11 world. This consensus historically saw the United States as a superpower shaping the international order and defending liberal democratic institutions. There is nothing universal about this consensus; analysts in Beijing, Moscow, New Delhi, or Brasilia will approach the truth-to-power responsibility in vastly different ways.

This is not to subscribe to a kind of relativism, but rather to stress that even intelligence truths are relationships with propositions, and those relationships are more fluid than practitioners generally acknowledge. Take for example Usama bin Ladin's safe haven in Abbottabad, Pakistan, in spring 2011. Known but to him and the inner circle that protected him, the fact of his location was transformed into a secret by his need to keep it from us. In turn, for the United States, Bin Ladin's presence was not understood at the time as a fact, even though it was ultimately true. It was at best a proposition.

Contingency

Abbottabad reminds us that secrecy is a value model between discovery and concealment. This contingency depends on a relationship between parties who keep or seek secrets, often both at once. The long hunt for Bin Ladin was an interplay between prey and pursuer, with each side shifting between those roles, along the way creating, protecting, and discarding secrets. For those in the know, Abbottabad was an unmentionable secret, then in a blink, it was not.

What changed was the value of withholding versus revealing the information, not the fact itself. In essence, the secret of Abbottabad was demonetized by Bin Ladin's death.

For intelligence practitioners, however, the idea of contingency is naturally fraught. For one, keeping secrets is exceptionally difficult even within secret organizations. The temptation to share a secret can be overwhelming; once loosed it spreads exponentially. How many times has an intelligence officer said or heard, "this is close hold, but…"? Extending Sissel's argument, the need to know clashes with the brief thrill of sharing, whether gossiping online or in a sensitive compartmented information facility, in the way that we most treasure some precious object the moment we lose it.

Carrying Costs

One effect of this blurring is to obscure the substantial costs of secrecy imposes, beginning with carrying costs. There is some hazard in trying to apply business models to government activities, but intelligence is a commodity like any other. It requires capital and labor to produce, and this production involves carrying costs: property, maintenance, depreciation, training, insurance, warehousing, etc. States, institutions, or groups require hierarchy, rules, norms, infrastructure, and workers to gather, assess, sort, distribute, and store secrets. The more expansive security organizations become, the more banal their records. Witness the trivial but thorough documentation of citizens' daily lives by domestic spy agencies in East Germany or Albania, among others, whose mundane secrets spilled into the streets when their authoritarian governments collapsed. (Garton Ash, Ypi) Intelligence organizations need the capacity to gauge requirements for new secrets, prevent theft or chase down leakers and spies, deflect inquiry, vet those who may need access, or selectively divulge secrets. (Pozen)

We can think of this as system-secrecy, with its complex interplay of internal and external forces affecting an ever-shifting population of secrets. In the United States, this system began to take shape at scale during World War I with the passage of the Espionage Act of 1917, faltered in the interwar years, and established a permanent foothold after World War II with the National Security Act of 1947 and subsequent legislative and executive actions. Eight decades on, it is a colossus. As one former policymaker noted, in 2017—the last year for which data are official and public—roughly four million Americans with security clearances classified some 50 million documents at a cost of around $18 billion. (Hathaway)

Furthermore, we can reasonably postulate that these reflect only direct costs. A complete accounting is utterly impossible because secrets come in a variety of forms: tangible goods, like documents, records, and physical property, of course, but also intangibles like identities, memories, relationships, knowledge, plans, intentions, and desires. However one measures them, the costs of secrecy last multiple generations and inevitably grow over time. Just as we cannot calculate the costs of existing secrets and secrecy, there is no estimate of their future costs in the national security realm. In budgetary terms, we might think of them as a deferred obligation akin to social service programs or infrastructure repairs.

Health Care Analogy

To understand the enormity of future carrying costs, we looked for analogous problems. One is the cost of providing veterans' health care in the United States. Like secrets, wars create a bow wave of future expenses; unappropriated for in the present, they must be reckoned with eventually. For example, according to a prominent scholar, Veterans Administration expenditures for World War I veterans peaked in 1969, 50 years after the armistice, and those for World War II veterans crested in 1982. (Bilmes, 2011) Her updated estimates of total health-care costs for 9/11-generation veterans (2001–21) are upward of $2.5 trillion in 2050. These costs grow because the complexity of veterans' healthcare needs increases with age even as the number of

living veterans in the cohort gradually declines and eventually reaches zero. (Bilmes, 2021)

This analogy only takes us so far, however, because unlike generational cohorts that can be projected over time with a high degree of actuarial confidence, secrets are unbounded cohorts that move along multiple axes. Put more bluntly: all veterans eventually die; secrets live on. One might, for example, first array secrets along an x-axis of *time* and a y-axis of *value*. To this simple quadrant we might add a third dimension: *volume*. The complexity of our mental graphic grows if we consider that an individual secret's placement is not fixed. A secret's importance can grow or fade, for example, and new secrets alter old.

