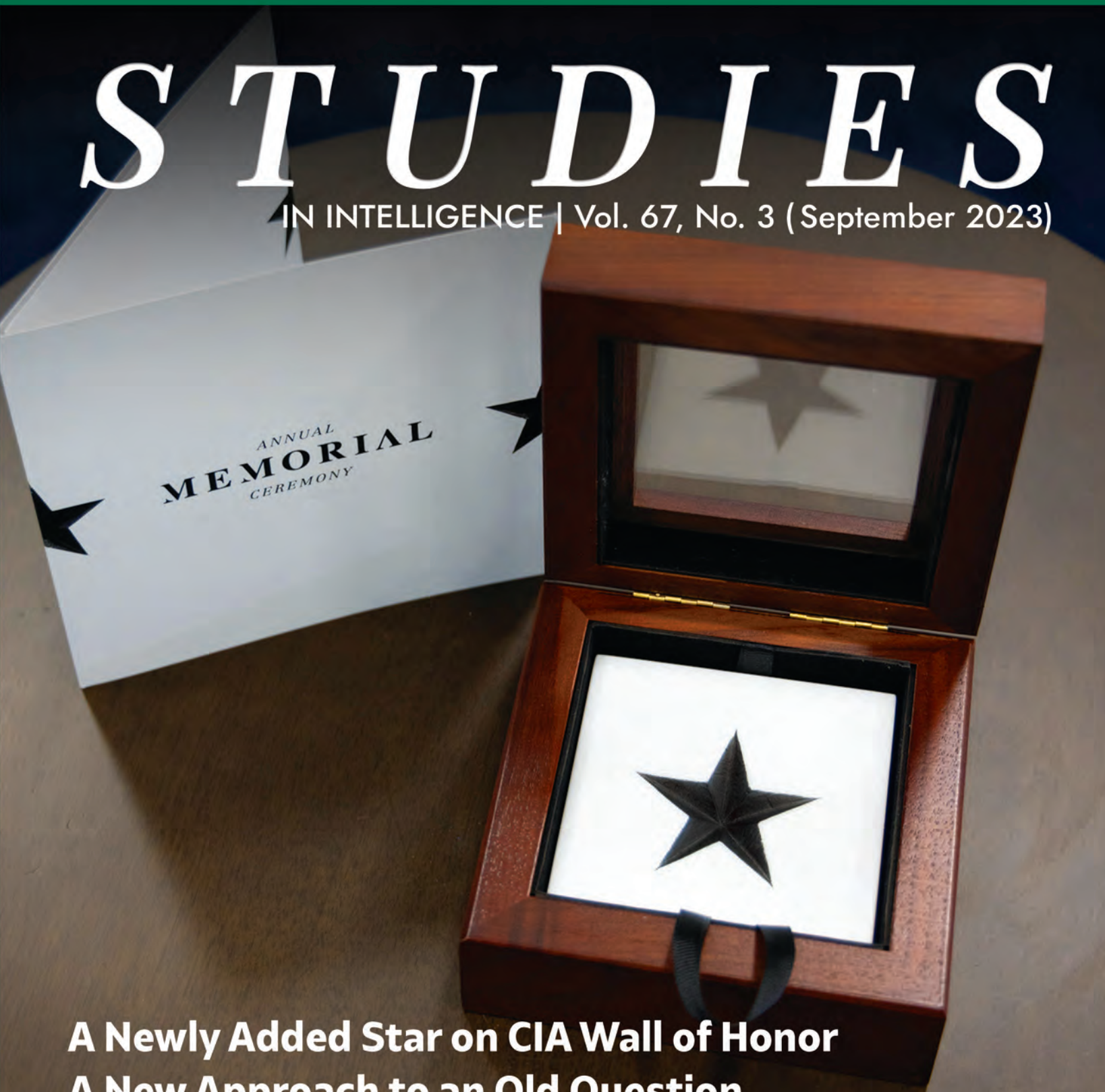
STUDIES

IN INTELLIGENCE | Vol. 67, No. 3 (September 2023)



A Newly Added Star on CIA Wall of Honor
A New Approach to an Old Question
An Idea for Transforming Intelligence Production

New from NIU
Intelligence in Public Media

Requests for subscriptions should be sent to:

Center for the Study of Intelligence
Central Intelligence Agency
Washington, DC 20505

ISSN 1527-0874

Owing to a redesign of cia.gov that was introduced in January 2021, URLs for *Studies in Intelligence* and other unclassified CSI products can now be found in the following locations:

For the homepage of the Center for the Study of Intelligence, go to:
https://www.cia.gov/resources/csi/

Unclassified and declassified *Studies* articles from the journal's inception in 1955 can be found in three locations.

- Articles from 1992 to the present can be found at
  https://www.cia.gov/resources/csi/studies-in-intelligence/
- Articles from 1955 through 2004 can be found at
  https://www.cia.gov/resources/csi/studies-in-intelligence/archives/
- More than 200 articles released as a result of a FOIA request in 2014 can be found at "Declassified Articles from Studies in Intelligence: The IC?s Journal for the Intelligence Professional" | CIA FOIA (foia.cia.gov)
  https://www.cia.gov/readingroom/collection/declassified-articles-studies-intelligence-ic%E2%80%99s-journal-intelligence-professional

Cover image: Star memorializng the life and death of Dr. Jon Evans being placed on CIA's Memorial Wall. CIA photo.

Mission

The mission of *Studies in Intelligence* is to stimulate within the Intelligence Community the constructive discussion of important issues of the day, to expand knowledge of lessons learned from past experiences, to increase understanding of the history of the profession, and to provide readers with considered reviews of public media concerning intelligence.

The journal is administered by the Center for the Study of Intelligence, which includes the CIA's History Staff, Lessons Learned and Emerging Trends Programs, and the CIA Museum.

Contact

Studies in Intelligence welcomes articles, book reviews, and other communications. Hardcopy material or data discs (preferably in .doc or .rtf formats) may be mailed to:

Editor
Studies in Intelligence
Center for the Study of Intelligence
Central Intelligence Agency
Washington, DC 20505

Awards

Unless otherwise announced from year to year, articles on any subject within the range of *Studies*' purview, as defined in its masthead, will be considered for monetary awards. They will be judged primarily on substantive originality and soundness, secondarily on literary qualities. Members of the Studies Editorial Board are excluded from the competition.

The Sherman Kent Award of $3,500 is offered annually for the most significant contribution to the literature of intelligence submitted for publication in *Studies*. The prize may be divided if two or more articles are judged to be of equal merit, or it may be withheld if no article is deemed sufficiently outstanding.

Another monetary award is given in the name of Walter L. Pforzheimer to the graduate or undergraduate student who has written the best article on an intelligence-related subject.

CENTER for the STUDY of INTELLIGENCE

Washington, DC 20505

Studies in Intelligence

Vol. 67, No. 3 (Extracts, September 2023)

Contents

(Continued on following page.)

Intelligence in Public Media (cont.)

❖ ❖ ❖

Contributors

Article Contributors

Dr. Andrew Macpherson is an assistant professor of security studies at the University of New Hampshire and the program coordinator for the UNH master's degree in National Security Intelligence Analysis and the principal investigator for the Northeast Intelligence Community Centers for Academic Excellence, a long-term partnership with the Office of the Director of National Intelligence.
Dr. Glenn Hastedt is a professor emeritus of the Justice Studies Department at James Madison University, where he served as the chair. Dr. Hastedt supports the Northeast Intelligence Community Centers for Academic Excellence.
Tracy Rich was a CIA historian when she researched and wrote the story of Dr. Jon Evans. She has since retired.
Dr. William Schlickenmaier is a senior strategist and member of CIA's Senior Analytic Service.
Dr. Adrian Wolfberg is a member of the staff of the National Academies of Sciences, Engineering, and Medicine.

Reviewers

Graham Alexander is the pen name of a CIA operations officer.
Michael J. Ard is a former CIA officer and a professor at Johns Hopkins University, where he directs the master's of science in intelligence analysis program.
John Ehrman is a retired CIA analyst.*
Joseph W. Gartin is managing editor of *Studies*.
Darryl Lansey is a retired CIA officer and author of the memoir, *A Thin Line Between Love and Hate: A Black Man's Journey Through Life and the CIA*.
Yong Suk Lee is a former deputy associate director of CIA and a visiting fellow at the Hoover Institution, Stanford University.
Alissa M. is a CIA analyst focusing on Middle Eastern governance issues.
Radhika M. is a CIA analyst focused on health security.*
Hayden Peake served in CIA's Directorates of Operations and Science and Technology. He has contributed to the Intelligence Officer's Bookshelf since 2002.
Mike R. is a member of CIA's History Staff.
David Welker is a member of CIA's History Staff.*

* Reviews included in Intelligence Officers Bookshelf.

❖ ❖ ❖

Dr. Jon Evans, 22 Charlie, and CIA Operations in Laos

Tracy E. Rich

Left: The Air America flight line at Udon Thani. Below: A CASI Beech Baron like the one Dr. and Mrs. Evans boarded on January 5, 1969.

An Ill-fated Flight

On the evening of January 5, 1969, Dr. Jon Evans stood on the Air America operations flightline at the sprawling Royal Thai Air Force Base at Udon Thani[a] awaiting the arrival of the CIA pouch run to Vientiane. At his side in the gathering dark was his wife of 25 years, Dorathea. A registered nurse, she worked part-time in the Bangkok medical unit where he was a regional medical officer (RMO). The couple had traveled to Udon Thani from Bangkok on the "50 Kip," a shuttle flight that got its nickname from the Thai currency and the 50K at the end of its tail number. With the first leg of the journey behind them, they would board a second plane for the short hop across the Mekong River to the Laotian capital.

Evans had retired from the US Army Medical Corps several years earlier, but he had not been ready to settle down. He had tried civilian life two decades before, when he left the military after World War II, volunteering to serve a community that had been without a physician for four years. Disenchanted with the routine of private practice, however, he was soon back in uniform.

Evans and Dorathea enjoyed the Army's challenging assignments and overseas experiences, including a stint at the US Army Hospital in Tehran in the mid-1950s and as senior medical adviser to the Korean army. The two of them, he said, had "a ball." During the early 1960s, Evans was back in Iran, serving as senior medical adviser to the shah and the Iranian army and command surgeon for the US Army Mission. By

a. Udon Thani was generally referred to as Udorn during this period.

1967, however, with little chance of reaching flag rank and every prospect of being stuck stateside in hospital administration, Colonel Evans was ready for something new and different. Besides, his two daughters were now married, and he and his wife had more freedom to take on interesting assignments.

Evans's decision to leave the Army after 23 years and sign on with CIA in May 1967 may also have been influenced by his longstanding ties to the world of intelligence. According to an unconfirmed report, Evans had spent some of World War II with the Office of Strategic Services, and his subsequent military career included both a tour as military attaché in India and an assignment in what is now the National Military Intelligence Center. In 1948, Evans had been detailed to the newly created CIA, where he met Dr. John Tietjen, CIA's Chief of Medical Services. During his 18 months with CIA, he served as an operational support officer, a post in which he helped organize first-aid courses and develop medical kits for use in the field.

After his return to the Army, he continued to work closely with CIA; during his tour of duty in Tehran, for example, he treated agents in Tehran, and in New Delhi he expedited the flow of information from the attache's office to the agency. Now, once more on the CIA payroll, he waited patiently at Udon Thani in the night chill.

The flight that would take Dr. and Mrs. Evans to Vientiane was operated by Continental Air Services, Incorporated (CASI), a subsidiary of Continental Airlines that provided contract flying services to CIA and others in Southeast Asia. Unlike the better known Air America, CASI was purely commercial and available to CIA through contract with the US Agency for International Development (USAID). The airline owned a variety of small and medium transport planes, including the Beechcraft Baron, a twin-engine piston-driven aircraft that was a workhorse in the fleet and was highly regarded by the airline's pilots for its dependability. CASI's missions, transporting men and supplies as part of the agency's support to the Indochina war, were sometimes overt and sometimes covert—a practice that could complicate normally routine business practices in an emergency.[a]

It was well known in aviation circles in Indochina that contract flying in Laos was not for the rule-bound or faint of heart. CASI pilots had to be skilled at dealing with mountainous terrain, short takeoffs and landings mandated by jungle airstrips, and even an occasional water buffalo on the runway. Anthony "Tony" Bertucci was one of the airline's veteran fliers. His partner on the flight, Richard

Jon Price Evans, M.D.

A career military physician, Jon Price Evans was commander of the hospital at Fort Carson, Colorado, when he retired from the Army in 1967. Before assuming that post, he had commanded the hospital at Patrick Air Force Base in Florida and served at McDonald Hospital in Fort Eustis, Virginia. He had also served at the headquarters of Gen. Matthew Ridgway, in the office of the Surgeon General, and at the Army's Kennedy General Hospital in Memphis, Tennessee. Evans signed a contract to work for CIA after leaving the Army and was almost immediately sent to Bangkok as a regional medical officer.

Evans, the only child of a well-to-do florist, was born on December 14, 1914 in Wilkes-Barre, Pennsylvania. According to his daughter, he changed his given name from John to Jon when he went into the military because a cousin also named John Price Evans enlisted at the same time. After attending Wyoming Seminary (a coeducational boarding school), he obtained a degree from Washington and Lee University and a medical degree from Temple University. He specialized in obstetrics and gynecology. Evans joined the Army in 1943 while doing his residency at Wilkes-Barre General Hospital. He later obtained a degree in public health from the Walter Reed Institute of Research. In addition, he was a graduate of the US Army's Command and General Staff and Armed Forces Staff Colleges.

Evans enjoyed sports and was on the wrestling team during high school and college. In addition, he held several elective offices. He was also a keen photographer who processed his own black-and-white film. A "tinkerer," he bragged that he could fix almost any common household item. At his wedding to Dorathea Ruth Thomas on October 21, 1943, he cut the wedding cake with a Civil War–era sword from his family's collection. The Evanses had two daughters, Jean and Jone. At the time of his death, Evans had three grandchildren.

a. See Timothy Castle, "At War in the Shadow of Vietnam: United States Military Aid to the Royal Lao Government, 1955–75. PhD dissertation approved for public release by AFIT/CI, Wright-Patterson AFB and provided to DTIC, December 17, 1991.

Arlie Harter, had come to CASI from Air America but had far less seniority. Harter was bucking for a promotion to the captain's seat—and this pouch run was supposed to help him seal the deal.

As the Evanses stood on the tarmac at Udon Thani, opposition to the Vietnam War was soaring back home, and the US role in ostensibly neutral Laos was becoming controversial in Washington. Although it would be almost a year before Senator Stuart Symington would launch Congressional hearings into US involvement in East Asia, the media had been speculating about possible US paramilitary activity in Laos. Such involvement would be in direct contravention of the Geneva Agreements of 1962, and public verification that it existed would pose problems for a sitting administration.

Laos was nevertheless regarded by US policymakers as central to containing the spread of communism in East Asia, and Washington had been providing economic and military aid to the kingdom since 1950. In March 1961, Kennedy issued the orders that created a program of extensive CIA paramilitary operations supported by Thai-based covert US military agencies—a program that escalated after the Geneva Agreements forced the withdrawal of overt US military components. The neighboring kingdom of Thailand, equally determined not to let Laos fall to the communists, became Washington's "unsinkable aircraft carrier" in the region.

By 1969, when Jon and Dorathea Evans were on the flightline awaiting the arrival of 22 Charlie, the airbase at Udon Thani was a beehive of activity, playing host to dozens of US Air Force fighter jets and to a fleet of fixed and rotary wing aircraft operated by CIA proprietary Air America. Despite this presence in Thailand, CIA had so far been able to conceal the full extent of US assistance to anti-communist authorities in Laos. US officials in Washington, Bangkok, and Vientiane knew, however, that they were walking a very fine line.[a]

The flight from Udon Thani to Vientiane should have taken 15 minutes. It crashed near Nong Khai, just short of the Mekong River and the Laos.

The CASI Beechcraft Baron designated 22 Charlie had left Vientiane early on January 5 en route for Luang Prabang, the Lao royal capital; Long Tieng, the headquarters of General Vang Pao and his CIA-backed guerrilla army; and Nam Yu, the isolated highland village from which the legendary Anthony "Tony Poe" Poshepny mobilized the hill tribes in support of the agency's secret war. Udon Thani was its last stop before the return to Vientiane.

Bertucci was in the captain's seat when the pouch run left Vientiane. Harter took over at the halfway point. He would be in command of the aircraft as it completed its well-worn route. There was no pouch to collect in Udon Thani, and at about six o'clock, once Dr. and Mrs. Evans

a. See Bill Lair memoir, "An Excellent Idea": Leading Surrogate Warfare in Southeast Asia, A Personal Memoir," www.cia.gov

were aboard, the plane taxied down the runway to join the queue awaiting clearance for takeoff. Apparently because the flight was a fixture in Udon Thani's daily routine, Harter did not announce their departure to the military air controllers or the nearby Brigham GCI (ground control intercept) station.

The flight to Vientiane usually took about 15 minutes. It was not a big deal for Evans, who had already earned praise for his willingness to travel on short notice. Just weeks before this trip, Evans had been awarded the Legion of Merit by the ambassador to Thailand for "exceptionally meritorious conduct in the performance of outstanding services." Since late 1968, he had paid regular visits to Vientiane as medical adviser to the chief of station. At the time of his current trip, that COS was Larry Devlin, who had replaced Saigon-bound Ted Shackley several months earlier. On arrival, Evans would presumably be whisked from the airport to learn more about the operational requirement that had led the station to summon him this time.

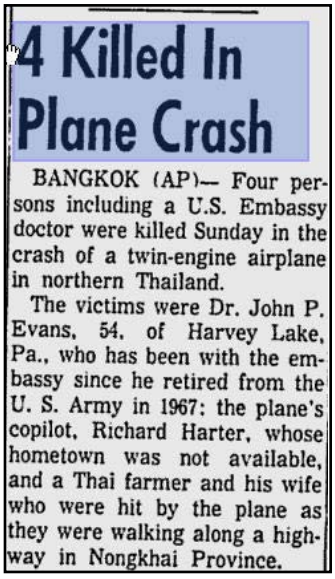
At 051356Z, the CIA Station in Vientiane sent a flash cable to Bangkok. It was almost midnight, and Baron 22 Charlie was overdue. The delay in realizing the plane was missing was attributable in part to the lack of notification to the tower and ground intercept station in Udon Thani. The pilots had also failed to make an emergency radio call, an act that should have been standard operating procedure.

Eventually, wreckage was spotted 8 miles south of Vientiane along the narrow road that paralleled the Laotian-Thai border. Given the location, the debris could belong to 22 Charlie. The station dispatched two helicopters and its senior air officer, Charlie Gabeler, to investigate. Doctors aboard the choppers, including the Vientiane Embassy physician, would determine if that was the case—and if there were any survivors.

Within a few hours, another cable was flashed from Vientiane to Bangkok. Two Americans had been brought to the hospital in Nong Khai, then a sleepy provincial town on the Thai side of the Mekong. The first, a woman, was reported to be in critical condition. The second, a man, was less seriously injured and was conscious. The two had been aboard 22 Charlie. The embassy physician headed from the crash site to the hospital as a medevac was put on standby.

As the investigation of the wreckage continued, a Thai doctor on the scene radioed Vientiane with news of a grim discovery. Two bodies had been found in the plane. The crash had also killed a Thai couple on the ground. The remains from the plane were put on board a Jolly Green Giant helicopter for evacuation and identification. The chopper bearing the two bodies headed to Udon Thani, leaving several CIA officers behind. They would remain at the crash site until dawn, when they could determine if Evans had been carrying any classified documents in his personal belongings and if there were other security concerns.

While the officers waited in the dark by the wreckage, another station officer radioed Vientiane from Nong Khai, alerting the station that Mrs. Evans, though still in shock, had



4 Killed In Plane Crash

BANGKOK (AP)— Four persons including a U.S. Embassy doctor were killed Sunday in the crash of a twin-engine airplane in northern Thailand.

The victims were Dr. John P. Evans, 54, of Harvey Lake, Pa., who has been with the embassy since he retired from the U. S. Army in 1967; the plane's copilot, Richard Harter, whose hometown was not available, and a Thai farmer and his wife who were hit by the plane as they were walking along a highway in Nongkhai Province.

been stabilized and was being flown to the base hospital at Udon Thani. Vientiane informed COS Bangkok, who requested that agency officials in Udon Thani ensure that friends of the Evanses get to the hospital as soon as possible to comfort her.

22 Charlie had been airborne for seven minutes. Harter would never get his promotion, and Dr. Evans would never complete his mission in Vientiane.

Aftermath

Three hours after Bertucci, Harter, and Dr. and Mrs. Evans had taken off for the quick flight to Vientiane, CIA officers in Washington, Bangkok, Vientiane, and Udon Thani had mobilized and were working to determine what had occurred and how best to deal with it. At CIA Headquarters, Air Branch officers were trying to understand the cause of the accident. DCI Richard Helms was informed that an agency officer from Vientiane had positively identified Dr. Evans as one of those who died in the wreckage of 22 Charlie. As agency officials looked after Mrs. Evans, arrangements were

being made to transport her husband's remains back to the United States, and a memorial service was scheduled for January 16 at the International Church in Bangkok. CASI officials assumed responsibility for Bertucci's treatment and Harter's burial.

In Vientiane, Amb.William Sullivan, who controlled the entire US program of covert aid to Laos, was contemplating the broader political implications of the downed aircraft. There would be an accident investigation and, inevitably, press coverage. How would US officials explain the presence of officers from Embassy Vientiane at the crash site in Thailand? What would the media say if and when they found out that the plane was flying from Udon Thani to Vientiane? How would they explain Dr. Evans's travel from Bangkok to the Laotian capital? In short, how could all concerned keep the incident from fueling press speculation about US engagement in Laos?

In Bangkok, station officers greeted with skepticism Ambassador Sullivan's suggestions for heading off a public controversy. They pointed out that it was well known that CASI did not operate Beechcraft Barons in Thailand. They also argued that denying that Vientiane was the ultimate destination of 22 Charlie could create more problems than it solved. If it turned out the destination was widely known—a reasonable prospect given the regularity of the pouch run—the crash of 22 Charlie would be surrounded by an air of mystery and would thus attract more attention. Bangkok suggested that officials neither confirm nor deny that the plane was headed for Vientiane. Embassy press officers were advised to keep the announcement of the crash short and factual.

Back in Washington, CIA officials were also reluctant to go along with the ambassador. They pointed out that, when Thai and US aviation authorities investigated what happened to 22 Charlie, they would inevitably discover the true destination of the flight. Indeed, they saw no alternative but to record the truth on the requisite forms and notifications. At the same time, they reminded agency officers in Vientiane, Bankgkok, and Udon Thani that all aircraft crashes were sensitive—and that this crash was more sensitive than most. As a result, even in notifying the Evanses' next of kin, they had confined the details released to time, location, type of aircraft, and identification of casualties. Coverage in major newspapers was minimal.

As State and agency officials debated the best way to minimize the political fallout and preserve deniability of CIA operations, routine administrative issues assumed a much greater importance. CASI needed information on Dr. and Mrs. Evans to submit its insurance claim, but there was disagreement about who should submit the information in order to maintain cover. There was similar disagreement over the filing of employee compensation forms. With one of Evans's sons-in-law brandishing the prospect of a lawsuit against CASI, these details had to be addressed quickly—but carefully. They might wind up in court. CIA's Office of General Counsel was brought into the picture, but it would be months before all of the insurance, pension, and other financial details were settled

Meanwhile, in Vientiane, a medical officer was still needed to carry out the duties that had put Evans in the seat in 22 Charlie, and a request was sent to Saigon for assistance. A medical officer was duly assigned some months later.

Interment and Memorial

Jon Price Evans was buried in Arlington National Cemetery near the Memorial Chapel Gate on February 6th. Dorathea, who died 30 years after the plane crash, is buried with him.

Dr. Evans's death would not be reflected on CIA's Memorial Wall until May 23, 2023, when during CIA's annual Memorial Day function, CIA Director Burns made public the names of five previous inductees to the Hall of Honor and introduced one new one, Dr. Jon Evans. Director Burns opened the dedication of the new star by saying,

> *Today, we dedicate the 140th Memorial Star to Dr. Jon Evans. This new star commemorates a life that was lost decades ago—but the passage of time neither lessens his sacrifice nor diminishes the debt we owe him and his family....*
>
> *We are joined by one of his daughters and 13 members of Dr. Evans's extended family, including grandchildren and great-grandchildren. On behalf of everyone at CIA, thank you for being here. We are immensely proud to count Jon as a member of our Agency family, and we will always be grateful for his heroic service to our country.*

Before the dedication ceremony, the family of Dr. Evans received briefings that detailed Dr. Evans's and his wife Dorothea's service. Participants in the meeting at a follow-on luncheon said the family genuinely appreciated the discussions because it filled in so many gaps in their understanding of why Jon and Dorothea were traveling to Laos. The family members noted that even in the later years, Dorothea never disclosed to them what the mission was in Laos, and even what they were doing in Bangkok. Dorothea kept her commitment to secrecy of our mission even with her own family despite the tragedy and passing of time. His daughter would tell another guest at the ceremony that "her father had been her hero, and he is even more of a hero now."

Afterword

Since the Memorial Wall was installed with 31 stars in 1974 many have been added. By 2008, when former CIA historian Nicholas Dujmovic reviewed the wall's history in *Studies in Intelligence* Vol. 52, No. 3 (September 2008), there were 89 stars. Perhaps it was inevitable, given when the Memorial Wall was first engraved, that sacrifices in the line of duty which predated its creation would be lost in past history and will for a time go unnoticed, as Dujmovic pointed out in his article. In Dr. Evans' case, his story was raised in this manuscript, which only recently led to the reconsideration of the circumstances of his death and the decision to commemorate his death on the Memorial Wall.

A note on sources:

This article is based on staff cables, personnel records, newspaper accounts, and interviews with and recollections of CIA and CASI personnel familiar with the setting and events. For a broad, unclassified examination of the US government's secret war in Laos, see *At War in the Shadow of Vietnam*, by Dr. Timothy Castle (Columbia University Press, 1993). For an in-depth, assessment of CIA operations in Laos, see *Undercover Armies: CIA and Surrogate Warfare in Laos* by Thomas Ahern, Jr. (Center for the Study of Intelligence, 2006). Originally published as a classified history, CIA declassified most of the book and posted it to its Freedom of Information Act Electronic Reading Room on CIA.GOV.

❖ ❖ ❖

The author: Tracy E. Rich was a member of CIA's History Staff when this article was originally written in 2016. She has since retired.

A New Quantitative Approach to an Old Question

Andrew Macpherson and Glenn Hastedt

We offer an alternative, quantitative analysis of intelligence definitions and intelligence organizations worldwide to advance the debate over the correct definition of intelligence.

In numerous books, manuscripts, and journal articles (including recently in these pages), IC practitioners have offered their definitions of "intelligence" and why the definition is important to practitioners. These works—including Kent (1949), Bimfort (1958), Random (1958), Lowenthal (1999), Warner (2002), and Simms (2022)—are must-reads for intelligence-studies scholars and represent a venerable who's who in the discipline. Spanning some seven decades of scholarship, the volumes provide qualitative assessments of what intelligence is and is not. (The above, later cited works, and additional readings are listed in full bibliographic detail beginning at "References" on page 13.)

In this article, we offer an alternative, quantitative analysis of intelligence definitions and intelligence organizations worldwide to advance the debate over the correct definition of intelligence, which we hold to be:

> *National security intelligence is a secret state activity to understand, influence, or defend against a threat to gain an advantage.*

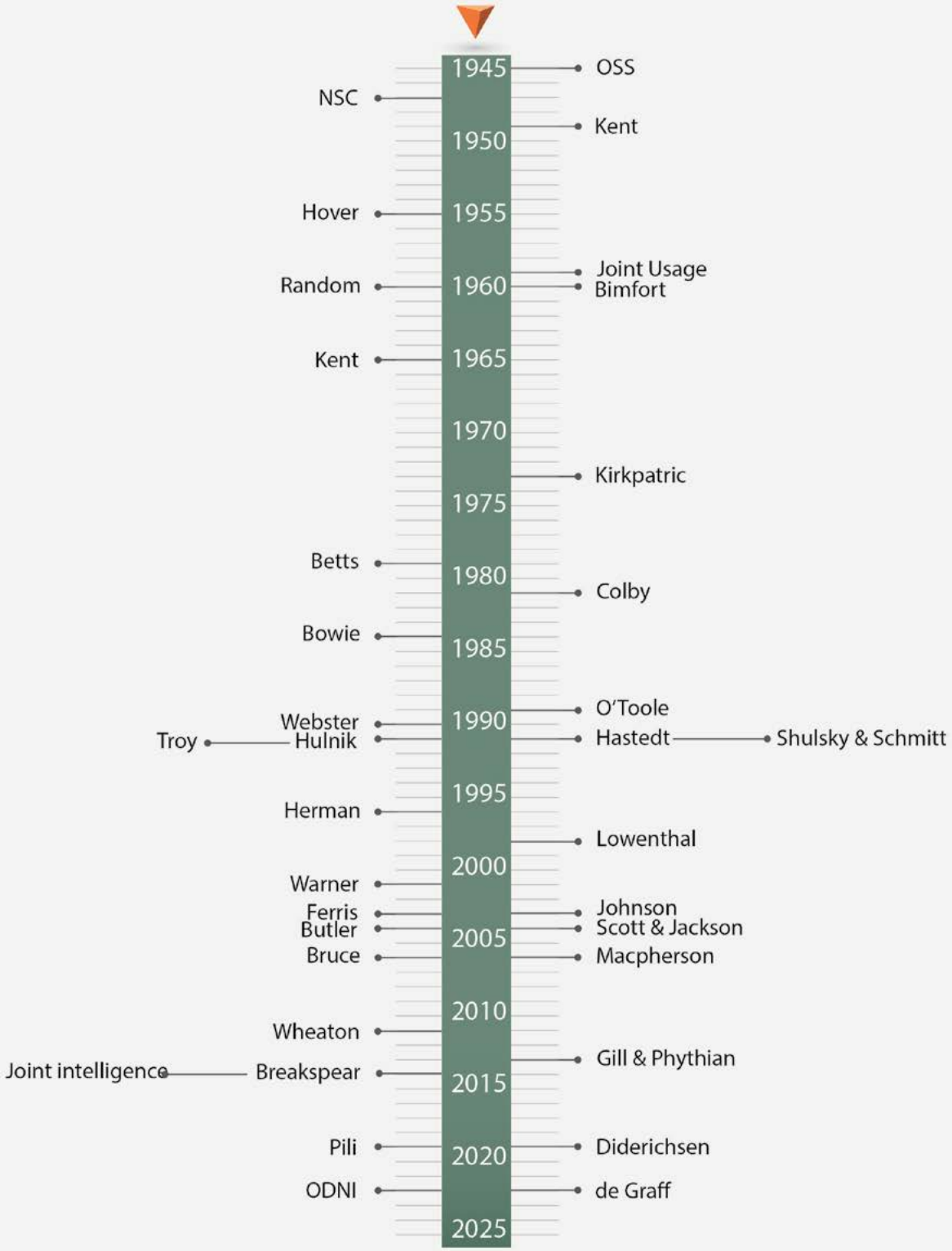
As we will demonstrate, this definition iterates upon existing definitions and includes all of the key elements required for practitioners and scholars alike. Practitioners may use the definition to describe their work. Academics may use the definition to identify intelligence as a phenomenon, develop theories, and test causal relationships.

Why Develop Definitions?

The scientific method was developed to challenge traditional notions of the absolute truth of knowledge. Individuals employing the scientific method seek to develop relevant and accurate statements that serve to explain an observed phenomenon or examine the validity of observed causal relationships of interest. Adherents to the scientific method believe that absolute truth can never be found. Instead, claims that are supported by the strongest current evidence are accepted but may always be rejected if new evidence proves them to be false.

Social scientists using the scientific method develop operationalized definitions. Operationalization is a process for assigning rules so a defined phenomenon or object may be measured or a hypothesis of causal relationships tested. Operationalized definitions facilitate measurement and objectivity, because a discrete observer should be able to make the same observation or measurement under similar conditions. Beyond technical definitions used for specific scientific activities, broader definitions may be used to generally

Figure 1. National Security Intelligence, 1945–2023



classify phenomena or the objects of study. Intelligence is a phenomenon that can be defined. Researchers can develop measurable variables for intelligence. For example, by counting the intelligence organizations countries operate, researchers can develop descriptive statistics and determine if there are patterns. In some cases, identifiable patterns may be predicted using statistical methodologies.

The 1948 National Security Council Intelligence Directive No. 3 states, "National Intelligence is integrated departmental intelligence that covers the broad aspects of national policy and national security." This tautology is an example of applying Supreme Court Justice Potter Stewart's "I know it when I see it" standard.[a] Many definitions of intelligence have been proposed, lamented, and debated both inside and outside the IC.

Existing Definitions

In 1955, Sherman Kent called for a comprehensive intelligence literature that included rigorous definitions. Over the intervening years, many practitioners and scholars have responded. Wesley Wark (1994, 4) called efforts to define intelligence a "separate project" among scholarly work in the domain. A RAND practitioner/academic workshop titled "Toward a Theory of Intelligence" found no consensus on a definition (Treverton et al., 2006, 20). A survey of academics and practitioners published in the journal *Intelligence and National Security* notes that defining intelligence is one of the principal scholarly debates advancing knowledge in the domain (Johnson and Shelton, 2013, 110).

As a boundary condition, we stipulate that the type of intelligence we are investigating is focused on national security and practiced by national governments.

These findings are not due to a lack of definitions. We identified 36 definitions of intelligence in practitioner, scholarly, and legal works from 1945 through 2023 (figure 1, opposite). We plot a different course in this narrative, providing a quantitative analysis to highlight the critical elements that must be included in a definition of intelligence.

The Boundaries of this Study

As a boundary condition, we stipulate that the type of intelligence we are investigating is focused on national security and practiced by national governments. If we were developing a typology of intelligence practiced by heterogeneous organizations, we would use examples of real-world activity to develop categories. For example, private-sector organizations such as oil companies collect and analyze information that helps their decisionmakers limit risk. Law enforcement agencies collect criminal intelligence to facilitate their investigations or proactively interdict illicit activity. Terrorist entities conduct intelligence activities to plan their violent actions.

Although these are all categories worthy of study, we leave them to other scholars. The units of analysis we are interested in are the government agencies practicing intelligence. We specifically exclude intelligence oversight organizations from our focus, as these entities generally focus on accountability or compliance.

Term-Document Matrix

We used a text-mining framework to compile the definitions for analysis and to create a term-document matrix (TDM). A TDM is a mathematical representation of a corpus of text, in which rows represent unique terms in the vocabulary and columns represent documents in the corpus. The matrix contains a count or frequency of each term's occurrence in each document. Each cell in the matrix corresponds to a specific term and document combination, and its value indicates the number of times that the term appears in that document.

The compiled definitions contained a total of 608 words, of which 345 were unique. The TDM sparsity was 96 percent, meaning that most of the terms in the vocabulary do not appear in most of the definitions in the corpus. As seen in the word cloud (figure 2), the words "information," "policy," and "foreign" are prominent, proportional to their count in the corpus.

What can we glean from this analysis? The definitions that exist likely meet their authors' requirements; however, the lack of common keywords represents the lacuna of operationalized definitions with specific measurable components.

We can sample the definitions to test this hypothesis. The definition with the fewest words is Troy's (1991) adoption of Constantine Fitzgibbon's assertion that intelligence is "knowledge of the enemy." While Troy vigorously defends his assertion that this is the "correct"

a. See Paul Gewirtz, "On 'I Know It When I See It,'" *Yale Law Journal* 105, no. 4: 1023–47 (1996).

Figure 2. A word cloud derived from a term-document matrix of 36 English-language definitions of intelligence shows the higher frequency of terms like "information," "foreign," and "policy" and the relative sparsity of terms like "evaluation" and "integration."

definition of "intelligence," it is so broad that it limits our ability to focus on what should and should not be considered intelligence. Wilhem Agrell noted as much in his speech at the Sherman Kent Center of Intelligence Analysis when he asserted that "when everything is intelligence—nothing is intelligence." (Agrell, 2002)

Not all knowledge of the enemy is intelligence. Diplomats are dispatched to overtly monitor foreign events and communicate adversarial governments' intentions back to their leaders. Intelligence operatives are sent to covertly gather information; their true intentions are secret. National leaders employ intelligence organizations so they can secretly gather information to gain an advantage. Shulsky and Schmitt (1991) and Warner (2002) also stress that secrecy is an essential component of any definition of intelligence. The term secrecy appeared in eight of the 36 (22.2 percent) definitions we collected.

Collection

Three other terms featured prominently in the frequency table of terms across definitions: "collection" (36.1 percent), "analysis" (16.6 percent), and "covert action" (11.1 percent). Shulsky and Schmitt (1991) call these activities the elements of intelligence. They are found in intelligence studies textbooks including Lowenthal's work, *Intelligence: From Secrets to Policy* (1999). Information gathered via espionage or human intelligence (HUMINT) is an essential approach to collecting data on enemy intent and capabilities. Collection of technical data (TECHINT) broadly includes intercepted signals and communications (radio, electronic, and telemetry), photographs and images, measurements and signatures, and public or open sources (OSINT) that may be observed or requested (Shulsky and Schmitt 1991, 11). HUMINT, TECHINT, and OSINT may collectively be categorized as intelligence collection.

Analysis

Analysis may be defined as "the process of transforming bits and pieces of information that are collected in whatever fashion into something that is useable" (Shulsky and Schmitt 1991, 41). Political, military, economic, and other analysis form the basis from which leaders may take action to gain an advantage over their international adversaries. We categorize collection and analysis as activities undertaken to understand a threat.

Covert Action

Random's (1958) definition of intelligence stresses that an essential element of intelligence is "the conduct of covert activities abroad to facilitate the implementation of foreign policy." For example, the National Intelligence Council in March 2021 assessed that "Russian President Putin authorized, and a range of government organizations conducted, influence operations aimed at denigrating President Biden's candidacy and the Democratic Party, supporting former President Trump, undermining public confidence in the electoral process, and exacerbating sociopolitical divisions in the US."

In the United States, the Title 50 definition of covert action is activities of a government to "influence political, economic, or military conditions abroad," with the intent that the government's role "will not be apparent or acknowledged publicly" (DeVine 2022). The Russian activities are clearly congruent with this definition. We believe an operationalized definition of intelligence should include

covert actions conducted to influence threats.

National leaders see foreign intelligence activities as threats, and thus they expend resources to develop counterintelligence capabilities. Counterintelligence may be broadly defined as "information collected and analyzed, and activities undertaken, to protect a nation (including its own intelligence-related activities) against the actions of hostile intelligence services." (Shulsky and Schmitt 1991, 99) The term "counterintelligence" was found in three of the 36 (8.3 percent) intelligence definitions. We searched for synonyms such as "defend" or "protect" without success. The terms "safeguarding," "subversion," and "unauthorized" each occurred in one (2.7 percent) of the definitions. Counterintelligence is also undertaken to limit the risks from inadvertent or intentional breaches in security, such as the leaking of information. We argue that counterintelligence must be included in an operationalized definition of intelligence.

Instrument of Foreign Policy

The three most prevalent terms in the definitions— "information" in 26 of 36 (72.2 percent), "policy" in 15 of 36 (41.7 percent), and "foreign" in 14 of 36 (38.9 percent)—indicate that the authors of the definitions see intelligence as a foreign policy tool. Johnson's definition of intelligence, the longest in the corpus, is representative of the key elements found in the corpus of definitions from 1945 to 2023. He argues that intelligence is

> *a set of activities conducted by government agencies that operate largely in secret. These activities include, foremost, the collection and interpretation of information drawn from a mixture of open and clandestine sources to arrive at a product—knowledge—useful to illuminate foreign policy deliberations.… They also engage in covert action to advance a nation's international interests by seeking clandestinely to manipulate events and conditions abroad.… These agencies have a mandate to conduct counterintelligence operations designed to protect a nation's citizens and secrets against attacks from hostile intelligence services and other threats* (Johnson 2003, 1).

Yet Johnson's definition, like many of the definitions in the corpus, has a substantive deficiency that must be addressed.

The definitions in this corpus come from Western authors who may be guilty of mirror imaging. For example, readers would be forgiven for thinking that intelligence is exclusively used as a tool for foreign policy after reading the definitions we analyzed. This may be true for many democratically governed countries, but what about more authoritarian states? In his contribution to the 1988 book *Comparing Foreign Intelligence*, John Dziak notes that in many states, "the security service and foreign intelligence tend to be the same organ of the state." (66) As Christopher Andrew and Vasili Mitrokhin (2001, 561) note in their book *The Sword and the Shield*, the KGB was essential to the conduct of Soviet foreign policy as well as to the running of the one-party state.

Brassey's International Intelligence Yearbook profiles the intelligence organizations in 50 countries, many of which focus on both foreign and domestic threats (Henderson, 2003). After examining even a cursory sample of state intelligence activities, we can clearly see that a general definition of "national security intelligence" should not be limited to a focus on foreign entities or policy; many governments use intelligence as tools of power over their own citizens.

After examining even a cursory sample of state intelligence activities, we can clearly see that a general definition of "national security intelligence" should not be limited to a focus on foreign entities or policy; many governments use intelligence as tools of power over their own citizens.

Quantifying Intelligence Agencies

Over the past five years, we have worked with students to collect data for the National Security Intelligence Dataset (NSID). The NSID contains information on 416 intelligence agencies in 113 United Nations member states and Taiwan. These countries represent 58 percent of the UN's total membership and 89 percent of the world's population. Agencies in the NSID are official state organizations whose function is to conduct national security intelligence activities. Government entities that provide oversight of intelligence organizations are not included. The NSID does not include the financial intelligence units of most countries; only FIUs that are specifically part of a country's intelligence services are included in the NSID.

	Count	Percent	N	SD
HUMINT	264	66.8	395	0.47
TECHINT	315	78.3	402	0.41
Analysis	360	89	405	0.31
Counterintelligence	290	73	397	0.44
Covert Action	58	4.7	394	0.35

Table 1. National Security Intelligence Dataset of 316 intelligence organizations shows the emphasis on collection, analysis, counterintelligence, and covert action. Agencies may have multiple functions, so these variables are not mutually exclusive.

Many of the organizations found in the NSID have a single function, national security intelligence. Other organizations included in the NSID have multiple roles. For example, interior ministries frequently have domestic security functions in addition to a national security intelligence role.

Using the NSID, we summarized the functions of each country's intelligence agencies. The average number of intelligence organizations found in states is 3.67, with a high of 18 and a low of 1. There were 234 civilian (56.3 percent) and 181 military (43.6 percent) intelligence agencies. Table 1 presents data on the types of activities that an intelligence agency performs. Agencies may have multiple functions, however, so the shown variables are not mutually exclusive.[a]

How do these data contrast with the definitions of "intelligence" that we analyzed? Recall that collection was in 36.1 percent of the definitions and analysis was in 16.6 percent. HUMINT and TECHINT are activities undertaken by the majority of intelligence organizations included in our study. Analysis, found in a minority of the definitions, is an activity in the vast majority (89 percent) of the intelligence entities in our study. Counterintelligence, found in only 8.3 percent of our definitions, is conducted by almost three-quarters (73 percent) of the organizations we identified that conduct government intelligence activities. Covert action was found in 11.1 percent of our definitions. We found that 4.7 percent of the intelligence organizations we identified conducted covert activity.

What are the countries doing with the intelligence they gather? We argue that national security intelligence is focused on both foreign and domestic adversaries. In the NSID, we developed a variable regarding the focus of the intelligence agency. We made judgments based on available open sources to answer the question: Did the agency primarily focus on foreign intelligence (including military intelligence) or on domestic intelligence used to give the government control over its population? We defined domestic intelligence as collection, analysis, and covert activity focused on a country's own citizens.