Moreover, we can attribute value to secrets in their final states and in their constituent elements. In other words, if a chocolate chip cookie is a secret, so too are the ingredients (flour, sugar, eggs, etc.). But it doesn't end there. Much like the coastline paradox, in which the fractal properties of a coastline make it hard to decide on the minimum feature to be measured, secrets spawn geometrically more secrets. Thus, our secret cookie also means secrets about recipe testing, marketing strategies, social media data, pricing, demand, production rates, customers, packaging, supply chain vulnerabilities, competitors, corporate ambitions, and so forth. Acknowledging that there are many uncertainties and variables that will affect the future cost of safeguarding today's secrets, it seems likely that transactional costs will grow as the volume of information grows.

Epistemic Costs

In addition to carrying costs, we think practitioners should also confront the non-monetary costs of secrecy. Knowledge is central to intelligence, and so first among secrecy's non-monetary costs is its effect on the formation and distribution of knowledge. The fuzzy consensus among epistemologists carves up knowledge into justified true belief, absent spoilers. Setting aside justification and spoiler cases as worthy of their own investigation in other forums, we focus simply on true belief.

Secrecy in the first instance aims to prevent some particular person or group from forming a belief. The trouble is that secrets cannot themselves discriminate. Secrecy keeps the intended *incognoscenti* in their darkness along with all else who lack formal and actual access. Formal access bypasses act-secrecy; a person has the clearance to be informed and thereby update his beliefs. But system-secrecy also requires informal access. Contrary to popular depictions or questions from family back home, there is no secret scrolling ticker on our screens or Big Book of Cool Secrets we receive after the oath of office. Secrets in a system move strangely or not at all compared to the chatter of ordinary life. Practitioners must recognize a gap in their beliefs or the beliefs of others and know what office, system, or person might fill it. In a sprawling enterprise like the IC, this is not trivial.

A would-be knower's belief must be true. For some questions, achieving a true belief is straightforward, even if difficult. "Is Bin Laden in Abbottabad now?" enjoys strict bivalence: it is either true or false. This type of thin question—one person, one place, one time—can be consequential for the IC, but more often, intelligence questions are conceptually thick. "Is the regime stable?" brims with possibilities. The question decomposes into a host of individual propositions: a line of boxes that must be filled with true beliefs individually to reach a true belief about the regime's stability collectively. These boxes are roughly joined by conjunction, meaning that a top-line true belief is achieved by the truth of the series of propositions {A and B and C and D and… N}. A single false belief could be a spoiler for epistemic success.

Secrecy acts like a tax on each individual proposition in a conceptually thick intelligence question. The obvious tax is the secrecy of our adversary. This tax is often transparent, however. We often know we have seen through the secrecy or we have not. Within the IC, secrecy (and functional

specialization) distributes information unevenly across departments and agencies, but is it difficult to account for exactly how. The secrecy of compartmentalization, multiple computer networks, and the core sources-and-methods protections interfere with true belief formation by blocking-access to information as a default position.

Susan Maret gives us a more elegant vocabulary for the problem of information distribution within the IC. Writing in the journal *Secrecy and Society*, Maret describes a phenomenon outside the intelligence community that we find resonates equally well within it. In the context of the challenges of teaching secrecy (based on her work on government secrecy around environmental policy), Maret makes a useful distinction between information that is open, closed, or what she dubs as twilight.

The first two categories will be familiar to the intelligence professional. Open information is available to the public, and "it does not violate official secrets and is approved for public dissemination." Closed information is controlled by the institution and depends on a need to know; it "will either never be made public or become known decades later." Her third category is more intriguing: twilight information, she says, is the space between, "the half-knowing that results from redacted, declassified documents; while redaction suggests disclosure, openness, publicity, and transparency, it also contains uncertainty."

To extend Maret's analysis, the phenomenon of twilight information exists within the IC just as much as outside of it, whether in a nod to some proposition behind a compartment without disclosing the details, the unknown half-life of one's understanding after being read out of an old account, or a pack of lawyers heading to a closed-door meeting. These suggest there is a truth, and it is out there, but not here.

Informed Choice

In considering how the IC might reframe its relationship with secrecy and better contemplate costs, we looked at an unlikely source of inspiration: shopping.

In a traditional mental model of the intelligence cycle, the end user is someone remote to the process: an elected official, policymaker, soldier, etc. Yet in reality, intelligence practitioners are the principal consumers of intelligence, vastly outnumbering policymaking/decisionmaking consumers. As such, they exert a powerful collective force over what intelligence is targeted, collected, disseminated, analyzed, and evaluated. In essence, the internal IC consumer is the crucial intelligence sub-cycle—the sun gear within a planetary gearbox, if you will—in the traditional schematic of the intelligence cycle.

Over the years, intelligence organizations have tried to understand how intelligence practitioners value specific types of information, first through simple surveys (i.e., what users say is important) and in more recent years through data analytics (what users actually cite, download, share, etc.) These evaluations are useful to a point, but they do not require the user to account for carrying or epistemic costs. Furthermore, they measure what was used, but not what will be or should be used; they are neither predictive nor normative.

For practitioners, secrets are the ultimate free goods. They do not routinely consider the cost to acquire, use, ignore, store, or dispose. As with all (perceived) free goods, this leads to distortions in consumer behavior. Let's imagine that an intelligence analyst is writing an assessment based on two essentially identical pieces of information, one unclassified and one highly classified. The carrying costs of the unclassified information are *de minimus*, while the classified report would need to be safely handled and stored for 25–50 years, maybe more. The analyst, having no incentive to consider costs, relies on other factors in making their decision, such as perceived accuracy, reliability, exclusivity, or prestige.

Could intelligence practitioners rewire the secrecy heuristic? One option would be to explore strategies that increase the information available to the intelligence

consumer at what we might think of as the point of sale. Such strategies address what are known as information-market failures, i.e., when individuals or firms lack information about economic decisions because of ignorance, uncertainty, or inattention. The IC borrows terms from business and economics—client, customer, product, and so forth—but it lacks actual market mechanisms to inform consumers choices. Two long-running programs—Proposition 65 and Energy Star—offer a starting point for how the IC might change this model.

Proposition 65

In 1985, California lawmakers enacted the Safe Drinking Water and Toxic Enforcement Act, more widely known as Proposition (Prop) 65 after the original referendum, requiring that businesses provide clear and reasonable warnings to consumers when products contain substances that are known to cause cancer or reproductive harm. Prop 65 also banned the discharge of those substances into any source of drinking water.

Eventually Prop 65 became a national and even global phenomenon; each of us has encountered the now familiar warning that a particular item contains an ingredient known to cause cancer. Sometimes maligned as government overreach or used as a punchline for jokes about rats getting cancer, scholars of Prop 65 argue it has been extraordinarily successful in reducing toxic exposures to lead, ethylene oxide, perchloroethylene, and other substances, and in prompting significant reformulations of innumerable consumer products. For goods that cannot be reformulated, like seafood, Prop 65 has resulted in warnings about mercury that enables consumers to make informed choices. (Rechtschaffen, Willams)

EnergyGuide and ENERGY STAR

Another long-lived effort at informing consumer and producer choices can be found in the household appliance sector. In the wake of the energy crisis of the mid-1970s, the US government created the EnergyGuide labeling system that mandated that all products display a large label with detailed information about annual energy consumption and costs. In 1992, the Environmental Protection Agency established the ENERGY STAR certification program. Unlike the familiar yellow EnergyGuide label, the ENERGY STAR contains no information. Scholars note that regular updates to certification requirements are necessary as technology changes and new products come onto the market. (McWhinney, et al.)

Consumer surveys suggest these labeling schemes have an impact—known as a welfare effect—on retail purchase decisions, although the degrees vary. Scholars note that some consumers react more to detailed information in the EnergyGuide label or to the simpler ENERGY STAR certification; some will overpay (relative to projected cost savings); others will focus on expected operating costs versus efficiency or initial price. Still other consumers might disregard energy information altogether and focus on other aspects they value, like perceived prestige. These differences reflect the heterogeneity of purchasers that must be taken into account when designing information programs. Nonetheless, taken together, "the data suggest that the certification acts as a substitute for more accurate, but complex energy information."[a]

Objections

Could consumer-information systems help drive a dialogue among intelligence practitioners about which secrets to collect, evaluate, publish, and store? In turn, could individual decisions eventually scale to have collective impact, in essence setting a "price" for secrets, that might reshape the IC's approach? We think the answer to both questions is a qualified yes. That said, a brief discussion of objections is in order. At least three present themselves.

a. Sebastien Houde, "How Consumers Respond to Environmental Certification and the Value of Energy Information," E2e Working Paper 007 (December 12, 2016): 3.