Of the 416 intelligence organizations we evaluated, 268 (64.6 percent) primarily focused on foreign intelligence, while 147 (35.4 percent) focused on domestic intelligence. Because over one-third of the intelligence agencies we surveyed for the NSID focused primary on domestic intelligence, a definition of "intelligence" must not be limited to a focus on foreign targets. These data indicate that the intelligence agencies of many countries target their own citizens, and any definition of "intelligence" must account for this reality.

There is one more critical issue that should be noted in current definitions of intelligence. Many definitions characterize the focus of intelligence as countries or other foreign adversaries (countries) or groups (nonstate actors). Yet, the National Intelligence Council's latest long-range forecast, *Global Trends 2040: A More Contested World*, (ODNI March 2021) lists environmental and emerging technology developments as structural forces setting and breaking boundaries in the future. The publicly released National Intelligence Estimate on challenges to US national security posed by climate change articulates the risk from a threat that is potentially greater than any single country (ODNI October 2021).

Anyone who has experimented with ChatGPT can immediately recognize the parallels with Gartin's (2019) *Studies* article, "The Future of Analysis," in which machines enhance human activity. These examples demonstrate that, in practice, national security intelligence activity is broader than an exclusive focus on other countries or human adversaries. Intelligence is gathered on forces that shape what other countries and human adversaries can accomplish.

a. Each category has slightly fewer observations than the total of 416 due to missing data.

Offering a New Definition

In proposing a definition of "intelligence" that may be broadly adopted, we build on existing work from Warner (2002). We propose the following modified definition: *National security intelligence is a secret state activity to understand, influence, or defend against a threat to gain an advantage*.

We propose the following definition: National security intelligence is a secret state activity to understand, influence, or defend against a threat to gain an advantage.

Our definition includes all of the key elements required for practitioners and scholars alike. Practitioners may use the definition to describe their work. Academics may use the definition to identify intelligence as a phenomenon, develop theories, and test causal relationships.

Defining intelligence in a uniform manner is a necessary first step to advancing the conversation on the study of intelligence. Potential next steps involve using the definition to deepen and broaden our understanding of intelligence. The methodologies used to study intelligence, notably the use of quantitative analysis, may allow us to drill down and explore relationships between variables. In concert, practitioners and scholars may expand the nature of the qualitative questions they ask concerning intelligence. Here, we identify two possible questions (and acknowledge many more exist).

First, how is intelligence used regarding public goods problems such as climate change, pandemics, and emerging technologies? Intelligence may provide policymakers with a decision advantage in addressing collective goods negotiations between countries, however, key aspects of intelligence may not be relevant to policy decisions on collective goods at all.

A second question centers on the ongoing investigation of the relationship between intelligence practitioners and policymakers. Literature exists on specific issues, such as the politicization of intelligence, yet perhaps a broader lens is needed to explore the underlying dynamics of the policymaker–intelligence dynamic. Are the literature and methods used to investigate civil–military relations relevant to develop a broader understanding of civil–intelligence relationships?

Although we believe our proposed definition of intelligence is authoritative, we look forward to a conversation with our readers. We have found what we consider a useful definition of intelligence; however, some readers of *Studies in Intelligence* are sure to find areas to constructively critique our work.

❖ ❖ ❖

The authors: Andrew Macpherson is an assistant professor of security studies at the University of New Hampshire. He is the program coordinator for the UNH master's degree in National Security Intelligence Analysis and the principal investigator for the Northeast Intelligence Community Centers for Academic Excellence, a long-term partnership with the Office of the Director of National Intelligence. Glenn Hastedt is a professor emeritus of the Justice Studies Department at James Madison University, where he served as the chair. His publications include *American Foreign Policy: Past, Present, and Future* and numerous articles on intelligence in *Intelligence and National Security* and the *International Journal of Intelligence and CounterIntelligence*. He is a former coeditor of the journal *White House Studies*. Dr. Hastedt supports the Northeast Intelligence Community Centers for Academic Excellence.

❖ ❖ ❖

References

Agrell, Wilhelm. 2002. "When Everything Is Intelligence—Nothing Is Intelligence." *Sherman Kent Center for Intelligence Analysis Occasional Papers* 1, no. 4.

Andrew, Christopher, and Mitrokhin, Vasili. 2001. *The Sword and the Shield: The Mitrokhin Archive and the Secret History of the KGB*. Basic Books.

Bimfort, Martin. 1958. "A Definition of Intelligence," *Studies in Intelligence* 2 (Fall).

Breakspear, Alan. 2013. "New Definition of Intelligence." *Intelligence and National Security* 28, no. 5: 678–93.

De Graaff, Bob. 2023. "Two Souls in One Body: The Acknowledgment of Intelligence as Influence Activity." *Journal of Security Intelligence, and Resilience Education* 16, no. 5 (Spring).

Department of State Office of the Historian. 1948. *National Security Council Intelligence Directive No. 3*. Accessed April 15, 2023. https://history.state.gov/historicaldocuments/frus1945-50Intel/d426.

DeVine, Michael E. 2022, updated November 29. *Covert Action and Clandestine Activities of the Intelligence Community: Selected Definitions.* Congressional Research Service.

Diaz, Milton 2011, "Forming a Definitional Framework for 'Intelligence'" *American Intelligence Journal* 29, no. 1:53–64.

Dziak, John. 1988. "The Study of Soviet Intelligence and Security Systems." In *Comparing Foreign Intelligence: The U.S., the USSR, the U.K., and the Third World*, ed. Roy Godson. Pergamon-Brassey's International Defense Publishers.

Gartin, Joseph. 2019. "The Future of Analysis." *Studies in Intelligence* 63, no. 2.

Gill, Peter, and Mark Phythian. 2016. "What Is Intelligence Studies?" *International Journal of Intelligence, Security, and Public Affairs* 18, no. 1: 5–19.

Hastedt, Glenn. 1991. *Controlling Intelligence*. F. Cass.

Henderson, Robert. 2003. *Brassey's International Intelligence Yearbook: 2003 Edition*. Brassey's.

Johnson, Loch. 2003. "Bricks and Mortar for a Theory of Intelligence." *Comparative Strategy* 22, no. 1: 1–28.

Johnson, Loch, and Shelton Allison. 2013. "Thoughts on the State of Intelligence Studies: A Survey Report." *Intelligence and National Security* 28, no. 1.

Kent, Sherman. 1955. "The Need for an Intelligence Literature." *Studies in Intelligence* 1, no. 1.

Kent, Sherman. 1949. *Strategic Intelligence for American World Policy*. Princeton University Press.

Lowenthal, Mark. 1999. *Intelligence: From Secrets to Policy*. CQ Press, 1999.

National Intelligence Council. 2021, March 10. *Foreign Threats to the 2020 US Federal Election*. https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf.

Office of the Director of National Intelligence. 2021, October 21. *Climate Change and International Responses Increasing Challenges to US National Security through 2040*. https://www.dni.gov/files/ODNI/documents/assessments/NIE_Climate_Change_and_National_Security.pdf.

Office of the Director of National Intelligence. 2021. *Global Trends 2040*. https://www.dni.gov/index.php/gt2040-home.

Pili, Giangiuseppe. 2019. "Toward a Philosophical Definition of Intelligence." *International Journal of Intelligence, Security, and Public Affairs* 21, no. 2: 162–90.

Random, H. A. 1958. "Intelligence as a Science." *Studies in Intelligence* (Spring).

Simms, Jennifer. 2022. *Decision Advantage: Intelligence in International Politics from the Spanish Armada to Cyberwar*. Oxford University Press.

Shulsky, Abram, and Gary Schmitt. 1991. *Silent Warfare: Understanding the World of Intelligence*, 3rd ed. Potomac Books.

Treverton, Gregory et al. 2006. *Toward a Theory of Intelligence: Workshop Report*. RAND Corporation.

Troy, Thomas. 1991-1992. "The 'Correct' Definition of Intelligence." *Journal of Intelligence and Counterintelligence* 5, no. 4 (Winter).

Wark, Wesley. 1994. *Espionage: Past, Present, Future?* Frank Cass.

Warner, Michael. 2002. "Wanted: A Definition of 'Intelligence.'" *Studies in Intelligence* 46, no. 3.

Warner, Michael. 2009. "Building a Theory of Intelligence Systems." In *National Intelligence Systems Current Research and Future Prospects*, eds. Gregory Treverton and Wilhelm Agrell. Cambridge University Press.

❖ ❖ ❖

Transforming Intelligence Production Through Lean Start-up Methods

William Schlickenmaier

The changing commercial and technological landscape is creating a fundamental challenge to IC analysis that we have not faced since the creation of the US Intelligence Community after World War II.

IC analysis is at risk of obsolescence. Trends in data, software, and customers require new ways of doing business in the face of a new trend—the democratization of intelligence. This article offers a new, team-based "agile" analytic framework leveraging developments in software development and the commercial start-up community. I outline a seven-step process for finished intelligence production that combines all-source and collection expertise with data engineering and software development, and then I propose opportunities for experimentation as a way forward.

Reinventing Analysis, Again

Few professions seem as prone to self-reflection as intelligence. Scholars and practitioners inside and outside the profession have regularly called for reinventing intelligence analysis, often in the wake of intelligence failures or in reaction to advances in information technology. The topic has appeared regularly in these pages. Some prefer a return to the "glory days" of Sherman Kent, while others see opportunities in the changing technological environment. In some way this debate is evergreen—analysis seems always on the table for discussion, and we always wonder whether we have to rethink our capabilities and what makes us special as a community. I recognize that there are Cassandras who often say that doom is imminent, even when it is not. But the changing commercial and technological landscape is creating a fundamental challenge to IC analysis that we have not faced since the creation of the US Intelligence Community after World War II.

Commercial + Technological = Existential Crisis

The IC has profound organizational and cultural incentives to avoid transforming its analytic production processes or delivery systems.[1] It has been, to date, both a monopoly and a monopsony—the sole provider to a sole consumer locked into its access.[2] Yet both ends of this spectrum are breaking down, and scholars of entrepreneurship have made clear that institutions lacking disruptive innovation in their investment portfolio are doomed to eventual obsolescence when the commercial and technological landscape around them change.[3]

Why this is happening is what many have dubbed the "democratization of intelligence." Collection has already radically shifted. Commercial geospatial-intelligence (GEOINT) exploitation led the way on public discussions of Russia's preparations for its 2022 invasion of Ukraine, and now firms can even conduct signals intelligence collection from space

for commercial clients.[a] Commercial and leaked data are revealing the infrastructure that enables intelligence operations around the world.[4] Analysis is starting to change as well. Private-sector intelligence analysts are fielding network tools to target malign actors.[5] The recent emergence of large language models (LLMs) has raised more fundamental questions about the future of analysis.[6]

The IC has taken some steps to remedy this situation. DIA incorporated lean start-up insights in the development of MARS—the Machine-Assisted Analytic Rapid Repository System—and into other innovative programs.[7] CIA created the Directorate of Digital Innovation. These are important innovations for the development of capability and collection, but they have not fundamentally changed how the IC produces finished or current analysis.

The commercial sector, particularly the software industry, shows the changes that IC all-source analysis must consider lest it become irrelevant to policy customers in the future. As Marc Andreessen famously quipped over a decade ago, "Software is eating the world."[8] By this he meant that anything that *can* become software *will* become software. The ubiquity of "big data" amplifies these trends, creating a situation of dominance for those who can harness it by bringing software to bear for analytic purposes, and irrelevance for those who cannot.[9]

Beyond this, what Azeem Azhar describes as the "exponential age" goes to an additional important truth.[10] Obsolescence today is like Ernest Hemingway's observation about bankruptcy—it happens "gradually, then suddenly."[b] Under the complex conditions that define contemporary global geopolitics, surprise happens quickly, and organizations unprepared for it risk their relevance—or worse.[c,11] And commercial entities have learned the lesson of scaling quickly to gain monopoly power in the market, meaning that competitors are almost certainly eyeing IC analysis as a domain to outflank.[12]

What does this mean? A future of writing papers, be they *President's Daily Briefings* or long assessments, will be obsolete before we know it. And we are unlikely to be able to survive as an analytic ecosystem living in this past, with customers increasingly demanding different kinds of solutions and competitors providing it. However, the best of what we bring to bear as an analytic community is not in our written product. It is in the special intersection of expertise and creativity that make our minds, when harnessed properly, a national strategic asset.[13]

In the next sections, I offer a proposal to take advantage of the revolutions occurring in the software industry in particular to transform analysis. We can do so—moving from static documents like papers and briefing slides into software—in line with Andreeseen's vision, developed with commercial best practices, and consistent with DNI policy guidance including ICD-208.[d] And I believe this is our best chance to protect our analytic value-added for the future to come.

Step 1: From Analytic Production to Analytic Project Management

Reimagining finished intelligence through commercial best practices first requires a paradigm shift: thinking of analytic production as project management to produce analysis as software. Over the past 15 years, software development has shifted to flexible, team-based methodologies by leveraging agile and lean start-up methodologies developed by manufacturing firms like Toyota, Silicon Valley innovators, and software successes that now span industries.[14]

A software-centric analytic approach adds machine learning and AI to substantive expertise.[15] Advanced analytics show the "patterns of life" on topics to determine if events are deviations from "normal" in ways that human intuition cannot. As software-based solutions, analytic results are more transparent than a footnoted paper, despite concerns about machine learning's black-box effect.[16]

A move to agile, lean start-up project management yields changes to the existing analytic production process: a move away from

a. Examples of this include the social media feed of Michael Kofman (https://twitter.com/kofmanmichael/ and the work of the Institute for the Study of War, whose interactive map is available at https://storymaps.arcgis.com/stories/36a7f6a6f5a9448496de641cf64bd375. On commercial SIGINT from space, see https://www.he360.com/

b. *The Sun Also Rises* (Scribner's, 1926)

c. Adam Tooze famously describes this as a "polycrisis," borrowing from a body of work dating back over the past few years.

d. ICD-208 states analytic organizations "shall produce products in a format customers can easily discover, access, use, and disseminate to facilitate mission requirements."

Agile Analysis: Select Resources

The concept of agile analysis fits into a conversation on the future of analysis that includes, among a great many others, the following publications:

- Zachery Tyson Brown, "The US Intelligence Community Is Being Disrupted," *Defense One* (blog), June 23, 2020, https://www.defenseone.com/ideas/2020/06/us-intel-community-being-disrupted/166372/.
- Committee on a Decadal Survey of Social and Behavioral Sciences and for Applications to National Security, "A Decadal Survey of the Social and Behavioral Sciences: A Research Agenda for Advancing Intelligence Analysis," Consensus Study Report (National Academies of Sciences, Engineering, and Medicine, 2019).
- Joseph W. Gartin, "The Future of Analysis," *Studies in Intelligence* 63, no. 2 (June 2019).
- Josh Kerbel and Anthony Olcott, "Synthesizing with Clients, Not Analyzing For Customers," *Studies in Intelligence* 54, no. 4 (December 2010.
- John S. Mohr, "A Call for More Humility in Intelligence Analysis," *Studies in Intelligence* 61, no. 4 (December 2017).

On Kent, see Richards J. Heuer, *Psychology of Intelligence Analysis* (CIA, 1999), as well as Brown's critique, "What If Sherman Kent Was Wrong? Revisiting the Intelligence Debate of 1949," *War on the Rocks* (blog), October 1, 2020, https://warontherocks.com/2020/10/what-if-sherman-kent-was-wrong-revisiting-the-intelligence-debate-of-1949/.

On changes in the technological landscape, see:

- Aaron F. Brantly, "When Everything Becomes Intelligence: Machine Learning and the Connected World," *Intelligence and National Security* 33, no. 4 (2018): 562–73;
- Christopher Eldridge, Christopher Hobbs, and Matthew Moran, "Fusing Algorithms and Analysts: Open-Source Intelligence in the Age of 'Big Data,'" *Intelligence and National Security* 33, no. 3 (2018)
- Aaron Frank, "Computational Social Science and Intelligence Analysis," *Intelligence and National Security* 32, no. 5 (2017)
- Kwasi Mitchell, et al., "The Future of Intelligence Analysis: A Task Level View of the Impact of Artificial Intelligence on Intel Analysis," *Deloitte Insights* (Deloitte Center for Government Insights, December 11, 2019).

For information on agile, lean start-up efforts, The definitive work on lean start-up efforts is Steve Blank and Bob Dorf, *The Startup Owner's Manual: The Step-By-Step Guide for Building a Great Company*; an exemplar of agile and scrum methodologies can be found on the website of Mountain Goat Software, a leading developer of these capabilities and methods.

an author-contributors setup to a cross-functional team; prioritizing customer and source discovery; shifting from conceptualization and research to development "sprints"; from drafting product to fielding minimum viable products (MVPs); from formal review to customer-based feedback and pivots; from one-time publication to continuous analytic delivery; and from rewriting products to reviewing and refreshing existing analytics.

Step 2: From Author and Contributors to Cross-Functional Team

Analytic production shifts from a single author collaborating with occasional contributors to a cross-functional team led by an all-source analyst. The all-source analyst becomes what agile software development calls a "product owner" who drives the effort and determines what is important.[17] Product owners do not conduct research alone or in a small group of fellow analysts, bringing in collaborators for an occasional brainstorming session, then sharing a drafted piece for coordination. They serve as project managers on their all-source "accounts," be that a global coverage or hard-target question in any IC all-source analytic agency.

- The all-source analytic product owner leads a cross-functional team—consistent with agile principles—to generate tailored analysis on their account. This paper proposes a cross-functional

team of five full-time members and two part-time members:

- An all-source collection strategist compiles the full range of intelligence that could answer questions on the product owner's account. This includes both an understanding of all the "INTs" and the nature of potential and actual collection streams, such as the range of open-source and commercially available data; liaison services or unilateral sources providing human intelligence; or the relative value of different forms of technical collection. This allows the team to understand the implications of the collection enterprise on a topic and its gaps.
- A data engineer and integrator structures and analyzes data feeds on the team's account as defined by the product owner and her management. Feeds range from standing reporting fed into enterprise databases to automated reporting from national agencies or commercial sources. The data engineer and integrator would curate feeds to ensure they are analyzable, as well as creating the analytics to assess trends over time.
- A programmer and developer write code to deliver analysis through dashboards, other front-end interfaces, scripts and algorithms that auto-generate email updates on changes in patterns relevant to customers.
- A security and standards expert in the team ensures that the project is built consistent with security standards for websites, for the handling of intelligence streams, and with analytic standards like ICD-203. This team member also mobilizes structured analytic techniques and other ICD-203-consistent tools to help the project in development, building on continuous integration principles from the DevSecOps model.[18]
- Senior analysts bring analytic concepts and insights from previous production into the project to consider how it should fit with or diverge from analytic lines.[19] They also support coordination and equity checks with other stakeholders in an agency or across the IC. Finally, they serve as adversaries or devil's advocates to stress-test the effort and ensure it is the best possible work. Such an individual could support multiple projects, leveraging insights from multiple projects to generate analytic synergies.
- A facilitator coordinates the team's work through daily and biweekly meetings, potentially participating in multiple parallel analytic efforts at once.[20] In agile terms, this individual serves as a scrum master, bringing both specific training and an understanding of structured analytic techniques to the project.

Step 3: Putting Customer and Source Discovery First

Agile analysis puts a premium on understanding and responding to customers' ongoing feedback. The team therefore starts by applying the product owner's focus to two parallel tasks: customer and source discovery.[21]

- The product owner, senior analyst, and programmer/developer focus on a diverse range of policy and operational customers for the product owner's account.[22] They identify specific, concrete insight needs from those policy and operational customers and learn through a series of structured conversations the best ways to deliver those insights.[23] This discovery process generates users for initial MVPs the team will later field.[24]
- The collection strategist, data engineer, and security/standards expert focus on the full range of collection sources. They focus on what is being collected and exploited, what could be collected or exploited, and potential biases in collection. The data engineer/integrator ensures the appropriate structure of data feeds, while the security/standards expert manages access to compartmented collection.

Step 4: From Conceptualization and Drafting to Sprints

The team builds a flexible plan for how to provide analysis. This is similar to the way in which today's analytic organizations conceptualize finished intelligence production, providing managers an opportunity to review and approve the flow of analytic work. Unlike the current approach, which focuses on the "why" of analytic work and yields a static document, an agile analytic plan focuses on the "how" and changes over time.

The team manages its work using agile's scrum methodology, where it meets daily to collaborate on what to do that day, reviewing the overall state of the project every two weeks in a "sprint review".[25] Analytic

managers participate in sprint reviews to understand the arc of the effort and provide feedback, and the product owner uses reviews to determine the priority for delivery and development. Priorities are generated using "user stories," short examples of desired capabilities derived from customer and source discovery.[26] As discovery continues, these biweekly meetings allow the team to change its plan and pursue new capabilities.

Day to day work is integrated, collaborative, and colocated.[27] The product owner helps the data engineer/integrator shape analytics, tests software with the programmer/developer, and answers questions as a subject matter expert for the team. The data engineer/integrator creates analytics leveraging other team members' collection, code, security, standards and tradecraft expertise. The programmer/developer develops user interfaces and application programming interfaces for the product owner to test, as well as scripts and other automation solutions to integrate the data engineer's analytics into those interfaces. The security/standards expert engages with all team members to maintain compliance, and the senior analyst ensures that outside and divergent perspectives are considered. The facilitator keeps the team on track, running daily and biweekly meetings.[a]

Step 5: From Coordination to MVPs

Rather than waiting to provide a polished, final product, the team quickly fields initial insights through MVPs and shares them with policy and operational customers to get feedback on the analytic project and consider possible changes.[28] Analytic MVPs may be preliminary analytic insights or mock-ups of finished production in different formats, letting the team beta-test functionality. MVPs are important to the analytic process because market research indicates that customers, whether of software or of analysis, do not know what they really want and need until they can touch and feel a prototype and react to it.[29]

MVPs can also improve coordination within the IC by enabling stakeholders to stress-test a potential solution and consider whether it is consistent with best practices and existing analytic lines. That said, coordination cannot replace customer insights, as policy and operational requirements supersede the views of fellow analysts.

Step 6: From Review to Pivots

Agile teams "pivot" their efforts in response to interim customer feedback rather than waiting for post-production responses, adapting plans in sprint reviews and delivering new increments of analysis over time.[30] Pivots can range from developing a new user interface to focusing on different elements of an account or topic. This model eliminates the existing analytic review process, because thanks to MVPs, the team regularly releases interim analytic results directly to customers and adapts to feedback. Agile and lean start-up methods eschew detailed review processes because they find that whatever they may add in rigor, they reduce timeliness to the point that they render products irrelevant. This echoes the analytic IC's classic dilemma—beautifully written consensus text delivered too late to help customers with their problems.[b]

Openness to customer feedback can be a double-edged sword, as the product owner, senior analyst, and security/standards expert must guard against pivots turning into politicization or otherwise contaminating analytic objectivity.[31] The senior analyst and security/standards expert reinforce a product owner who could face politicization pressures.

Step 7: From Publication to Continuous Analytic Delivery

Agile analysis delivers an analytic program on an account with multiple delivery options instead of a single printed or published document. Delivery options include dashboards, advanced analytics for use in legacy printed production, scripts for the automatic delivery of analysis via email, or other software-based solutions.[32] Solutions the team develops ingest data from collection agencies and update themselves using a combination of machine learning and all-source human insight, eliminating the existing problem of intelligence cutoff dates and obsolete analysis. Programming audit trails, versioning, and cheap cloud storage allow the team to save analytics over time to show the "arc" of a story, including through the use of

a. This differs from the role of analytic facilitators, who typically are only brought in for a specific brainstorming or group activity at an early stage in finished intelligence production.

b. Every policy customer complains about this tension between timeliness and "perfection." I did when supporting policy on rotation to the National Security Council and and defense policy staffs, 2009–12.

large language models. Direct customer engagement through briefers, dashboards, and other software platforms provide a range of feedback for future analytic efforts.

Step 8: From Rewriting to Review and Refresh

Analytic solutions provided through the agile process will remain relevant for longer than traditional printed products. At a certain point, the product owner and her analytic management will determine that the solutions are stable enough that the team can disband from its active efforts and move the capability into a reserve or maintenance status. Team members other than the product owner would join other agile analytic efforts, while the product owner would move into an "offline" status, monitoring the analytic capabilities while conducting training or other professional development and continuing education activities. The product owner monitors whether analytics are getting stale or an adversary is applying denial-and-deception techniques to spoof pattern-of-life tracking, and works with management to quickly update and rework existing analytic capabilities.[33] Management creates a "review and refresh" cycle based on the President's Intelligence Priorities framework to determine how often an analytic capability requires a minor update or a complete rebuild.[34]

Four Implications of Agile Analysis

Agile analysis would, if fully implemented, have significant human capital, expertise, integration, and trust implications.

- All-source analysts can focus on creativity, thinking, and leading teams, which they consider rich, rewarding work where they can avoid the drudgery of filling out routine responses to taskers.[35] Rather than making analysts obsolete, agile analytics improve retention and analytic quality of life.
- The "online-offline" model, where analysts focus on building capabilities then go into maintenance with time for professional development, offers enhanced opportunities to build domain and regional expertise. [36]
- Cross-functional integration lets all-source analysts continue to lead analytic production but gives other components of the production process an equal voice in the team.
- The iterative nature of the new production process builds trust between analysts and customers and between analysts and their managers. Biweekly sprint reviews with managers allow those managers, over time, to delegate an increasing proportion of decisions to product owners, while MVPs and pivots let customers see that the team is responsive to their feedback. Agile and lean start-up methods make clear that significant management interference in the work of cross-functional teams will lead to mission failure.

What are We Waiting For?

In 2000, the consulting firm McKinsey developed the Three Horizons Model for growth investments. The model recognized that a majority of a firm's investments need to remain in current operations, but a healthy firm needs to invest some resources in incremental innovation to allow for changes to current practices, and a capability for truly disruptive innovation that would allow for game changing breakthroughs.[37] Firms from Amazon to TSMC, from Microsoft to Apple have done just this. A volatile, complex world makes these sorts of "hedge investments" even more critical.

Where are these for IC analysis? We have tended to focus on the areas where we are comfortable—writing, briefing, thinking, talking to policy customers or liaison partners. We need the space for disruptive innovation in analysis. Wherever it is—whichever agency, or for that matter whichever private-sector partner—decides to build out a capability like that described above may have a significant competitive advantage in the years and decades to come. Regardless of whether this specific pathway is the right answer, pursuing a portfolio of pathways is indispensable if we want IC analysis to matter for customers, and for that matter for the American people, in this era of technological change and strategic competition.

❖ ❖ ❖

The author: William Schlickenmaier is a senior strategist and member of CIA's Senior Analytic Service. He holds a PhD in international relations from Georgetown University, where he teaches classes on international relations theory and US foreign policy.

Endnotes

1. See Priscilla Clapp, Morton Halperin, and Arnold Kanter, *Bureaucratic Politics and Foreign Policy*, second edition (Brookings Institution Press, 2006) and Amy Zegart, *Spying Blind: The CIA, The FBI, and the Origins of 9/11* (Princeton University Press, 2007).
2. See Harvey Sapolsky and Eugene Gholz, "The Defense Monopoly," *Regulation*, 1999; Eric Lofgren, "Does the DOD Have Monopsony Power in Defense Markets?" *Acquisition Talk* (blog), May 25, 2019, https://acquisitiontalk.com/2019/05/does-the-dod-have-monopsony-power-in-defense-markets/.
3. Clayton M. Christensen, *The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail*, (Harvard Business Review Press, 2016); Gautam Mukunda, "We Cannot Go On: Disruptive Innovation and the First World War Royal Navy," *Security Studies* 19, no. 1 (2010): 124–59.
4. See Bellingcat, "305 Car Registrations May Point to Massive GRU Security Breach," October 4, 2018, available at https://www.bellingcat.com/news/2018/10/04/305-car-registrations-may-point-massive-gru-security-breach/ and "Russian Vehicle Registration Leak Reveals Additional GRU Hackers," October 22, 2020, available at https://www.bellingcat.com/news/uk-and-europe/2020/10/22/russian-vehicle-registration-leak-reveals-additional-gru-hackers/
5. See Naomi Garcia, "Trade Secrets: Exposing China-Russia Defense Trade in Global Supply Chains," July 15, 2022, available at https://c4ads.org/reports/trade-secrets/; "Party Capital: A Blueprint for National Security Due Diligence on China," September 16, 2021, available at https://c4ads.org/reports/party-capital/.
6. See for example Cade Metz and Keith Collins, "10 Ways GPT-4 Is Impressive but Still Flawed," *New York Times*, March 14, 2023; Drew Harwell and Nitasha Tiku, "GPT-4 has arrived. It will blow ChatGPT out of the water," *Washington Post*, March 14, 2023; Sandra Erwin, "On National Security: Analyzing intelligence in the age of ChatGPT," *SpaceNEWS*, January 14, 2023; and Stew Magnuson, "Just In: Pentagon's Top AI Official Addresses ChatGPT's Possible Benefits, Risks," *National Defense Magazine* (March 8, 2023); "Coffee and Conversation with Linda Weissgold," Intelligence and National Security Alliance (January 24, 2023), available at https://www.insaonline.org/detail-pages/event/2023/01/24/default-calendar/coffee-conversation-with-linda-weissgold
7. Katie Malone, "DIA Focuses on Data Prep for National Security AI," MeriTalk, (April 28, 2020), https://www.meritalk.com/articles/dia-focuses-on-data-prep-for-national-security-ai/. See also Craig Dudley, "Lessons from SABLE SPEAR: The Application of an Artificial Intelligence Methodology in the Business of Intelligence," *Studies in Intelligence* 65, no. 1 (March 2021).
8. Marc Andreessen, "Why Software Is Eating the World," *Wall Street Journal*, August 20, 2011, https://www.wsj.com/articles/SB10001424053111903480904576512250915629460.
9. Kareem Ayoub and Kenneth Payne, "Strategy in the Age of Artificial Intelligence," *Journal of Strategic Studies* 39, no. 5–6 (2016): 793–819; Mitchell et al., "The Future of Intelligence Analysis: A Task Level View of the Impact of Artificial Intelligence on Intel Analysis"; Committee on a Decadal Survey of Social and Behavioral Sciences and for Applications to National Security, "A Decadal Survey of the Social and Behavioral Sciences: A Research Agenda for Advancing Intelligence Analysis"; "Draft Final Report" (National Security Commission on Artificial Intelligence, January 2021), https://www.nscai.gov/reports.
10. Azeem Azhar, *The Exponential Age: How Accelerating Technology is Transforming Business, Politics, and Society*, (Diversion Books, 2021).
11. For more on the questions of complexity that drive risks to organizational stasis, see for example, Joshua Cooper Ramo, T*he Age of the Unthinkable: Why the New World Disorder Constantly Surprises Us And What We Can Do About It* (Little, Brown, 2009); Nassim Nicholas Taleb and Gregory F. Treverton, "The Calm Before the Storm: Why Volatility Signals Stability, and Vice Versa," *Foreign Affairs* (February 2015); and Duncan J. Watts, *Six Degrees: The Science of a Connected Age* (W.W Norton, 2004).
12. See Reid Hoffman and Chris Yeh, *Blitzscaling: The Lightning-Fast Path to Building Massively Valuable Companies* (Currency, 2018); Peter Thiel and Blake Masters, *Zero to One: Notes on Startups, or How to Build the Future* (Currency, 2014).
13. On creativity in the IC, see Josh Kerbel, "For the Intelligence Community, Creativity Is the New Secret," *World Politics Review* (blog), March 25, 2010, https://www.worldpoliticsreview.com/articles/5329/for-the-intelligence-community-creativity-is-the-new-secret; Josh Kerbel, "The U.S. Intelligence Community's Creativity Challenge," *National Interest*, October 13, 2014, https://nationalinterest.org/feature/the-us-intelligence-communitys-creativity-challenge-11451. On the role of expertise, see Gary Klein, *Seeing What Others Don't: The Remarkable Ways We Gain Insights*, (Public Affairs, 2013)
14. Kent Beck et al., "Manifesto for Agile Software Development," *Agile Manifesto* (blog), accessed November 3, 2020, http://agilemanifesto.org. Steve Blank and Bob Dorf, *The Startup Owner's Manual: The Step-By-Step Guide for Building a Great Company* (Wiley, 2020); Jeff Sutherland and J.J. Sutherland, *Scrum: The Art of Doing Twice the Work in Half the Time* (Currency, 2014); Eric Ries, *The Lean Startup: How Today's Entrepreneurs Use Continuous Innovation to Create Radically Successful Businesses* (Currency, 2011).
15. See Cheryl Pellerin, "Deputy Secretary: Third Offset Strategy Bolsters America's Military Deterrence," *DOD News/Defense Media Activity* (October 31, 2016); "3rd Offset Strategy 101: What It Is, What the Tech Focuses Are," *DODLive* (blog) (March 30, 2016), https://www.dodlive.mil/2016/03/30/3rd-offset-strategy-101-what-it-is-what-the-tech-focuses-are/.
16. See https://www.darpa.mil/program/explainable-artificial-intelligence
17. Richard Seroter, "Product Ownership Explained," *Agile Alliance*, https://www.agilealliance.org/resources/sessions/product-ownership-explained/; "Product Owner," *Agile Alliance*, accessed November 3, 2020, https://www.agilealliance.org/glossary/product-owner/.

18. On SATs, see Stephen J. Coulthart, "An Evidence-Based Evaluation of 12 Core Structured Analytic Techniques," *International Journal of Intelligence and Counterintelligence* (*IJIC*) 30, no. 2 (2017): 368–91. On DevSecOps, see "What Is DevSecOps?," *RedHat* (blog), accessed January 21, 2021, https://www.redhat.com/en/topics/devops/what-is-devsecops. On the need for continuous integration, see Gene Kim, *The Phoenix Project: A Novel about IT, DevOps, and Helping Your Business Win* (IT Revolution Press, 2013).
19. See Peter Gill and Mark Phythian, "Developing Intelligence Theory," *INS* 33, no. 4 (2018): 467–71. For an example of how a long time senior analyst applied such a model, see Andrew Skitt Gilmour, *A Middle East Primed for New Thinking: Insights and Policy Options from the Ancient World* (Center for the Study of Intelligence, September 2019). See also James D. Marchio, "Fostering Creativity in the IC: Insights from Four Decades Ago," *Studies in Intelligence* 65, no. 4 (December 2021).
20. Yi Lv, "Manager as Scrum Master," *Agile Alliance* (blog), accessed November 3, 2020, https://www.agilealliance.org/resources/experience-reports/manager-as-scrum-master/; Mark Rajpal, "Multiple Roles: Scrum Master as a Team Member," *Agile Alliance* (blog), May 2018, https://www.agilealliance.org/resources/experience-reports/multiple-roles-scrum-master-as-a-team-member/.
21. Steve Blank, "The Innovation Stack: How to Make Innovation Programs Deliver More than Coffee Cups," *Steve Blank* (blog), June 5, 2018, https://steveblank.com/2018/06/05/whats-next-for-getting-stuff-done-in-large-organizations-the-innovation-stack/; Blank and Pete Newell, "What Your Innovation Process Should Look Like," *Harvard Business Review*, September 11, 2017, https://hbr.org/2017/09/what-your-innovation-process-should-look-like; Blank and Dorf, *The Startup Owner's Manual: The Step-By-Step Guide for Building a Great Company*.
22. Blank and Newell, "What Your Innovation Process Should Look Like"; Blank and Dorf, *The Startup Owner's Manual*; Eric Ries, "The Lean Startup Methodology," *The Lean Startup*, accessed November 3, 2020, http://theleanstartup.com/principles.
23. Steve Blank, "The Mission Model Canvas: An Adapted Business Model Canvas for Mission-Driven Organizations," *Steve Blank* (blog), February 23, 2016, https://steveblank.com/category/business-model-versus-business-plan/. The programmer/developer is part of this team to understand code and user interface requirements.
24. Blank and Dorf, *The Startup Owner's Manual*; Ries, "The Lean Startup Methodology."
25. "Scrum," *Mountain Goat Software* (blog), accessed November 3, 2020, https://www.mountaingoatsoftware.com/agile/scrum; "The Scrum Guide," *Scrum Guides*, accessed November 3, 2020, https://www.scrumguides.org/scrum-guide.html; "New to Agile and Scrum," *Mountain Goat Software*, accessed November 3, 2020, https://www.mountaingoatsoftware.com/agile/new-to-agile-or-scrum.
26. "User Stories," *Mountain Goat Software*, accessed November 3, 2020, https://www.mountaingoatsoftware.com/agile/user-stories. In an ideal world, the software would leverage the low-code/no-code revolution. See Rex Woodbury, "The Building Blocks of Tech: Roblox, Airtable, and the Rise of Low Code/No Code," *Digital Native* (blog), October 21, 2020, https://digitalnative.substack.com/p/roblox-airtable-and-the-building.
27. "The Scrum Guide."
28. Blank and Dorf, *The Startup Owner's Manual*; Ries, "The Lean Startup Methodology."
29. Blank, "The Innovation Stack: How to Make Innovation Programs Deliver More than Coffee Cups"; Blank and Newell, "What Your Innovation Process Should Look Like"; Blank and Dorf, *The Startup Owner's Manual*.
30. "The Innovation Stack."
31. Michael Rubin, "The Temptation of Intelligence Politicization to Support Diplomacy," *International Journal of Intelligence and Counterintelligence* 29, no. 1 (2016): 1–25; Robert M. Gates, "Guarding Against Politicization," *Studies in Intelligence* 36, no. 1 (Spring 1992); Uri Bar-Joseph, "The Politicization of Intelligence: A Comparative Study," *International Journal of Intelligence and Counterintelligence* 26, no. 2 (June 2013).
32. Scripts build on a trend toward newsletters in the overall delivery of content. See Anna Wiener, "Is Substack the Media Future We Want?," *New Yorker*, January 4, 2021, https://www.newyorker.com/magazine/2021/01/04/is-substack-the-media-future-we-want.
33. On denial and deception, see Roy Godson and James J. Wirtz, "Strategic Denial and Deception," *International Journal of Intelligence and Counterintelligence* 13, no. 4 (2000): 424–37.
34. Intelligence Community Directive 204: National Intelligence Priorities Framework (Office of the Director of National Intelligence, January 2, 2015), https://www.dni.gov/files/documents/ICD/ICD%20204%20National%20Intelligence%20Priorities%20Framework.pdf.
35. Marchio, "Fostering Creativity in the IC: Insights from Four Decades Ago."
36. See Gary Klein, *Seeing What Others Don't: The Remarkable Ways We Gain Insights* (PublicAffairs, 2013); Rob Johnston, *Analytic Culture in the US Intelligence Community: An Ethnographic Study* (Central Intelligence Agency, 2005), 61–68.
37. Steve Blank criticized the Three Horizons Model for presuming that there is a luxury of time in disruptive innovation. I agree with his approach. See Blank, "McKinsey's Three Horizons Model Defined Innovation for Years. Here's Why It No Longer Applies," *Harvard Business Review* (February 1, 2019).

❖ ❖ ❖

How Intelligence Analysts Experience Threats to Rigor

Adrian Wolfberg, PhD

This article is extracted from Dr. Wolfberg's research monograph, In the Face of Ambiguity: How Intelligence Analysts Experience Threats to Rigor, *based on his work as a senior research fellow at the National Intelligence University (2020–22). The full report, with citations, as well as his previous monographs on artificial intelligence and the challenges of analytic insights, can be found in the NIU Caracristi Monograph collection at https://ni-u.edu/wp/caracristi/caracristi-monographs/. The views expressed are those of the author and do not reflect the official policy or position of the National Intelligence University, Office of the Director of National Intelligence, or any other US government entity.*

Key Findings

This study of 26 intelligence analysts reveals that ambiguity is ubiquitous in the worklife of imagery-based analysts who conduct foundational military intelligence (FMI). Yet, imagery-based products are expected to be precise and accurate in order to support military targeting and provide military commanders and policymakers with faultless situational awareness of adversaries. This is the wicked twofold nature of the problem: ambiguity is a threat to rigor and to the conclusions drawn by analysts about the adversary.

Analysts experience ambiguity through a three-step process: first, they are exposed to sources of ambiguity; then they confront barriers to overcoming the sources of ambiguity; and last, they leverage individual actions to surmount those barriers. Even if analysts can identify and understand sources of ambiguity, various individual and organizational barriers divert or prevent them from focusing on ways to mitigate ambiguity. Yet, the analysts interviewed for this study have found they can sometimes successfully act in the face of ambiguity to overcome barriers and to mitigate or resolve ambiguity.

Ambiguity arises from various sources, challenging analysts to accurately perceive causality and strategize effective actions to overcome

This study provides three contributions to the research on ambiguity within the IC context.

ambiguities. This study integrates disparate theoretical and empirical concepts of ambiguity into a holistic model, beginning with the three types of sources of ambiguity: individual, organizational, and combined individual/organizational. In the third type, also called dilemma-induced, the organization originates the dilemma of deciding between two choices, and the individual must then determine how to navigate between these two choices. Although these sources are the triggers for analysts to take mitigating actions, individual, organizational, and societal barriers to overcoming ambiguity may get in the way of completing the identified actions.

Analysts experience a diverse set of cognitive, emotional, and social effects when exposed to ambiguity, and organizations should be aware of their nature. Implementing solutions that target a cognitive issue may not work, and may even backfire, if the issue is emotional or social, for example. Of the three categories of ambiguity addressed in this study—sources, barriers, and actions—sources of ambiguity generate cognitive and social responses, barriers produce social and emotional responses, and actions are built on cognitive, social, and emotional behaviors.

Consequently, organizations may benefit from developing a three-legged strategy to reduce the risk of ambiguity so that it does not thwart the advancement of rigor. One leg of the strategy is to know the sources of ambiguity, and the second is to be aware of barriers to overcoming ambiguity. Barriers originate within the individual and within the organization and society. The third leg of the strategy is to take appropriate, realistic, and effective actions to overcome ambiguity. Organizational leadership is key to improving rigor by mitigating ambiguity, and the role of management is equally important to ensuring implementation.

This study provides three contributions to the research on ambiguity within the IC context.

- The first is practical, by creating a framework that combines sources of ambiguity—within the individual, within the organization and society, and a combined individual/organization dilemma-induced category—with the individual analyst's experience of ambiguity within the cognitive, social, and emotional domains.
- The second is methodological, by moving beyond the theoretical concepts from the literature and introducing empirically demonstrable and specific phenomena experienced by intelligence analysts.
- The third is theoretical, by providing imagery-based intelligence analysts who conduct FMI with a new mediational model of how barriers to overcoming ambiguity affect the relationship between the sources of ambiguity and the actions to overcome ambiguity. This model can be used to guide future research.

Organizations may benefit from professionalizing the workforce of the imagery-based FMI analysts. Key elements of such a policy would include theory, method, and practice. This study offers a theory of ambiguity as it applies to intelligence analysis: ambiguity has a negative effect on rigor in intelligence analysis because ambiguity and rigor are polar opposites, and—left unresolved—these opposites place the analyst in an untenable situation. The method would use qualitative research when phenomena are not well understood and quantitative research when they are. The practice would involve the effective use of policy and strategy. For example, introduction of specialized training, education, and certification; incorporation of research into the profession; engagement of governing bodies and ethics; and encouragement of forms of self-improvement, such as lessons learned.

The findings of this study, although focused on the ambiguity experience of imagery analysts, may apply to other collection disciplines that cope with ambiguity focused on FMI, such as signals intelligence, measurement and signature intelligence, and open-source intelligence. How imagery analysts cope with ambiguity may also resonate with all-source analysts within all-source intelligence agencies; intelligence directorates within US combatant commands; and allied intelligence organizations, particularly in the United Kingdom, Australia, and Canada.