The first objection is that we are am trying to commodify national security secrets, a category of goods that is not subject to market forces. In short, secrets aren't cans of tuna or dishwashers, and as such we cannot easily establish what economists refer to as a willingness to pay (WTP). We note that this exception is not as total as it might first appear. Markets do set WTP for goods and services that are similar to national security secrets, such as subscriptions for services that protect our personally identifying information on the web. This corollary only takes us so far, however, because there is no market to freely trade national security information. As the leading scholar in the field notes, "individual preferences, and aggregated WTP, may not capture the value of (some) goods."[a]

A second objection is that mechanisms like Prop 65 or EnergyGuide are intended to nudge consumers toward what should be, i.e., particular outcomes established by some third actor (such as state regulators), rather than what is. As such, even when the outcome might be widely considered to have a welfare effect—increasing organ donations, for example—the state is exercising influence over personal decisions or infringing personal choice. A discussion of debates within and about normative versus positive schools of economic thought is well beyond the scope of this article. It is sufficient for our purposes to acknowledge that objections in behavioral economics, social sciences, and popular media are likely to have parallels in intelligence that are not casually dismissed. All the same, these and other objections are a call to action rather than an argument for doing nothing.

Future Research Paths

That begins with the IC, which excels at understanding foreign trends and adversaries but spends less time trying to understand itself. How might we address the knowledge gaps?

- Applied ethnographic research blending qualitative and quantitative approaches, including observation, interviews, surveys, and data collection, could shed light on why, when, and how practitioners collect, evaluate, and share individual reports.
- Web analytics could tell us how information flows into, through, and out of IC components.
- Gaming could sharpen our understanding of when and why collectors, analysts, and customers under or over value intelligence reporting and how price sensitive they are.
- Artificial intelligence might provide deeper insights into the IC's vast information holdings, refine new information needs, discover alternative data, and reduce the inevitable tailings.

Taken together, these and other avenues of research could help animate a debate within the IC about how to evaluate and reduce the epistemic and carrying costs of secrecy.■

a. Cass R. Sunstein, "Five Objections to Commodification" (March 2, 2026). https://ssrn.com/abstract=6329338 or http://dx.doi.org/10.2139/ssrn.6329338.

Select Bibliography

Ben Jaffel, Hager, and Alvina Hoffmann, Oliver Kearns, Sebastian Larsson, "Collective Discussion: Toward Critical Approaches to Intelligence as a Social Phenomenon," *International Political Sociology* (2020) 14, 323–44.

Bilmes, Linda J., "Current and Projected Future Costs of Caring for Veterans of the Iraq and Afghanistan Wars," *M-RCBG Faculty Working Paper No. 2011-06* (2011).

Bilmes, "The Long-Term Costs of United States Care for Veterans of the Afghanistan and Iraq Wars," Costs of War Project, Brown University, Watson Institute of International & Public Affairs, August 18, 2021.

Bok, Sissela, *Secrets: On the Ethics of Concealment and Revelation*, (Pantheon Books, 1982).