Ambiguity as the Enemy of Rigor

Intelligence analysts make the effort to employ analytic rigor as part of their tradecraft. Rigor is an important criterion for both producers and consumers of intelligence because it shapes the believability, credibility, and truthfulness of the knowledge produced. For consumers

of intelligence, demonstrated rigor assures national security policymakers and operational commanders that intelligence assessments are credibly accurate and, therefore, can be trusted. However, analytic rigor does not have a clear or widely accepted definition among academics who study foreign intelligence and practitioners of foreign intelligence. For the purposes of this study, analytic rigor is defined as a process employing thoroughness, precision, or exactness.

Yet, a key threat to attaining rigor is ambiguity. The real-world problem with ambiguity is that it can hide the adversary from analysts. The research problem for this study, therefore, is if analytic rigor needs precision and exactness, how do analysts achieve rigor when faced with ambiguity? What makes this an interesting research problem is how ambiguity impedes rigor. Not doing anything or at least not enough to reduce ambiguity obstructs analysts from understanding the adversary—and the adversary's intent and capabilities. Alternatively, efforts resulting in the successful resolution of ambiguity can lead to revealing the adversary.

This study takes one step beyond acknowledging the "fact of" ambiguity to systematically inquire into the types of ambiguity experienced by intelligence analysts. As this study's literature review suggests, how analysts deal with ambiguity while solving an analytical problem directly impacts their ability to achieve product credibility and gain customer trust. The research gap is not knowing the precise role that ambiguity plays. To fill this gap, this study asks the following research question: What kinds of ambiguity do intelligence analysts face?

The research problem for this study, therefore, is if analytic rigor needs precision and exactness, how do analysts achieve rigor when faced with ambiguity?

Given the need for analytic rigor, the scope of this research study is to understand the analysts' cognitive and emotional interaction with their data as they work on an intelligence problem. To further limit the scope of the research, the study specifically focuses on the nature of analysts' interactions with data when facing ambiguity.

Research efforts have primarily focused on measuring or devising measures to assess the outputs of analysis, such as rigor in the intelligence product. However, none of the policy documents and very little of the existing literature on analytic rigor describe how individual analysts interact with their data during the process of analysis—before a product is created and with the organizational goal of achieving a rigorous assessment. Hence, the purpose of this research is to shed light on the role that ambiguity plays in the pursuit of rigor.

Analytic Reform Produces Standards But Not a Definition of "Rigor"

Since the surprise foreign terrorist attacks on US soil on September 11, 2001, the US government has focused on improving the credibility of the IC's analytic products. These reform efforts have been designed with the assumption that improving analytic credibility will lead directly to improved consumer trust. One of the first policy efforts to address the credibility of intelligence analysis in response to the 2001 terrorist attacks was the creation of the Intelligence Reform and Terrorism Prevention Act of 2004, which sought to improve the rigor of intelligence analysis.

Informed by this legal precedent, the IC has conceptualized rigor from an output- and compliance-based perspective. Executive Order (EO) 12333 on "United States Intelligence Activities," as amended in 2008, requires analysts to meet rigorous analytic standards in order to assist policymakers in the development of national security policies and the identification of foreign adversaries to the United States, but it does not define what rigorous means or the process of being rigorous. The Intelligence Community Directive (ICD) 203 on Analytic Standards goes on to specify nine assessment criteria—called "tradecraft standards"—that are indicative of a rigorous product.

Like EO 12333, however, ICD 203 neither defines rigor nor the process of how one is rigorous. The ICD 203 standards are focused on outputs of analysis, i.e., the rigor as might be measured in finished intelligence products. The ICD 203 analytic standards are:

- Describe quality and credibility of underlying sources, data, and methodologies;
- Express and explain uncertainties associated with major analytic judgments;
- Distinguish between underlying intelligence information and analysts' assumptions and judgments;

The IC needs to understand the process in order to systematically achieve and improve the output. Hence, understanding the role ambiguity plays in producing analysis is a worthwhile research pursuit for scholarship and for the IC.

- Incorporate analysis of alternatives;
- Demonstrate customer relevance and address implications;
- Use clear and logical argumentation;
- Explain change to or consistency of analytic judgments;
- Make accurate judgments and assessments;
- Incorporate effective visual information where appropriate.

The Office of the Director of National Intelligence *Rating Scale for Evaluating Analytic Tradecraft Standards* provides guidance for evaluating the nine standards in ICD 203, but the rating scale does not define rigor or the process of being rigorous. Measuring the process of being rigorous is much harder than measuring rigor in the output of an intelligence product. Focusing on analytic rigor, like focusing on analytic insight, has emphasized the need for improving an output—the product read by consumers—rather than understanding the process leading to that output. The IC needs to understand the process in order to systematically achieve and improve the output. Hence, understanding the role ambiguity plays in producing analysis is a worthwhile research pursuit for scholarship and for the IC.

❖ ❖ ❖

The author: Adrian Wolfberg is a member of the National Academies of Sciences, Engineering, and Medicine staff, a non-profit organization that provides evidence-based, scientific knowledge to policymakers in the US government. His empirical research work has concentrated on the challenges within large, complex organizations of knowledge exchange between intelligence analysts and senior-level decisionmakers.

Review Essay: Chips, Cyberweapons, and Larceny: Perspectives on Technological Risk

Yong Suk Lee

Chip War: The Fight for the World's Most Critical Technology
Chris Miller (Scribner, 2022), 464 pages, photos, illustrations, map.

This is How They Tell Me the World Ends: The Cyberweapons Arms Race
Nicole Perlroth (Bloomsbury, 2021) 528 pages.

The Lazarus Heist: From Hollywood to High Finance: Inside North Korea's Global Cyberwar
Geoff White (Penguin, 2022), 304 pages.

The revolution in information systems technology during the past 40 years has fundamentally changed how people live and relate to one another. Unfortunately, as with many innovations in history, human beings rapidly weaponized their latest discovery. The pace of innovation in weaponizing the computer-based technologies that form the fabric of our lives is moving as fast as the technology itself. Within 20 years, discussions about cutting edge automation in warfare went from GPS-guided munitions to artificial intelligence, swarms of autonomous drones, and quantum computing. Taken together, authors Chris Miller, Nicole Perlroth, and Geoff White offer a close examination of technological breakthroughs that made the computer revolution possible, how nation-states are competing against one another in a new cyberweapons arms race, and how one country is using these innovations to run a vast criminal enterprise.

Chris Miller, *Chip War*

War, *weapon*, *offense*, and *defense* are words often found in references to cybersecurity and advances in computing technology. Historian Chris Miller would say this is for good reason because, if nothing else, America's wars in the late 20th century provided the testing ground for innovation and spotlights the collaboration between early tech companies and the US military. *Chip War* is a paean to the US tech pioneers, such as Fairchild Semiconductors and Texas Instruments, that founded an industry and revolutionized the world, thanks in part to their Cold War partnership with the Department of Defense (only to later lose their competitive edge to Japan, South Korea, and Taiwan in the global consumer market).

Miller traces the history of a single technological innovation and its impact on modern geopolitical history: the microchip. The late Stephen Jay Gould, a renowned Harvard paleontologist, used the phrase *punctuated equilibrium* to describe periods of rapid change in evolutionary biology after a long period of stasis. This was the case in summer 1958 when a young Texas Instruments engineer, Jack Kilby, came up with an idea to assemble multiple transistor components on a single piece of semiconductor material. He called his invention an "integrated circuit," but it became colloquially known as a "chip." (14) Kilby did not know it at the time but he set the stage for a period of rapid evolution in the nascent computer industry and would receive the Nobel Prize in 2000. Gordon Moore, one of the early pioneering engineers in Silicon Valley, later coined the concept of Moore's Law to describe the exponential growth in computing power every two years that Kilby had unleashed. (15)

A few years after Kilby in 1965, another Texas Instruments engineer, Weldon Word, took on a Vietnam War–inspired challenge of producing a cheap precision weapon for the US Air Force. By 1972, Texas Instruments delivered the Paveway laser-guided bomb. As Miller writes, "Outside of a small number of military theorists and electrical engineers, hardly anyone realized Vietnam had been a successful testing ground for weapons that married microelectronics and explosives in ways that would revolutionize warfare and transform American military power." (60).

Microchips did more than make dumb bombs smart. The same chips made home computers possible, and Moore's Law of faster processing power and cheaper

manufacturing made them affordable. The Internet and email may have started as Cold War–inspired Pentagon programs, but rapid progress in integrated circuit technology brought them into our homes and into our hands. Global chip production and the supply chain that tied them together were beacons of hope for economic integration, with US companies, such as Apple, relying on chips made in Taiwan to be shipped to China to be assembled into devices that are shipped back across the Pacific and around the world. In theory, this level of integration and globalization is supposed to make the world more peaceful, with mutual dependence replacing mutually assured destruction. Today, age-old distrust among nations and political leaders who see their own people as a threat to their rule have formed a wall into which forces of globalization have collided.

When China's President Xi Jinping in 2014 said that "without Cybersecurity, there is no national security," Miller argues that he was not talking about hackers and phishing. (242) For Beijing, cybersecurity meant basic foundational technology that made computers possible. China's growing tech sector relied on data centers made possible only with US-produced components and "even the surveillance system that tracks China's dissidents and its ethnic minorities relies on chips from US companies like Intel and Nvidia." (245) China declared in its Made in China 2025 plan released in 2015 that it will be independent of US and foreign technologies in a decade and all components critical to China's global tech dominance will be made in China, signaling to the world its strategic intent and betraying the leadership's distrust of a Western rules-based economic order. As Miller eloquently argues, "From swarms of autonomous drones to invisible battles in cyberspace and across the electromagnetic spectrum, the future of war will be defined by computing power [and] the US military is no longer the unchallenged leader." (282)

Nicole Perlroth, *The Cyberweapons Arms Race*

As soon as computers and computer-based information management systems became indispensable, they also became vulnerabilities. The 1983 movie *War Games* first showed audiences what this vulnerability could look like, and, even if we are not yet near hackers being able to unleash global thermonuclear war, the ability of a non-state actor to hold a country hostage by threatening to turn off the lights is an ever increasing threat. *New York Times* reporter Nicole Perlroth dives into the dark world of hackers and a thriving underground market for bespoke cyberweapons and tools in *This Is How They Tell Me the World Ends: The Cyberweapons Arms Race*, and what she uncovers is as unnerving as the title of her book.

As military jargons litter the cybersecurity landscape, computer systems and their vulnerabilities borrow heavily from biology, using words such as a worm, virus, and infection to describe attacks against information systems as though they are an assault against the human body. The other term readers will learn from reading Perlroth is *zero-day*. Simply put, a zero-day is a previously unknown computer-software vulnerability an attacker can exploit.

A modern computer program has millions of lines of code and an innocuous error can open the door to a potential attacker. Perlroth shows that from the early days of computing, a select group of people have made a sport of trying to identify zero-day vulnerabilities in programs and operating systems, such as in Microsoft Windows. Some people do it to burnish their reputations within the hacker community, others do it for money and sell their discoveries to the highest bidders. Since the entire world has gone online, the stakes have increased and zero-day exploiters can now command hundreds of thousands of dollars for their discoveries.

For a long-time, the United States was the leader in zero-day exploits. It had the most active computer hacking community in the world, and the US Intelligence Community invested early in exploiting vulnerabilities in computer-based information systems for intelligence collection. This hidden capability came into the light as a new weapon in 2009. Perlroth claims the United States and its allies that year introduced a worm into the computers at the Iranian nuclear facility in Natanz, exploiting four zero-day vulnerabilities in Microsoft Windows. (122–23) Over the next weeks and months, the rotors controlling the uranium enrichment centrifuges spun out of control and wrecked themselves. The Iranians never acknowledged the destruction caused by Stuxnet, as this particular worm later became known. (130) The author quotes Michael Hayden, former director of CIA and NSA, as having said "this has a whiff of August 1945.

Somebody just used a new weapon and this weapon will not be put back in the box." (131).[a]

Perlroth argues the United States, in an attempt to prevent a possible Israeli raid against Iran and preserve peace in the Persian Gulf, crossed the "Rubicon," as she titled one of the chapters in her book. (117) If Perlroth is right, the US and its allies responsible for the operation against Natanz did more than cross the Rubicon against another nation state. She writes that, by the summer of 2010, security researchers around the world started picking up traces of the Natanz worm; the cyberweapon had escaped into the wild. (128) Although never officially confirmed, it wasn't long before intelligence exploits against Iran ended up as front-page news, and Perlroth says this was a wake up call for chief information officers everywhere: they were collateral damage in an escalating global cyberwar. (132)

Perlroth is focused on telling a good story and does not explicitly assign blame, but *This Is How They Tell Me the World Ends* is a harsh critique of the Intelligence Community. Her bottom line is that the US government developed a powerful cyber arsenal, the weapons leaked, and now the entire world is in danger. It is as if the US military lost control of the most powerful bombs in its nuclear arsenal and they are now for sale on the black market. Perlroth starts her book with a claim that "starting in 2016, the National Security Agency's own cyber arsenal—the sole reason the US maintained its offensive advantage in cyberspace—was dribbled out online by a mysterious group" that called itself the Shadow Brokers. The group started "trickling out NSA hacking tools and code for any nation-state, cybercriminal, or terrorist to pick up and use in their own cyber crusades."[b] (xx)

Stuxnet, Shadow Brokers, and revelations of US bulk-data collection have taken a toll on the level of trust between the US government and private industry, when government-industry cooperation is needed the most to defend the country's online infrastructure. Perlorth argues that US tech giants went to war against their own government, prioritizing protection of their users, and distancing themselves from Washington. (227–33) For the firms, this also made good business sense. Microsoft, for example, cannot be seen as cooperating with the US government against another country, and the government for its part lost credibility when it secretly exploited vulnerabilities in US-made computer products for intelligence collection and exploitation, leaving the businesses to scramble to contain the global fallout when these programs leaked.

Geoff White, *The Lazarus Heist*

One country that has benefited strategically from exploiting computer-security vulnerabilities is North Korea, where only a handful of elites go online outside the country's strictly controlled intranet. Geoff White, journalist and former BBC correspondent, chronicles North Korea's unlikely rise as a cybercrime kingpin in *The Lazarus Heist*. White claims what the North is doing in cyberspace is not warfare but larceny. Pyongyang has become the reverse Robin Hood, stealing from poor, impoverished nations to help fund the regime's one-family rule and its spending priorities, such as purchasing luxury goods and investing in its strategic weapons programs. White writes, "Whereas many country's cyber teams are focused on stealing information for strategic advantage, North Korea's online war is part of a battle for economic survival." (7)

There are no shortages of recent North Korean cyber exploits. but the heart of White's book is the breakdown of the attempted heist of $1 billion from Bangladesh's national bank in February 2016. The North's hackers, taking advantage of international time zones and the fact that the weekend starts on a Friday in most Muslim countries, attempted to transfer a billion dollars from Bangladesh's account at the US Federal Reserve in New York to the RCBC Bank in the Philippines. (106–107) In the end, the heist failed purely by chance when the word *Jupiter* raised a red flag. Of the many RCBC branches in Manila, the North Korean hackers picked the one on Jupiter Street as the receiving bank for the wire transfers from New York. It happens that M/V *Jupiter* is the name of a sanctioned Iranian ship and use of the word cost the hackers $951 million, after $101 million had been transferred. (109) Most, but not all, of the transferred funds were later recovered. A Gmail address on a phishing email that hackers used to gain entry into Bangladesh's banking

a. See also Hayden Peake, review of *Countdown to Zero Day: STUXNET and the Launch of the World's First Digital Weapon*, by Kim Zetter, *Studies in Intelligence* 60, no. 1 (March 2016).
b. See also Peake, review of *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*, by Ben Buchanan, *Studies in Intelligence* 64, no. 2 (June 2020).

system, according to the FBI, was also used to phish Sony Pictures Entertainment in 2014, pointing to Pyongyang as the culprit. (118)

It turned out North Korea's attack against Sony Pictures Entertainment for producing *The Interview*, a comedy about two reporters hired to kill the North's leader Kim Jong Un, was just a practice run. Following its failed billion-dollar heist, the North launched the Wanna Cry ransomware attack in 2017, hitting targets like Great Britain's National Health Service. (194–97)

Bottom Line

Of the three books reviewed in this article, *Chip War* is the best-researched and most informative, *They Tell Me This is How the World Ends* is the best written and most entertaining, *The Lazarus Heist* is the weakest. Miller is a historian of Russia by training, and Perlroth and White are journalists who can spot good stories. The fact that the authors are not technicians steeped in the subject matter makes these books more approachable. For IC professionals looking for an introduction to technology and cybersecurity, Miller, Perlroth, and White offer excellent starting points.

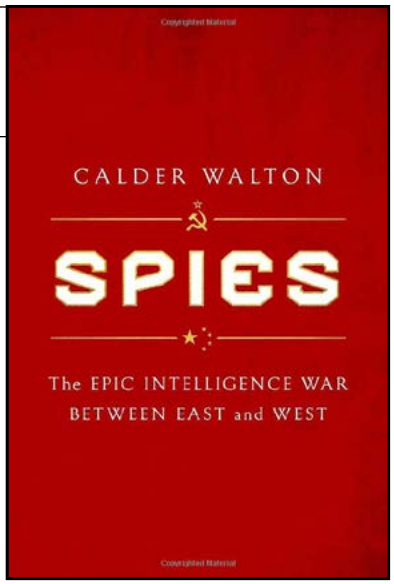
❖ ❖ ❖

The reviewer: Yong Suk Lee is a former deputy associate director of CIA and a visiting fellow at the Hoover Institution, Stanford University.

Spies: The Epic Intelligence War Between East and West

Calder Walton (Simon and Schuster, 2023), 672 pages, notes, index.

Reviewed by John Ehrman



Lucky are the people interested in intelligence history, for they are living in a golden age. Since the mid-1990s, when NSA and CIA jointly released the VENONA documents[a] and other Cold War–era archives began to open, scholars have produced a steady stream of books that have changed the public's understanding of the role of intelligence in international affairs and how, especially, it affected post-1945 diplomacy. The quantity of new material shows no sign of diminishing—memoirs and new releases (whether authorized or not) continue to give researchers plenty to chew on.

Much of this material, however, has been used for limited studies, such as biographies, case histories, or chronicles of individual intelligence services. What has been lacking, and what Harvard-based intelligence historian (and former English barrister) Calder Walton provides in *Spies*, is a book that ties together the histories of the major intelligence services. Walton's contribution is a survey of the development and operations of the Russian intelligence services, and then their competition with British and US counterparts, during the past century. It is a valuable work, but not quite as authoritative as Walton may have hoped.

Walton's major theme is that Western intelligence—first the British and then the Americans and British working (more or less) together—constantly had to play catch-up with Soviet and Russian intelligence. This, according to Walton, was because of deeply rooted differences in national political cultures. For the Soviets, suspicion, conspiracy, and clandestinity were fundamental to the Bolshevik and communist experiences and were integrated into the revolutionary state from its beginning. With these as their roots, the Soviet intelligence services served as instruments of repression as much as, if not more than tools, for collecting information.

Britain and the United States between the World Wars, with radically different political cultures, barely had intelligence services worth mentioning, even as the Soviets undertook hugely successful efforts to penetrate their governments. "On the eve of World War II," says Walton in one of his typically dry observations, "thanks to its Cambridge recruits, Soviet intelligence perversely [employed] more graduates of British universities than Britain's own intelligence services." Not until late in World War II did the UK and the United States realize the scope of the threat and begin to take steps against it.

By the late 1940s, however, Soviet foreign intelligence had passed its peak. It did not become clear until much later, of course, but VENONA-inspired investigations and a wave of defections led to the collapse of the Soviet spy rings. The recruits and volunteers who stepped forward during the next few decades were far fewer in number and lacked the ideological commitment of the Cambridge Five or the Rosenberg ring. Despite occasional successes, such as Geoffrey Prime, the Walkers, and Ames and Hanssen, Moscow never again enjoyed access to the inner circles of the US and UK governments and intelligence communities.

The British and Americans after World War II gradually built large espionage services of their own, but they never matched the Soviets' achievements of the 1930s and 1940s. Still, even without large-scale or top-level penetrations, Walton notes that the United States and the UK acquired valuable assets—especially Penkovskiy and Gordievskiy—who provided critical information. The services of the two countries also proved much more capable than the Soviets of using the information they collected. Unlike the KGB, which had to tailor its reporting

a. Robert Louis Benson and Michael Warner, eds., *VENONA: Soviet Espionage and the American Response, 1939–1957* (National Security Agency, Central Intelligence Agency, 1996), https://cia.gov/resources/csi/books-monographs/venona/

to official ideology and the preferences of the leadership, Western analysts were free to report what they believed. They did not always get it right, to say the least, but American and British leaders were overall much better informed than their Soviet counterparts. Walton especially credits objective reporting and analysis for enabling the US and UK policy decisions of the mid-1980s that led to the relaxation in tensions during the last years of the Cold War.

Meanwhile, and even worse for the Soviets, the British and Americans drew ever closer, especially in technical intelligence. Building on their wartime codebreaking collaboration, the two allies quickly outpaced Moscow's development of computers and satellites, building an essentially insurmountable lead in SIGINT and imagery. Because of London's declining economic and strategic position, Walton points out, much of this was financed by Washington and built with US technology, but Britain still contributed as much as it could afford to ensure that it remained a full partner.

Walton also provides a substantial account of the role of intelligence in East-West political competition in the Third World. When it comes to covert action, he does not like what he sees. The "CIA told anyone willing to listen that it could do the impossible," and politicians in Washington, as well as Moscow, came to believe that covert action could bring successes on the cheap even as the regional actors they sought to manipulate played the two sides against each other. In the end, says Walton, the results mostly "did immense damage to the governments and societies targeted." There is a good point to be made about this, but Walton tends toward oversimplification. Even in the absence of covert action, it is hard to believe that many of the countries on which it was focused—Zaire is of particular interest to Walton—would have done much better.

Returning to his main narrative, Walton chronicles the intelligence services' transitions to the post–Cold War era. Here his point is that little has changed. The USSR disintegrated, but the KGB and GRU continued their intelligence wars against the West and, since 2000, have become integral to Putin's project of avenging the Soviet collapse. The Washington and London, for their parts, assumed in the 1990s that the threat had disappeared along with communism, slashed their services, and turned many of their remaining capabilities to terrorism and other issues. As before, it took some 20 years for London and Washington to realize the scale of Moscow's espionage, hacking, disinformation, and political interference activities. Walton concludes that the use of intelligence to destroy as much as to inform remains as deeply ingrained a feature of Russian political life as ever. Similarly, distorted reporting to the leadership continues to warp Moscow's views and actions, leading to such disastrous decisions as the invasion of Ukraine, as well as to making it impossible for Moscow to trust the West. (Walton is particularly good on the Russian maintenance of its biowarfare establishments because they could not comprehend that the United States truly was destroying its own.) Thus, Walton says, the "West needs to brace itself for a long struggle" against Russian intelligence.

Spies is an impressive and accessibly written synthesis, deeply researched and drawing on the latest releases, intelligence histories, and the growing literature on the Putin era. Walton's overall point—that Russian intelligence for a century has been a continuous, often-underestimated threat—is spot on. Readers with backgrounds in intelligence history will find that they already are familiar with much of what Walton recounts, but his addition of new details and situating of services' behavior and operations in their larger political contexts will make *Spies* worth their time. Moreover, as a history of Soviet and Russian intelligence, it updates Jonathan Haslam's *Near and Distant Neighbors* (2015) and supplements the recent operations described in Gordon Corera's *Russians Among Us* (2020) and Catherine Belton's *Putin's People* (2020). Anyone reading *Spies* along with one of these books will come away with a good understanding of the intelligence battles of the past hundred years.

That said, *Spies* has its share of errors that keep it from being the authoritative book it seeks to be. Most are of a kind common in any intelligence history, the result of reliance on open sources or the flawed memories of interviewees rather than still-classified files. Some are the minor mistakes that happen in books of this length (Yezhov did not get a show trial before his execution, and it was William Casey, not William Colby, who was DCI under Reagan). Others, however, raise questions about Walton's (or his research assistants') familiarity with the details—he mixes up the KGB's and SVR's Directorate T and Line X; Khrushchev may have been poorly educated, but he did know how to write; and the number Walton cites for Congolese killed by Belgians seems at the very

high end of scholars' estimations. The dates in Walton's account of Rick Ames's career are off by half a decade. More unfortunate, he gives Robert Baer's "Fourth Man" theory far more attention than it deserves[a] and includes unnecessary speculation about former President Trump's links to Putin and Russia. The cumulative effect is to make the reader question an otherwise scholarly effort.

Walton closes on a pessimistic note. We are repeating our Russia experience with China—acting late against an underestimated intelligence threat—and he says the West remains badly behind in dealing wth the threat from Beijing's intelligence services. In addition to the obvious threats from industrial, political, and military spying, Walton believes that, as with Russia, ideology and the need to show loyalty to top leaders causes the Chinese services to provide distorted reporting. The chances of a disastrous miscalculation by Beijing, on a scale far greater than Putin's in Ukraine, are high. Given the near misses we had with nuclear disaster during the Cold War, it is a point well worth considering, and another reason to read *Spies*.

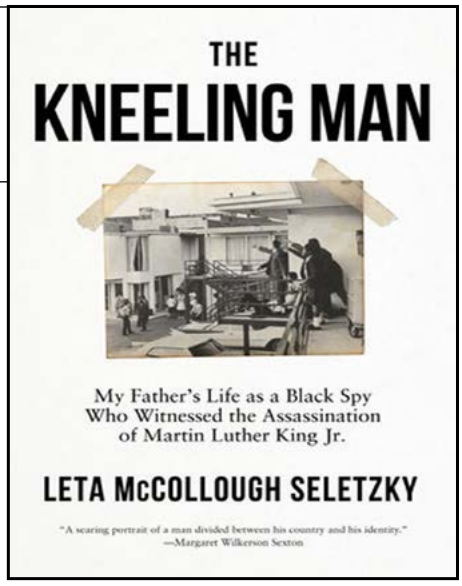
❖ ❖ ❖

The author: John Ehrman is a retired CIA intelligence analyst who has focused on counterintelligence.

a. Robert Baer, *The Fourth Man: The Hunt for a KGB Spy at the Top of the CIA and the Rise of Putin's Russia* (Hatchette Books, 2022) and Dr. Richard Rita, "Review Essay: Former Intelligence Officer Responds to 'The Fourth Man'" in *Studies in Intelligence* 67, no. 1 (March 2023) https://cia.gov/static/3-Response-to-The-Fourth-Man.pdf

The Kneeling Man: My Father's Life as a Black Spy Who Witnessed the Assassination of Martin Luther King Jr.
Leta McCollough Seletzky (Counterpoint, 2023), 304 pages, no index.

Reviewed by Darryl Lansey



In US history, three assassinations have shaken the country to its foundation: President Lincoln's, President Kennedy's, and Dr. Martin Luther King, Jr.'s. All three assassinations changed the trajectory of history and civil rights in America. Dr. King's assassination also changed the trajectory of Marrell ("Mac") McCollough's life. At 6:01 p.m. on April 4, 1968, McCollough's life was transformed from that of an inexperienced undercover police officer into history's "kneeling man," as he desperately tried to save Dr. King, who laid mortally wounded on the second-floor balcony of the Lorraine Motel in Memphis, Tennessee. How McCollough ended up on the balcony kneeling over Dr. King's body, and his subsequent journey to become a CIA employee, is the theme of Seletzky's book.

As McCollough's daughter, Leta McCollough Seletzky's isn't a dispassionate biographer. She is the oldest child from his first marriage. Seletzky was still a young girl when her parents separated. She spent most of her life estranged from her father. *The Kneeling Man* is Seletzky's attempt to tell the story of her father's role in history, his CIA career, and her own cathartic journey to reconnect with him and learn more about his life. Seletzky gives a voice to her father's experiences, while simultaneously reconnecting with him through a series of one-on-one interviews.

Seletzky's story about her father's life is the quintessential American story. McCollough was born in Mississippi at the height of segregation in the early 1940s into a large family of poor sharecroppers. As it was for many Black Americans, McCollough's journey out of Mississippi was via the US Army. He served in the early days of the Vietnam War, though he served as a military policeman (MP) stateside.

In 1967, after his army tour, McCollough exchanged his MP experience for a job with the Memphis Police Department (MPD). He was one of the few Black officers on the force. After McCollough served a brief stint as a patrolman, MPD's Special Operations Division recruited him to be an undercover officer. His first assignment was to infiltrate the Black Invaders, one of several predominantly Black "militant" groups the MPD and FBI were concerned might fuel unrest in Memphis. The day of Dr. King's assassination, McCollough and a few other Black Invaders had come to the Lorraine Motel to meet with Dr. King to discuss how they might help with Dr. King's objectives for the Poor People's Campaign and the trash workers' strike.

By 1972, McCollough believed his five years of excellent work as an MPD undercover and plainclothes officer and the acquisition of a Bachelor's degree in police administration would lead to a promotion. He didn't get promoted as expected. However, according to McCollough, many of his white police academy classmates with less street experience and education were promoted. As a result, McCollough decided he needed to leave the MPD.

A doctor who worked with the MPD encouraged McCollough to apply to CIA, which indeed hired him into its Office of Security. His career with CIA was split between domestic security jobs and overseas assignments supporting operational activities. Dr. King's assassination haunted McCollough throughout his CIA career. Congress subpoenaed him in 1978 and 1998 to testify about Dr. King's death, including efforts to debunk multiple conspiracy theories about the assassination and McCollough's possible role.

As a biographer, Seletzky is emotionally attached to her father's recollections. This is evident as she conveys his CIA accomplishments, including his successful efforts

to recruit more than 60 Blacks into the security profession. Her emotional attachment is also clear when discussing her father's principal career disappointment when CIA denied him a promotion into the Senior Intelligence Service. According to Seletzky, her father believed he ran afoul of the CIA system as he pressed it to do more about the recruitment and retention of Blacks and other employees of color.

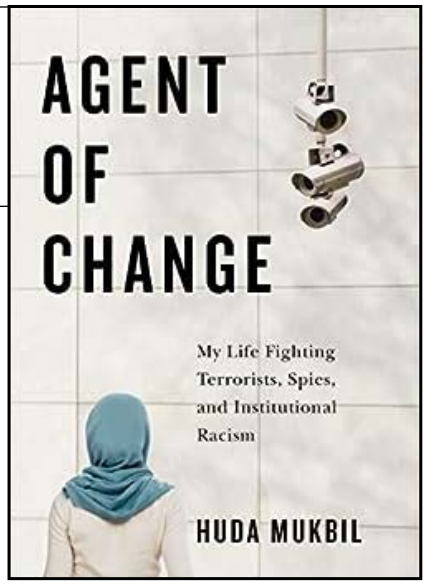
I enjoyed reading Seletzky's book. Although I was only six years old when Dr. King was assassinated, his death is seared into my memory. Seletzky, with the help of her father's firsthand account, brings to life one of the darkest days in US history in ways only a few other people could have done. Some readers may, as I did, feel a bit whipsawed by Seletzky's writing style. It jumps back and forth between the past and present as her father, and others like Ambassador Andrew Young, recalled Dr. King's assassination decades later. Additionally, there are times when Seletzky spends significant time exploring her journey to reconnect with the father she never knew, and her own thoughts about race relations in America. In both cases, these felt more like asides rather than critical elements of her father's story. Overall, I would recommend the book as an interesting addition to a reader's historical nonfiction collection.

❖ ❖ ❖

The reviewer: Darryl A. Lansey is a retired CIA officer and author of the memoir, *A Thin Line Between Love and Hate: A Black Man's Journey Through Life and the CIA* (Bookbaby, 2020).

Agent of Change: My Life Fighting Terrorists, Spies, and Institutional Racism

Huda Mukbil (McGill-Queen's University Press, 2023), 238 pages, photos, abbreviations, prologue, afterword, acknowledgments, notes.



Reviewed by Joseph W. Gartin

Huda Mukbil's *Agent of Change* is an affecting account of her experiences as—in her words—the first Black, Muslim, female intelligence officer in the Canadian Security Intelligence Service (CSIS). The identifiers are important, not least as a multilingual immigrant whose family fled Ethiopia and eventually Egypt in search of safety before arriving in Montreal in November 1987. As the book's title suggests, Mukbil's background is also central to her story as a pathbreaking intelligence officer who found success but also formidable challenges trying to forge a career in the face of systemic discrimination.

Mukbil became a Canadian citizen in 1990 and graduated from Carleton University in June 2000. Encouraged by a professor, Mukbil applied to CSIS and entered on duty in February 2002. In those fraught months after 9/11, CSIS was grappling with how to fill its ranks with intelligence officers (IOs) who had the requisite language, cultural, and regional expertise needed to deal with the threat from Islamic extremism. CSIS had been formed in 1984 from elements of the Royal Canadian Mounted Police, and its ethos reflected a strong orientation toward law enforcement and a distinct lack of diversity. (66) Mukbil would find herself in a kind of no-woman's land: at once valued and distrusted because of her ethnicity, race, faith, and gender. The 9/11 attacks in her view had "racialized being Muslim," forcing Mukbil to defend her "religious identity and to categorize [herself] as a moderate Muslim opposed to political violence." (57–63)

This insider-outsider dichotomy would permeate Mukbil's experience in CSIS's IO Entry Training. In what she describes as the most diverse CSIS class since the service's formation in 1984, Mukbil would be commended for her, expertise and language skills, and yet continuously reminded of her otherness: "In our CSIS data search exercises, analysis, and findings, it was a racialized Muslim that we were trained to investigate. When given examples on how to conduct searches on the bulky computers of the nineties, names used during exercises were, more often than not, Middle Eastern names like Mohammed and Ahmed." (68)

Mukbil was assigned to CSIS's counterterrorism unit to work on Sunni extremism. Her sense of being both an insider and an outsider would be shaped by multiple factors, including her success working on CT issues, the US invasion of Iraq, the arrest in New York and rendition to Syria of Canadian-Syrian citizen Maher Arar, and her own faith journey as a Muslim woman in a distrusting organization. Her decision to begin wearing a hijab was personally important and professionally fateful: "The culture was deeply conformist and intolerant, and I was an unprepared fool." (101)

In the years that followed, Mukbil served with distinction as a seconded officer in London after the terrorist bombings in July 2005 and was posted to Toronto as an investigator, but she would find herself repeatedly shunted aside, assigned to "backwater" projects, (154) passed over for desirable assignments, and confronted with pervasive prejudice. A colleague advised that to advance, Mukbil "needed to demonstrate [her] loyalty." (186) By December 2016, overlooked once again for an important job, Mukbil reached a breaking point and initiated a lawsuit against CSIS—later joined by colleagues in a process that would last more than a year and play out in the courts and media. The final 20 pages of *Agent of Change* rush to a conclusion, thanks to nondisclosure agreements, (226) but the reader is left with little doubt about the challenges Mukbil experienced or her courage confronting them.

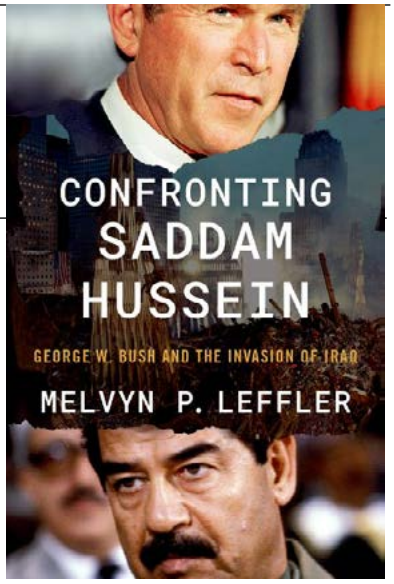
❖ ❖ ❖

The reviewer: Joseph W. Gartin is the managing editor of *Studies*.

Confronting Saddam Hussein: George W. Bush and the Invasion of Iraq

Melvyn P. Leffler (Oxford University Press, 2023), 346 pages, preface, acknowledgments, notes, bibliography, index.

Reviewed by Michael J. Ard



In *Confronting Saddam Hussein*, distinguished Cold War historian Melvyn Leffler delivers a balanced and penetrating analysis on why President George W. Bush took the United States to war in 2003. Leffler relies on numerous interviews with key participants to supplement his careful examination of the written record. This new history will satisfy anyone interested in a compact and dispassionate treatment of what brought the United States to war and why it went awry.

The book dispatches various theories that Bush was motivated by avenging his father, or religious zeal, or manipulation by neoconservatives. What we see instead is a president beset by daunting foreign policy challenges, knocked off kilter by the 9/11 attacks, and uncertain of his overall strategy in coping with Iraq. Leffler's narrative skil

lfully delineates the uncertainty and difficult trade-offs the Bush administration faced on how to secure America and defend our commitment to collective security. Although evenhanded, this book offers no apologia for the Bush administration's handling of the invasion and occupation of Iraq.

Leffler sees the key drivers to war as fear, power, and hubris, which may have underlaid the causes of the war, but they did not make war inevitable. Leffler centers this story on the calculations and will of two presidents, Bush and Iraqi President Saddam Hussein. Ultimately, they each made crucial decisions that made the war happen. Both had opportunities to take another course that might have avoided the war.

One of the book's strengths is describing the mounting psychological pressure Bush and his administration faced in the aftermath of 9/11. They were beset daily by a lengthy and alarmist "threat matrix" on possible terrorist attacks (a "god-awful idea," said presidential briefer Michael Morell), (68) and FBI Director Robert Mueller's warning of 300 potential terrorists in the United States. The unsolved anthrax attacks that began on September 18, 2001, (letters containing anthrax were mailed to prominent politicans and US media outlets, killing five and infecting 17 others) raised the stakes for resolving ongoing Iraq challenge, which the administration viewed as getting out of control. No wonder that when the administration announced the Global War on Terrorism, it did so with the phrase, "our way of life is threatened."

Bush feared underestimating a looming threat again. Therefore, his administration concluded it could ill afford business as usual with Iraq, given its reputed weapons of mass destruction program, flouting of numerous UN Security Council resolutions, and long-established links to terrorist groups. A point Leffler might have made was that the West had been in a quasiwar with Iraq since 1991, with the country under heavy economic sanctions and with two-thirds of its territory declared no-fly zones enforced by the United States and United Kingdom.

Besides investigating causes, Leffler attempts to dispel numerous misconceptions that have since dominated interpretations of this tragic episode. For one, Leffler portrays a US president firmly in charge of his cabinet. Bush, as Leffler makes clear, also did not believe Saddam was behind 9/11, nor did his cabinet members. Moreover, neither he nor his cabinet entertained grand designs to remake the Middle East in a democratic image, at least not in the beginning.

Leffler also stresses the policy continuity from one administration to the next on Iraq; Congress passed and President Clinton signed the Iraq Liberation Act in 1998.

Both Republican and Democratic politicians insisted that Saddam Hussein had to go. Despite this commitment, Leffler argues the Bush administration had no plan to attack Iraq before or immediately after 9/11; there was no rush to war. Far from a portrayal of a single-minded, determined government, we find instead an administration buffeted constantly by conflicting viewpoints and independent information flows. As this account makes clear, the Bush administration in many ways was making up Iraq policy as it went along.

Ironically, given the longtime Iraq focus in Washington, the poor mechanics of US foreign policy making comes through. The administration suffered from the opposite of groupthink—instead, key advisers were querulous and divided. Bush, although in charge, was besieged by numerous different opinions on what to do. Important nodes like the IC, the Office of the Vice President, the State Department, and the Office of the Secretary of Defense offered their own perspectives on information. The overwhelmed NSC failed to achieve policy consensus. Perhaps as influential as even his closest advisers, British Prime Minister Tony Blair, who shared Bush's disdain for Saddam, convinced Bush to push for more WMD inspections and a new UN resolution.

This organizational breakdown led to significant fundamentals being ignored, such as how the United States would manage the aftermath of the war. There was poor coordination on the Future of Iraq project between State and Defense—a massive failure, concludes Leffler. A report on the widespread looting and disorder that broke out after the US invasion of Panama in 1989 went unheeded. Secretary of State Powell himself, according to Leffler, could not pinpoint when Bush made Iraq the central focus. (96)

Like the Enron Corporation, which filed for bankruptcy around that time and whose leadership was famously dubbed "the smartest guys in the room," the Bush administration featured a team of highly capable, experienced people who worked in their own information siloes and whose risk management capabilities were sorely lacking.[a] Ultimately, the sum was much less than its parts.

But they were united in their concept of US power as a force for good. In 1998, Secretary of State Albright said America "stands tall and sees farther into the future than other countries."[b] This bold declaration of the fundamental righteousness of America found a willing adherent in President Bush. Coupled with self-righteousness may be a tincture of US naiveté about the world. Puzzling over the 9/11 attack, Bush mused, "I'm amazed that there is such misunderstanding of what our country is about, that people would hate us … like most Americans, I can't believe it, because I know how good we are." (74)

Still perplexing is the lack of debate in the Bush administration on how the country had fared in similar wars of national policy. The Korean War damaged the Truman presidency, and the Vietnam War Johnson's. Did Bush and his advisers not seek any lessons from these tragic histories? As the crisis grew, Bush increasingly saw war in grandiose terms, to not simply end the Iraqi threat, but even reshape the entire Middle East. Once again, "Hubris" has taken its role on the stage.

Bush's embrace of US power and desire to expand freedom probably did not prompt him to assess the cost of an invasion. He asked US Central Command Commander Gen. Tommy Franks, can you win? But he never asked, what will come next? Leffler cites as a huge failure CENTCOM not focusing on Phase IV—the occupation after main combat operations in Iraq—a policy neither Franks nor his boss Defense Secretary Donald Rumsfeld seemed to care about. (207–208)

The IC likewise bears its share of the responsibility. An avid consumer of intelligence, Bush appeared to understand its limitations. Often forgotten is that before CIA Director George Tenet said, "It's a slam dunk," Bush had asked, "Is that all you've got?" Cheney may have challenged CIA on the al-Qa'ida connection, but "intelligence analysts," Leffler concludes, "were not bullied or intimidated." (157) Leffler, guided mostly by the 2005 Robb-Silberman Report, concludes the White House did not press intelligence analysts to make different conclusions. Leffler avoids chasing red herrings like the purported uranium yellowcake from Niger or the fabricated reporting from the infamous Curveball source, which never influenced decision-making.

a. Bethany McLean and Peter Elkind, *Smartest Guys in the Room* (Portfolio Trade, 2003).
b. Madeleine Albright, interview on NBC-TV "The Today Show" with Matt Lauer, Columbus, Ohio, February 19, 1998, as released by the Office of the Spokesman, US Department of State.

But some key intelligence admittedly was weak, with reporting on WMD coming from Kurdish opposition groups. Still, all decisionmakers thought Saddam Hussein had WMD, even relative doves like Powell and his deputy Richard Armitage; and key foreign partners concurred. One senior adviser noted, "Nobody told Bush that Hussein did not have WMD." No IC product or briefing doubted the reality of Saddam Hussein having a WMD arsenal. Although the 2002 Iraq National Intelligence Estimate exaggerated the threat, it was restrained compared to the intelligence reporting the principals were used to seeing.