Brown, Zachery Tyson, "Biden Has a Golden Chance To Remake US Intelligence," *Foreign Policy*, January 22, 2021
Connelly, Matthew, *The Declassification Engine* (Pantheon, 2023).
Coulthart, Stephan, and Abebe Rorissa, "Growth, Diversification, and Disconnection: An Analysis of 70 Years of Intelligence Scholarship," *Intelligence and National Security* 38, No. 1 (June 2023): 1–17.
Fabre, Cecile *Spying Through a Glass Darkly: The Ethics of Espionage and Counter-intelligence* (Oxford University Press, 2022)
Garton Ash, Timothy, *The File: A Personal History* (Random House, 1997).
Hathaway, Oona "Keeping the Wrong Secrets: How Washington Misses the Real Security Threat," *Foreign Affairs* (January/February 2022).
Hatlebrekke, Kjetil Anders, *The Problem of Secret Intelligence* (Edinburgh University Press, 2019).
Hegghammer, Thomas, "The War on Terror Supercharged State Power," *Foreign Affairs* (September/October 2021).
Hofstadter, Richard, "The Paranoid Style in American Politics," *Harper's Magazine* (November 1964).
Houde, Sebastien, "Consumers' Response to Quality Disclosure and Certification: An Application to Energy Labels," E2e Working Paper 007 (December 2016).
Lathrop, Charles, ed., *The Literary Spy* (Yale University Press, 2004).
Lebovic, Sam, *State of Silence: The Espionage Act and the Rise of America's Secrecy Regime* (Basic Books, 2023).
LeCompte, Margaret, and Jean Schensul, *Designing and Conducting Ethnographic Research*, Vol. 1 (AltaMira Press, 1999).
Lester, Genevieve, *When Should State Secrets Stay Secret? Accountability, Democratic Governance, and Intelligence* (Cambridge University Press, 2015).
Mahnken, Thomas G., Selective Disclosure: A Strategic Approach to Long-Term Competition (Center for Strategic and Budgetary Assessments, 2020).
Maret, Susan, "Concealing in the Public Interest, or Why We Must Teach Secrecy," *Secrecy and Society* 2, No. 2 (January 2021).
Marrin, Stephen, "Analytic Objectivity and Science: Evaluating the US Intelligence Community's Approach to Applied Epistemology," *Intelligence and National Security* 35, No. 3 (2019).
Manosevitz, Jason, review of Genevieve Lester, *When Should State Secrets Stay Secret? Accountability, Democratic Governance, and Intelligence* (Cambridge University Press, 2015), *Studies in Intelligence* 60, No. 3 (September 2016).
Miller, Bowman, "The Death of Secrecy: Need To Know…With Whom To Share," *Studies in Intelligence* 55, No. 3 (September 2011).
Monyihan, Daniel Patrick, *Secrecy: The American Experience* (Yale University Press, 1998).
Pfaff, Debora and Bowman Miller, "From a Whisper to a Shout: The IC Should Use Its Outside Voice," *Research Short* (National Intelligence University, June 23, 2021).
Pozen, David, "The Leaky Leviathan," *Harvard Law Review* 127, No. 512 (2013).
Rechtschaffen, Clifford, and Patrick Williams, "The Continued Success of Proposition 65 in Reducing Toxic Exposures," *ELR News & Analysis* (December 2005).
Sawyer, Ralph, "Traditional Chinese Conceptions and Approaches to Secrecy, Denial, and Obfuscation," *Studies in Intelligence* 64, No. 1 (March 2020).
Schklar, Judith, "The Liberalism of Fear," in *Liberalism and the Moral Life*, (Harvard University Press, 1989).
Shils, Edward, *The Torment of Secrecy The Background and Consequences of American Security Policy* (The Free Press, 1956).
Sissel, Georg, "The Sociology of Secrecy and of Secret Societies," *American Journal of Sociology* 11, No. 4 (January 1906).
Stolze, Travis D., review of Matthew Connoly, *The Declassification Engine* (Pantheon, 2023), *Studies in Intelligence* 67, No. 2 (June 2023).
Spivack, Miranda S., *Backroom Deals in Our Backyard: How Government Secrecy Harms Our Communities and the Local Heroes Fighting Back* (The New Press, 2025).
Sturm, Brian, and Renee Bosman, Sylvia Leigh Lambert, "Windows and Mirrors: Secret Spaces in Children's Literature," *New Review of Children's Literature and Librarianship* 14, No. 2 (2008).
Travers, Mark, and Leaf Van Boven, Charles Judd, "The Secrecy Heuristic: Inferring Quality From Secrecy in Foreign Policy Contexts," *Political Psychology* (2013).
Tzamarelou, Sofia, *Intelligence in Democratic Transitions: A Comparative Analysis of Portugal, Greece, and Space* (Georgetown University Press, 2024).
Ypi, Lea, *Free: A Child and a Country at the End of History* (W.W. Norton & Co., 2021).
Weinbaum, Cortney, and Bradley Knopp, Soo Kim, Yuliya Shokh, *Options for Strengthen All-Source Intelligence: Substantive Change Is Within Reach* (RAND Corporation, 2022).
Whitesmith, Martha, "Justified true belief theory for intelligence analysis," *Intelligence and National Security* 37, No. 6 (2022).■