Although ill-served by the IC, the chief policymakers never questioned their own assumptions or seriously challenged the reporting. In the end, it all boiled down to the "decider," and Leffler is incisive in describing the administration's contradictory policy of containing Iraq and overthrowing Saddam. Washington wanted Saddam's cooperation on WMD while openly demanding regime change. Leffler cites an interview in which Bush said Saddam needs to go, and that Baghdad also must let inspectors return. 117–18) The diplomacy advocated by Condoleezza Rice was long on coercion but short on diplomacy. Meanwhile, Saddam Hussein, far from yielding to threats, grew more defiant. When he could not be cajoled into changing his behavior, "US credibility itself" became at risk. (173)

In the end, the Iraq war, which started out with strong US public support, came at great cost: some 4,400 US and coalition military dead, at least 110,000 Iraqi killed (at the lower end; estimates vary widely), $2 trillion expended, and US confidence and prestige badly damaged. Fear, power, and hubris overcame sound process, clear thinking, and prudential wisdom. This is a damning verdict by Leffler, and largely accepted wisdom today, but perhaps future historians will make a more refined judgment. By going to war, Bush administration defended an important ideal—the concept of collective security as enshrined in the UN charter—as only the United States was capable of doing. The war put an end to a significant and persistent security threat of WMD in the Middle East. Saddam was removed from power, and Iraqis—especially the Shias and the Kurds—were offered a legitimate chance to forge their own political futures. These evident benefits should be weighed along with the high costs.

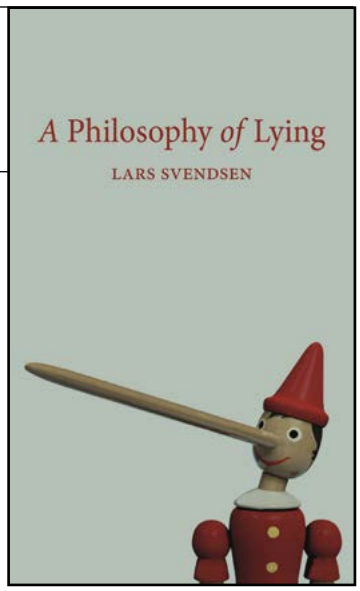
❖ ❖ ❖

The reviewer: Michael J. Ard is a former CIA officer. He is now a professor at Johns Hopkins University, where he directs the master's of science in intelligence analysis program.

A Philosophy of Lying

Lars Svendsen, Matt Bagguley (trans. from Norwegian) (Reaktion Books, 2022), 122 pages, notes, index.

Reviewed by Mike R.



A Philosophy of Lying bills itself as a "comprehensive investigation of lying in everyday life." The intelligence profession is not under the microscope, but the book raises a number of issues that practitioners might find worthy of further reflection or exploration. While the author has occasional missteps, his material could easily form the basis for discussion in an intelligence-themed TED Talk or classes on intelligence ethics or leadership.

The author, Lars Svendsen, a philosophy professor at the University of Bergen in Norway, is not as well known to US readers as fellow Scandinavian Sissela Bok, the Swedish-American famous for her award-winning 1978 work, *Lying: Moral Choice in Public and Private Life*. But what Svendsen lacks in name recognition, he makes up for in delivering a product readily accessible to the lay reader. Although Svendsen might have felt obliged to infuse the slim volume with serious citations for the sake of his academic reputation, he clearly wanted to make it enjoyable for a wide audience. *A Philosophy of Lying* would be as much at home at the beach or in a college seminar. He plays to modern sensibilities by calling upon plenty of nontraditional figures, including, on the small screen, the animated character Homer Simpson and *Mad Men* protagonist Don Draper.

While the author conveys a range of views on lying as expressed by luminaries across the ages, he makes clear his own sentiment right from the start. Svendsen believes lying is wrong but understands the need for exceptions; likewise, he advises—for one's mental health and our ability to live in a society—acting as if everyone is telling the truth even though it can lead to disappointment. "[You] are wise to mostly assume that people are telling the truth for the simple reason that in general they do. You will be fooled every now and then, but it is better to be fooled occasionally than to go through life with a chronic distrust of other people." (11)

The book roughly divides into two parts. The first half is definitional and foundational, the second more practical. In the opening "What is Lying?" Svendsen establishes "truthfulness"—requiring both accuracy and sincerity—as the gold standard. He places three concepts on the opposite side of the ledger, of which lying is just one.

- "Truthiness," the 2005 "Word of the Year" associated with comedian Stephen Colbert, is one of lying's key compatriots. Gut feelings overrule facts and logic: "The idea is that if something *feels* true, then it is true." (16) In a "truthy" world, one can never pin down the truth; its notion is meaningless.

- A close relative is "bullshitting." Whereas lying deviates from truthfulness in its lack of sincerity, and truthiness in its lack of accuracy, a bullshitter simply does not care. Drawing on examples from *1984*'s Winston Smith toiling away in the Ministry of Truth to former President Donald Trump, the author notes that sometimes the truth is irrelevant; whether objectively true or false, what matters more is the effect.

- Having dispensed with two legs of the tripod, Svendsen settles on lying as the more interesting subject to pursue, describing it as follows: "To say something you do not think is true in a context where others can reasonably expect you to be telling the truth." (30)

"The Ethics of Lying" is the book's most academic chapter, a sort of "Philosophy 101" that readers can skip over or skim with little impact to their enjoyment of the rest of the work. While missing an opportunity to reference an obvious humorous touchstone in the form of the 2009 movie *The Invention of Lying,* starring Ricky Gervais as the first person to develop the ability to fib in a world of otherwise brutal honesty, Svendsen makes clear that not even the great German philosopher Immanuel Kant was as dogmatic as frequently portrayed. Despite

professing a duty to be truthful, "Kant believes that we are not always obliged to convey our innermost thoughts. If we always said exactly what we were thinking, we would find each other unbearable." (41) Fans of former Director of Central Intelligence Allen Dulles, whose fondness for a certain line from scripture wound up etched in stone at CIA's Headquarters, will also feel on familiar ground when Svendsen closes out the chapter by speaking, in his own words, of truth's critical role:

> *If I lie to you, then I am blocking your access to reality and this applies to both white and black lies. By doing so, I am depriving you of your freedom. No matter how much goodwill my white lie is based on, I am denying you an insight you could have gained from your surrounding or from yourself. The truth could have set you free.* (57)

The second half of *A Philosophy of Lying* applies the subject's central tenets to a few particular facets. "Lying to Yourself" raises unstated but obvious questions for operational practitioners, and all those not at liberty to freely disclose their intelligence affiliation, of whether one can be true to oneself if so much of one's life involves telling lies to others. Does leading a double life lead to self-deception? The author cites La Rochefoucauld: "We are so accustomed to disguise ourselves from other people, that in the end we disguise ourselves from ourselves." (71) Svendsen asserts that the more one lies, the "more inclined to believe that what you are saying is true." (72)

He relates self-deception concerns to our consciences as well, citing the extreme case of Lt. William Calley of 1968 My Lai massacre infamy during the Vietnam War. Calley was shocked to be charged with mass murder when he thought he was being a good soldier: "It couldn't be wrong or I'd have remorse about it." (67) Can intelligence officers called upon to break other nation's laws in the performance of their duties be counted on to be scrupulously aboveboard at home? It is a tall order, yet that is exactly what is asked and expected of these professionals.

"Lies and Friendship" might strike a chord with anyone who has ever wondered, "Did I just get 'case officered'?" What happens to one's relationship when the other party is deemed a fraudster? According to the author, "Friendship is entirely conditional on there being mutual trust. If you don't trust other people or they don't trust you, friendship is impossible." (74) It puts an interesting spin on that survey question that was once a litmus test of an organization's health: "Do you have a best friend at work?" Without ever saying "need-to-know," the tensions in requiring colleagues to limit what they say to each other are brought to the surface as well. Both parties must be open with one another, Svendsen argues; sharing secrets, rather than keeping them closed up, should be the rule. But for those hoping for a clear way forward, he can only acknowledge the difficulty:

> *A secret is shared on the condition that it isn't passed on, but what do you do if you seemingly have to choose between revealing the secret or lying to someone else? You would obviously experience a conflict of duty, and I don't think the problem has a general and satisfactory answer.* (75)

The friendship conundrum has a special resonance for those in the business of asset recruitment. To the degree that one adopts false pretenses to achieve an objective, there is a risk that it can all come crashing down. Svendsen calls upon research showing that the more an individual realizes that they have been deceived, the greater the severing of a connection that will occur with their deceiver:

> [The] *better the fraudster played the role, the more provoked we are, because it weakens the connection we initially assume exists between someone's right and ability to play a role. In short: it weakens the trust we have that someone really is who they are presenting themselves to be. This is especially upsetting when someone has played the role of your friend.* (74)

It is one thing for an intelligence officer to feign interest in a sport or hobby to sidle up next to a target. But what is the reaction when things go awry—as they inevitably do from time to time—upon finding out that an alias was being used; that one was not from their purported organization; or that they hailed from a different country? Is it safe to discount the impact of tactical lies told in the name of strategic truth, or will they always come at a cost, even when things go well?

Svendsen's largest chapter, "The Politics of Lying," focuses on the nation-state level, where the microcosm of individual lying takes on macro overtones. He begins by quoting someone close to home, a former Norwegian leader: "Sometimes a prime minister has not only a right but a duty to lie." (83) And although he does not dwell on deception, per se, he highlights the famed Italian author

of *The Prince*, Niccolò Machiavelli, as among those claiming that "in politics one must always be prepared to lie and deceive when it is to one's advantage." (85) The author sees such behavior often aligning with Max Weber's ethics of responsibility, acknowledging that at times one has to break the rules for a higher purpose: "For Weber, the 'responsible' politician is someone who acts immorally and feels burdened by it." (90) In other words, lying is sometimes necessary, but the individual should at least feel a tinge of guilt.

Looking at societies where lying has become commonplace, Svendsen cites a World War II–era writer who served as inspiration for famed author Hannah Arendt: "The totalitarian regime is based on the primacy of the lie." (91) Whether speaking of Nazi concentration camps or life under the grip of the Soviet Union, reality becomes blurred through efforts at state control, and a "giant echo chamber" is created. (93) Turning to contemporary Russia, Svendsen opts for understatement, describing Putin as having "a relaxed relationship with the truth." (104)

In a subsection on "Lying in Modern Politics," the author points up assertions by President Jimmy Carter who said that he would "never tell a lie," (96) and notes that President George Washington continues to be revered for similar mythical professions about cutting down a cherry tree as a child. Virtuous as these attributions may be, Svendsen relates, both proved false. The cherry tree episode reportedly was planted by an early Washington biographer who plagiarized it from a Scottish work. President Carter's press secretary Jody Powell admitted lying was in fact necessary at times in the White House, such as in the case of not revealing military plans to attempt to rescue American hostages held in Iran in 1980.

Svendsen also raises several topics with an intelligence or national security connection that unfortunately leave the reader in need of a saltshaker to temper the findings. He claims, for instance, that "there's no doubt that the Bush administration lied to justify the invasion of Iraq." (97) But one of the argument's two pillars, a supposed relationship between Saddam Hussein and Usama bin Laden, even though embraced by some, did not underpin the ultimate US rationale for going to war, and the intelligence never supported such a strong assertion. The other pillar, claims of Iraqi weapons of mass destruction, contravenes his own logic; writing elsewhere in the book that to qualify as a lie one has to consciously assert something known to be false, it is hard to see how a belief then widely held by the White House (and numerous allies), even though subsequently proved false, could be considered lying.

The author takes liberties as well in citing the September 1941 engagement between the destroyer USS *Greer* and a German U-boat to show that the US commander-in-chief lied about German actions for ulterior motives. While there were questions over what exactly happened, paralleling the later 1964 Tonkin Gulf incident leading to stepped-up US involvement in Vietnam, to say that "Franklin D. Roosevelt lied to the American people in order to ensure the United States' participation in the Second World War" oversimplifies a more complex and nuanced event. (99)

Svendsen also writes of "playing the national security card" when the underlying motive is seen to be something else. In the classic example of Watergate, he speaks in general terms of President Richard Nixon's efforts to "cover up incompetence, corruption, or some other criminal act," yet curiously omits reference to Nixon's specific attempt to enlist CIA to block an FBI investigation by claiming national security was at issue. (101) From the same era, he describes the Pentagon Papers episode as one of secrecy "not so much to prevent the enemy from acquiring knowledge as it is to stop its own population from getting it." (90) While both incidents involved the intersection of politics, the law, and claims of national security, omitted is the fact that in one of these classified information was at stake. Nonetheless, a sullied history in this regard leads Svendsen to call into question the degree to which a populace can trust that its leaders are being truthful; "How can citizens know that a government with the option to lie does so only when national security is at stake?" (103)

Closing out his work, the author returns to themes of the pervasiveness of lying and of lie detection. Studies would have us believe that lying is rampant, occurring in some 25 percent of all our interactions, yet he writes that this is misleading. The average is heavily skewed: "A minority are responsible for most of the lying, while the majority account for very little of it." (115) And because most people speak the truth and expect it in return, liars can be enormously successful taking advantage of this predisposition.

Is there a way, then, to take steps to ensure one is not being lied to? Svendsen dismisses most techniques or "tells," such as the avoidance of eye contact, arguing that the behaviors speak more to perceived trustworthiness—a separate issue from being a liar or a truth-teller. While acknowledging some correlation between lying and voice modulation and eye dilation, even this slight benefit is for naught in the bigger scheme of things:

> *People who are trained to expose liars get slightly better at identifying them, but at the same time they become slightly worse at identifying people who are telling the truth, which makes them no more accurate in general. It is tempting to say that their training hasn't made them experts at distinguishing between honest and dishonest people, but has simply made them more suspicious.* (116)

❖ ❖ ❖

The reviewer: Mike R. is a member of the CSI History Staff.

❖ ❖ ❖

Further Reading

Joseph Gartin, review of *Through a Glass Darkly: The Ethics of Intelligence and Counter-Intelligence*, by Cécile Fabre, *Studies in Intelligence* 67, no. 1 (March 2023).

John Harington, review of *Secrets: On the Ethics of Concealment and Revelation*, by Sissela Bok, *Studies in Intelligence* 28, no. 2 (Summer 1984).

John P. Langan, S.J., "National Interest, Morality, and Intelligence: Search for Reconciliation," *Studies in Intelligence* 27, no. 3 (Fall 1983).

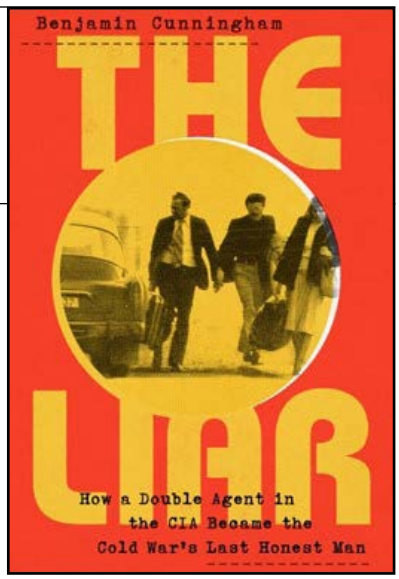
———, review of *Secrets: On the Ethics of Concealment and Revelation*, by Sissela Bok, *Studies in Intelligence* 29, no. 2 (Spring 1985).

David Robarge, review of *Fair Play: The Moral Dilemmas of Spying*, by James Olson, *Studies in Intelligence* 51, no. 1 (March 2007).

The Liar: How a Double Agent in the CIA Became the Cold War's Last Honest Man

Benjamin Cunningham (Public Affairs, 2022), 268 pages, endnotes, photos, index.

Reviewed by Graham Alexander



Karel Koecher holds the dubious distinction of being the only known Eastern bloc operative to successfully infiltrate CIA through a seeding operation. Former correspondent Benjamin Cunningham recounts this incredible story in *The Liar*, detailing many of the case's most significant milestones and showing how the amoral, louche, and often cantankerous Koecher succeeded where so many others failed.

Cunningham is an obviously skilled writer and, despite his lack of intelligence experience, he reveals a surprisingly sophisticated comprehension of intelligence tradecraft.[a] His brisk, highly readable account burns most brightly in the early chapters, where Cunningham weaves details of Koecher's life together with the main plot-points of Central Europe's turbulent mid-twentieth-century experience. Frustratingly, Cunningham is unable to maintain this high standard throughout the work when his narrative compass spins in multiple, competing directions. Political opinions, historical analysis, personal animosity, and an ironic personal affinity for Koecher all elbow for copy in highly limited space. They prevent Cunningham from coaxing the full payout for what might have been a more balanced review of a complex, often fascinating espionage story.

Cunningham breaks cleanly from the blocks with a cliffhanger opener detailing a portentous 1976 meeting between Koecher and KGB Colonel Oleg Kalugin at a safehouse just inside the Czech border with Austria. Events then skip back into Koecher's early life where Cunningham persuasively details how the collapse of the Hapsburg monarchy, Germany's 1939 annexation of most of Czechoslovakia, and Czechoslovakia's transformation into a Soviet satellite shaped Koecher's personality.

Closer to home, Koecher's cynicism and libertinism feel like logical, even inevitable, responses to the shifting loyalties that marked Czechoslovak society and the often spittle-laced remonstrations of Koecher's devoutly Catholic father. Cunningham avoids the trap of armchair psychology while still painting the picture of a man whom the reader believes is ready to sell his services to the intelligence war, albeit less on behalf of the workers of the world than his own unbridled ambitions.

Scene-setting complete, Koecher's move to the United States in December 1965 with instructions to penetrate the US national security apparatus constitutes the drama's main act. Incredibly, this often dilettantish, incorrigibly venal agent succeeds in obtaining US citizenship, passing a polygraph examination, and by 1973, beginning translation work as a CIA contractor. Cunningham recounts various parts of this story using interviews from Koecher and a smattering of other sources, including often unsourced details from Czechoslovak intelligence archives.

Frustratingly, Cunningham does not dwell at sufficient length on the case itself. Details on the wider world of politics were useful in understanding Koecher's formative years but, too often in later chapters, Cunningham meditates unnecessarily on various world events and US presidents whose policies he variously critiques or praises. The trend culminates with the final disintegration of the fourth wall as Cunningham recounts his impressions of

a. See also Hayden Peake's brief review in the Intelligence Officer's Bookshelf, *Studies in Intelligence* 66, no. 4 (December 2022). For a broader historical perspective, see Cleveland C. Cram, *Of Moles and Molehunters: A Review of Counterintelligence Literature, 1977–92* (Center for the Study of Intelligence, 1993), available at https://cia.gov/resources/csi/books-monographs/of-moles-and-molehunters-a-review-of-counterintelligence-literature-1977-92/.

Koecher's home during their interviews, and their discussions on social issues and US elections. His unconcealed disdain for Kalugin, whom he sheepishly admits avoided him by providing a false phone number, also suggests Cunningham wants to cast heroes and villains.

The ultimate verdict on *The Liar* is that it is a solid, usually entertaining, account of a case that could have been so much better. The epic sprawl of Koecher's story begs for an even more detailed examination weighted more evenly among its main protagonists, several of whose stories are equally dramatic. The reader understands well how Koecher came to work in the world of espionage but much less so the drivers behind the sometimes unpredictable turns in the case. Cunningham desperately needs, for example, better sourcing from FBI, KGB, and Czechoslovak intelligence to widen the aperture and to verify Koecher's sensational, self-serving claims.

In the final act, Cunningham cannot resist the temptation for a verbal flourish by recalling how, on the night before his 1984 arrest, both Koecher and his wife "went down swinging" with a local couple. How much more worthwhile would *The Liar* have proven, however, had it eschewed word games and, perhaps, even weighed this lifestyle among the variables that explained Koecher's often astonishing espionage career?

❖ ❖ ❖

The reviewer: Graham Alexander is the pen name of a CIA officer.

Marianne Is Watching: Intelligence, Counterintelligence, and the Origins of the French Surveillance State

Deborah Bauer (University of Nebraska Press, 2021), 360 pages, photos, illustrations, appendix, index.

Reviewed by John Ehrman

Pop quiz: Which country invented the modern, professional intelligence service? Was it Germany, with its highly developed military staff system and master bureaucrats? Russia, needing information to thwart anti-czarist revolutionaries? Or Britain, fumbling around as usual and coming up with a workable solution by accident?

The answer is none of the above. It was France that after its disastrous defeat in the Franco-Prussian War (1870–71) realized that collection of accurate information about potential adversaries in general, and Germany in particular, would be critical to national security and military success. How the French created their service, the problems they ran into, and their long-term consequences are the subject of historian Deborah Bauer's *Marianne Is Watching*.

Bauer starts with a review of the origins of French intelligence. Beginning with the ancien regime and Napoleonic eras, she traces the emergence of French intelligence as an internal police function. In the 1830s, when France took over Algeria, the military confronted the need to "understand and classify both the land and its population." (31) The French saw the usefulness of such information and were beginning to develop a basic peacetime military intelligence system and spy networks under Napoleon III but, alas, did not have it in place before the 1870 war.

As part of its reorganization after the defeat and founding of the Third Republic, the French army staff established what proved to be the first of the professional intelligence services we know today—that is, one on a permanent bureaucratic footing, staffed by professionals, and collecting and archiving information for long-term use. It took several years and additional reorganizations, but by the mid-1870s the army's Deuxieme Bureau had emerged, with responsibility for conducting intelligence collection and analysis (*renseignement*) essentially as we understand it today. Its role, writes Bauer, was to "analyze, synthesize, and disseminate information collected … through a number of avenues: from military sources like officers on mission, military attaches, agents … as well as from nonmilitary sources" that included the foreign press and exchanges with other countries' attachés. (53) Bauer's descriptions of the bureau's organization, staff, and operations—and especially those of the Statistical Section, which ran agents and later expanded into counterintelligence and counterespionage—also show it to have been a sophisticated outfit, instantly recognizable in form and function to any 21st century intelligence officer.

It is not surprising, then, that the French ran into some familiar problems. The Deuxieme Bureau had to work with civilian police agencies, which had intelligence roles of their own, and the Foreign Ministry, which was especially strong on cryptanalysis. Things did not always go smoothly. Bauer recounts how, despite their codebreaking successes, the services did not cooperate on cryptanalysis, "thus hampering [France's] ability to take advantage of technical breakthroughs," while politicians leaked information from decryptions and "further thwarted cryptanalytical effectiveness." (82)

Gradually, however, the Deuxieme Bureau emerged as the leading agency in the nascent French intelligence community and began taking over internal security roles. This was especially so in counterespionage, which traditionally had belonged to the civilian police. The Bureau and Statistical Section became increasingly powerful and autonomous, with direct and unsupervised access to top government ministers. Catastrophe followed, says Bauer, as "it was this privileged relationship, as well as the lack of checks and balances on a service that itself was never

actually defined by any written code" that led to the Dreyfus Affair. (91) Nor are these problems completely in the past. Bauer concludes by noting that French intelligence remains dominated by a military culture that downplays analysis in favor of confirming policymakers' preconceived ideas.

Turf battles and legal ambiguities are not the only aspects of intelligence work that readers will recognize. French intelligence collection had to respond to consumer requirements. Bauer's description suggests they did this well, but unfortunately, reports mixed speculation with facts to provide readers what they wanted to hear and then cited the secrecy of the information as validation. This was especially the case regarding Germany, as reporting consistently overstated the scope and effectiveness of German espionage against France and stoked anti-German paranoia. (109) On a more positive note, however, the French made effective use of liaison relationships, engaging in intelligence diplomacy to help solidify overt diplomatic alliances. France, for example, passed information on Paris-based revolutionaries to Russia and also worked with the Russians to break German codes.

So far, so familiar. *Marianne is Watching* is most interesting in its discussion of the social and cultural impact of the development of French intelligence before World War I. A new law in 1886 defined espionage for the first time and enabled military intelligence to expand into the nonmilitary world and prosecute suspected civilian spies. The Deuxieme Bureau and Statistical Section began compiling lists of suspicious foreigners and French citizens to be arrested on the outbreak of war and developed extensive informer networks to identify such people. Not only did this lead to extensive surveillance of innocent people, French and foreign, but the law's vague definitions of what constituted espionage and who qualified as a spy left it to judges and other officials to decide. Journalists became a particular target of the War Ministry, which undertook numerous actions to suppress reporting that was unfavorable or perceived (on flimsy grounds) as compromising sensitive information. The government also brought cases against amateur photographers and people who sold postcards judged—again, on the weakest of pretexts—to contain sensitive images.

Given the atmosphere of fear, in which war with Germany was viewed as inevitable, spy mania was bound to break out. The new and growing genre of spy novels, says Bauer, portrayed intelligence work and counterespionage no longer as grubby and sleazy but as noble, patriotic callings. At the same time, the press warned of spy threats and described how certain types of people—notably foreigners, Jews, and women who had stepped out of their traditional roles—were especially threatening. Egged on by the press and novels, ordinary people began denouncing neighbors and acquaintances; French archives still contain denunciation letters, both anonymous and signed, based on nothing more than gossip and personal grudges. In this heated atmosphere, what's amazing is not that the Dreyfus Affair took place, but that it did not happen earlier.[a]

Bauer, who teaches French and intelligence history at Purdue University Fort Wayne, presents all of this in clear and well-organized prose. Perhaps like anyone who writes French history, she occasionally drifts into academic jargon and citations of Michel Foucault, but the references are mercifully brief. Overall, *Marianne Is Watching* is an informative and thought-provoking book that addresses the intersections of intelligence and social history.

Bauer also speaks to the present. Her narrative of the expanding bureaucratic power of the Deuxieme Bureau and Statistical Section, and the fanning of flames of paranoia in the context of a growing external military and economic threat, bring to mind our current concerns with China. France certainly had good reason to fear Germany, but the Deuxieme Bureau's slanted reporting and the popular fear of German espionage ratcheted up the anxiety. Most of the information on France that the Germans gathered, Bauer points out, came from such open sources as the army's own journals and politically motivated leaks from within the government. As important as vigilance against espionage is, moreover, Bauer shows how easily watchfulness can drift into fantasies and petty score-settling.

Is Bauer suggesting that the same is happening now in the United States? She never makes an explicit link, but her points still raise uncomfortable questions. Is the consensus that China poses an existential threat to the

a. A similar phenomenon took place in the United Kingdom before World War I. See Dr. Christopher R. Moran and Dr. Robert Johnson, "Of Novels, Intelligence and Policymaking: In the Service of Empire: Imperialism and the British Spy Thriller 1901–1914" in *Studies in Intelligence* 54, no. 2 (June 2010).

United States warping intelligence collection and analysis? Are the frequent press reports and investigations of Chinese espionage and influence operations creating a spy fever? To what degree are our fears justified and in what proportion are they exaggerated? The French experience leaves one with the uneasy feeling that for all our technical wizardry and analytic prowess, we might not be much more advanced than the French 150 years ago.

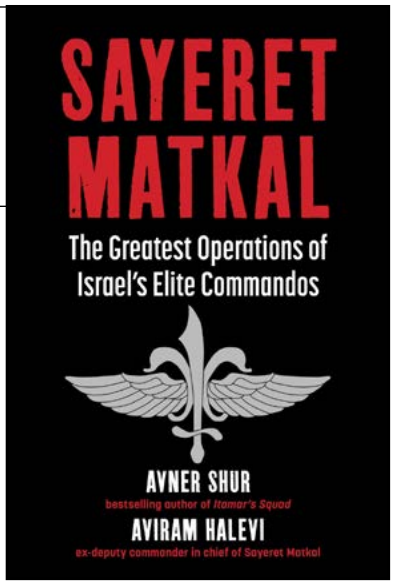
❖ ❖ ❖

The reviewer: John Ehrman is a retired CIA analyst.

Sayeret Matkal: The Greatest Operations of Israel's Elite Commandos

Avner Shur and Aviram Halevi (Skyhorse Publishing, 2023), 247 pages, photos.

Reviewed by Alissa M.



The stories of Israeli spies and special operations have been told so many times in books (*Rise and Kill First; Mossad: The Greatest Missions of the Israeli Secret Service*) and on film (*Raid on Entebbe* and *Munich*) that they often seem like the stuff of legend. A new book by two veterans of Sayeret Matkal—the commando force behind the hostage rescue mission at Entebbe and many other famous operations—tells the stories from a new and sometimes touching perspective. It shows the exhilaration, the agony, the grief, and sometimes the boredom of participating in some of the most famous Israeli commando operations.

Sayeret Matkal's original mandate was reconnaissance, with commando raids a side job that eventually became its primary remit. When Sayeret Matkal—commonly known simply as "the unit"—was founded in 1958, Israeli independence was only a decade old and memories of pre-independence paramilitary groups organizing prison breaks and nighttime raids against the British Mandate were fresh. Sayeret Matkal inherited much of the can-do spirit and courageousness of the young men and women of the Palmach and Hagana. And these are the stories of very, very young men indeed. Even the "old" men—there are no women playing operational roles in this book—are in their early thirties. (9)

The introduction sets the tone for the book as a set of stories in which the authors took part and whose other participants are personal friends, or sometimes even relatives. The narrative is crisp and compelling, with stories that move along apace. In many regards it reads like a series of spy novels in short-story form, with just the action scenes and little time spent on policy or historical context.

The operations recounted in this volume span 1969 to 1994, corresponding to the time when Sayeret Matkal was primarily engaged in commando operations and had mostly abandoned its reconnaissance mission. The unit subsequently shifted focus back to reconnaissance, and the commando role now largely belongs to the counterterrorism-focused Yamam. In that regard, this book is like a greatest-hits album for a band that no longer tours. Sayeret may have returned to its original reconnaissance focus, but it still undertakes some daring missions like the one described in *Shadow Strike: Inside Israel's Secret Mission to Eliminate Syrian Nuclear Power*.[a]

In those busy years of counterhijacking and counterterror operations, the soldiers of Sayeret Matkal experienced exhilaratingly high highs and profoundly low lows. But even the highs were tempered by nearly every mission experiencing a loss. Many of the missions were impossible and therefore they often failed, but nonetheless the men of Sayeret Matkal saved many lives in the process. A chapter on the attempted rescue of paratroopers from the Peak of Hermon is devastating, with operational misstep after operational misstep culminating in a mission that is both tragic and embarrassing in its overconfidence.

At the same time it is a marvel that Sayeret Matkal operators were consistently able to differentiate friend from foe and identify hostage-takers from hostages (194, for example) and that there are so few instances of friendly fire resulting in collateral deaths. Few, but not none. The deep pain felt by the operators at their losses is evident in their narrative. Such stories are told in such a plain and frank tone that it is gut-wrenching to read but extremely compelling.

a. Yaakov Katz (St. Martin's Press, 2019).

The voice of the authors is unexpectedly likable, in contrast to the faux humility common in many other commando memoirs (e.g., *No Easy Day*[a]). Wry humor shines through, as when the authors poke fun at the stature of typical Sayeret Matkal commanders by describing them as having "superb mental faculties, at the apparent expense of physical size." (185) Or when they convey the commitment of the team to conduct a planned raid on a target in southern Lebanon on schedule by noting it was the man's birthday and "nobody in the force want[ed] to ruin the surprise party that they ha[d] been working on for months." (222)

This book would be extremely useful to the understanding of a generation of Israeli political and security leadership, but its value as a research tool is undercut by the absence of an index. An organizational chart would also have been useful—I kept losing track of where in the hierarchy each position fell, which is only compounded by the normal turnover of leadership in a book spanning four decades of operations.

Many of Sayeret Matkal's members have gone on to have prominent careers in Israeli government and politics—most notably Benjamin Netanyahu and Ehud Barak—and most of them are cast in a flattering light, but none more so than Barak. Barak is portrayed as a leader of real integrity while Netanyahu is treated with much less reverence. But during a time when Netanyahu is moving further to the right on the Israeli political spectrum and facing tremendous public protests, it's almost quaint to return to an era when he was part of a team willing to risk his life in relative anonymity to protect any one of his fellow citizens.

In any event, there's very little policy commentary or criticism of political decision-makers. The authors are operators and not policymakers and that is clearly the view from which they are telling these stories. There is, however, occasional criticism of leadership. "The chief of staff is upfront about the price the IDF is willing to pay for the extra deterrence from a physical invasion as opposed to plain old airstrikes: ten men." (45)

This book fills a gap in the literature on Israeli commando operations by telling riveting stories of derring-do from a personal perspective with very little credit taken, and much given.

❖ ❖ ❖

The author: Alissa M. is a CIA analyst focusing on Middle Eastern governance issues.

a. Mark Owen with Kevin Maurer, *No Easy Day: The Autobiography of a Navy Seal: The Firsthand Account of the Mission that Killed Osama bin Laden* (New American Library, 2014).

Intelligence Officer's Bookshelf—September 2023*

Current Issues

Intelligence for Homeland Security: An Introduction, by Jeffrey Douglas Dailey and James Robert Phelps

Lessons from the COVID War, by the COVID Crisis Group. Reviewed by Radhika M.

The Real Special Relationship: The True Story of How MI6 and the CIA Work Together, by Michael Smith

Memoir

Never Give an Inch: Fighting for an America I Love, Mike Pompeo

History

Agents of Influence: How the KGB Subverted Western Democracies, by Mark Hollingsworth

Before Bletchley Park: The Codebreakers of the First World War, by Paul Gannon

Danger Zone: US Clandestine Reconnaissance Operations Along the West Berlin Air Corridors, 1945–1990, by Kevin Wright

Double Agent Balloon: Dickie Metcalfe's Espionage Career for MI5 and the Nazis, by David Tremain

Forging Secrets: Faces and Facts Inside the Nazi Operation Bernhard Scheme, edited by Kiel Majewski et al.

Hitler's Trojan Horse: The Fall of the Abwehr, 1943–1945, Vol. II, by Nigel West

The Lion and the Fox: Two Rival Spies and the Secret Plot to Build a Confederate Navy, by Alexander Rose. Reviewed by David Welker.

The Madam and The Spymaster: The Secret History of the Most Famous Brothel in War-time Berlin, by Nigel Jones, Urs Brunner, and Dr. Julia Schrammel

The Peacemaker: Ronald Reagan, The Cold War, and the World on the Brink, by William Inboden

The Soldier Statesman in the Secret World: George C. Marshall and Intelligence in War and Peace, by David Robarge

Spy Ships: One Hundred Years of Intelligence Collection by Ships and Submarines, by Norman Polmar and Lee J. Mathers

Intelligence Abroad

Revealing Secrets: An Unofficial History of Australian Signals Intelligence & The Advent of Cyber, by John Blaxland and Clare Birgin

Fiction

Citizen Orlov, by Jonathan Payne. Reviewed by John Ehrman.

*Unless otherwise noted, reviews are by Hayden Peake.

Current Issues

Intelligence for Homeland Security: An Introduction, by Jeffrey Douglas Dailey and James Robert Phelps (Lynne Rienner Publishers, 2021) 275 pages, end of chapter notes, bibliography, index.

The Department of Homeland Security was created by the Homeland Security Act of 2002 in response to the 9/11 attacks. The nine separate operating agencies and offices were formed from some 20 preexisting organizations subordinated to various government departments. The Office of Intelligence and Analysis is the only organizational component of DHS with an intelligence and counterintelligence mission. (87)

In *Intelligence for Homeland Security*, authors Dailey and Phelps present a primer on DHS intelligence missions and functions that includes basic definitions and historical background on the need for domestic security. The focus is on the intelligence elements that contribute to the homeland security mission, especially with respect to terrorist threats and the interaction with related agencies like the FBI and CIA. They also mention peripheral organizations within the department, such as the Border Patrol, Federal Emergency Management Agency, and the Transportation Security Agency, that sometimes affect its intelligence mission. Unfortunately, the authors do not provide an organizational chart naming all existing agencies in DHS, although they are named in the text.

The authors include topics on which intelligence is collected, for example, border violations but do not provide actions proposed or taken.

Intelligence for Homeland Security is a good start but for a more complete picture it should be read in conjunction with the Wikipedia entry for DHS.

Lessons from the COVID War: An Investigative Report, by the COVID Crisis Group (PublicAffairs an imprint of Hatchette Book Group, 2023), 347 pages, illustrations, sources, notes, index**.**

Published shortly before the US government and the World Health Organization declared in May that the national and global public-health emergencies, respectively, had expired, *Lessons from the COVID War: An Investigative Report* aims to reignite public interest in the US response to the global pandemic and call attention to the need to continue investing in public health infrastructure, response, and organizational capacity to prepare for "the next one." Billed as the most comprehensive look at the pandemic response, *COVID War* traces the causes of what the authors assess is America's dysfunctional response to the COVID-19 pandemic and compares it to various other country's responses and historical examples, such as the 1918 influenza pandemic and cholera in the 1800s.

The COVID Crisis Group comprises 34 health experts and practitioners, scholars, and government workers who addressed various aspects of the COVID-19 response. Assembled two years ago by University of Virginia professor Philip Zelikow (who was executive director of the 9/11 Commission), the group was created in anticipation of a congressional or presidential 9/11-like commission. When the prospect of such a commission faded, the authors turned to Hatchette Book Group for publication.

Unlike the 9/11 Commission that interviewed more than 1,200 people, including key government officials under oath, the COVID Crisis Group had no legal authority to order individuals to testify under oath, and instead held "listening sessions" with 300 people, but did not interview most Trump and Biden administration officials leading the response they assessed.

COVID War is critical of the US government and takes especially harsh, repeated aim at the US Centers for Disease Control and Prevention, blaming its organizational structure for what they assess was America's inability to put together an effective response. At times, though, *COVID War* reads like a partial retelling of the US response based on others' reporting and memories, with no notable revelations. It also fails to acknowledge the experience of many Americans, especially front-line workers.

The authors describe the COVID war in five key parts. Firstly, as a story of advances in scientific knowledge that outpaced human ability to practically apply that knowledge. They often cite the US response as "a 21st century pandemic addressed with structures mainly built for 19th century problems," which resulted in the US suffering more casualties than any other affluent country, despite having the best access to vaccines. Secondly, that partisan divisions were the result of policy failure and not its cause. Thirdly, there is not enough evidence from China to identify the origin of COVID-19. Fourthly, containment failed. Lastly, systemic problems that existed before 2020 continue to exist today.

Despite this morbid outlook, *COVID War* offers recommendations to address future pandemic threats, including installing a new HHS undersecretary for health security who would oversee the CDC and other relevant organizations, developing better data systems, and accelerating vaccine manufacturing.

This book presents itself as an investigative report, but fails to dive deep into the key players and instead gains its insights from tertiary figures who many times offer partisan opinions. Interviews with key administration officials, those involved in the vaccine development or rapid deployment, or front-line workers may have helped to offer more unique or new insights. If globally, or even within the United States, governments aim to avoid a repetition of what the authors describe as a "catastrophe of national incompetence in governance," focusing on refuting long-resolved arguments or harping on personality-based conflicts fails to offer a nonpartisan strategy or playbook for the future.

The reviewer: Radhika M. is a CIA analyst focused on health security.

The Real Special Relationship: The True Story of How MI6 and the CIA Work Together, by Michael Smith. (Arcade Publishing, 2023) 558, endnotes, photos, index.

After service in the British Intelligence Corps, the BBC, and the *Daily Telegraph*, Michael Smith turned his attention to writing books about intelligence operations, both British and American. His most recent work, *The Real Special Relationship,* combines those topics and is very positively recommended in the foreword by Gen. Michael Hayden, former director of NSA and CIA, and in an introduction by Sir John Scarlett, former chief of the British Secret Intelligence Service.

Smith dates the origins of the "special relationship" to a secret meeting on February 8, 1941, at Bletchley Park, the British codebreaking facility, 10 months before Pearl Harbor. In attendance were the wartime head of Bletchley Park, Cdr. Alastair Denniston, his key staff, and four US cryptographers. (33) In the days that followed, the British and Americans, in a move approved by their political leaders, shared their most important cryptographic secrets.

As Smith views it, the special relationship that began at Bletchley gradually broadened to include British-American contacts generally and to matters of intelligence involving the Five Eyes nations. But as this book emphasizes, the key to the special relationship is the cooperation of the British and US intelligence and security services that informs their leaders.

In support of his position, Smith presents a chronological account of robust collaboration. An example, in addition to cryptography, was the combined Anglo-American intelligence unit that was set up in the immediate aftermath of the US atomic bomb attacks on the Japan to focus on possible Soviet atomic efforts—a futile endeavor since unbeknownst to the Allies, Soviet agents had already passed the secrets to Moscow. (162)

In other areas, cooperation included the risky air reconnaissance of East Europe, Soviet agent operations in East Germany and Vienna, the Berlin Tunnel, the overthrow of Mossaddeq in Iran in 1953, support of the mujahideen in Afghanistan, and relations with Gaddafi in Libya.

The handling and impact of defectors and penetrations among the competing services—CIA, MI6, KGB, GRU—is also covered with emphasis on Penkovsky, Mitrokhin, Gordievsky, Kuklinski, and Ames.

There were, of course, organizational tensions. One resulted from US intelligence failures concerning the 1950 Chinese military intervention in Korea. But in this case, Smith makes clear, there was also impressive intelligence reporting on the Chinese buildup before the intervention. The key misjudgments, he argues, were at the top political and military levels.

Political tensions also arose, as in the Suez Crisis, the Cuban Missile Crisis, and the US invasion of Iraq in 2003. In each case Smith shows how intelligence cooperation nevertheless continued throughout. The same was true in Vietnam, where Britain's head of station in Hanoi, Daphne (later Baroness) Park, developed good relations with her counterpart in Saigon, William Colby. She had, in fact, trained Colby in communications security during World War II when he was in the OSS. (415)

The links between Britain's signals intelligence (SIGINT) agency, GCHQ, and NSA are also a vital component of the relationship, though some have wondered whether NSA should go it alone. Smith dashes the thought by telling of the time in January 2000 when "the main signals intelligence processing computer" at NSA crashed and for "seventy-two hours, with the NSA unable to send out any intelligence, GCHQ stepped in to keep the intelligence flowing to the NSA's US customers." (553)

In Smith's view, the history of how MI6, CIA, GCHQ, and NSA work together is "The Real Special Relationship." (603) Well documented, well told, a fine contribution to the intelligence literature.

Memoir

Never Give an Inch: Fighting for the America I Love, by Mike Pompeo (Broadside Books, 2023) 435 pages, photos, index.

From high school in California, life has taken Michael Pompeo down many paths: to West Point and service as a tank commander in Cold War West Germany, Harvard Law School, the aviation business in Kansas and to the US Congress as a representative of the state, CIA director, and secretary of state. Adopting an unpretentious tone, *Never Give An Inch* adds personal and professional details to Pompeo's impressive record.

Pompeo addresses his strongly held religious beliefs and political preferences, but his experience with intelligence, gained since his election to Congress in 2010 and his appointment to the House Permanent Select Committee on Intelligence is reflected throughout the book. It was as a member of HPSCI that Pompeo learned a valuable political lesson after publicly and unjustifiably attacking Senator Dianne Feinstein (D-CA) for her views on a report on enhanced interrogation. He explains his error and how he apologized to the senator. (381)

Pompeo also tells how honored he was to be nominated to be CIA director in 2017 and how, before his confirmation, he recommended to President-elect Trump that he visit CIA Headquarters on Inauguration Day. He explains the bureaucratic reasons that made such a visit not possible. (21)

Throughout the book, Pompeo expresses candid opinions. For example, he characterizes his predecessor at CIA as too risk-averse and too concerned with reorganizing to solve operational problems. He goes on to tell how he supported a risk-taking approach to the core mission and problems within CIA and how this resulted in his selection of Gina Haspel as his deputy. (24)

Never Give an Inch also includes discussion of Pompeo's relationship with the president and his contacts with agency overseas elements, friendly-nation counterparts, and foreign adversaries—Iran, North Korea, China, and Russia. With respect to Russia, he tells how CIA cooperated with Russian intelligence services to alert them to an imminent attack by ISIS terrorists on Kazan Cathedral in St. Petersburg. (120–21)

Within CIA itself, Pompeo describes an infuriating moment when it was discovered that "a set of CIA cybertools that assisted with surveillance and [disruption of] adversaries' plans" had been compromised by Julian Assange.

As CIA director and secretary of state, he would pursue Assange's extradition.

In April 2018 came the surprise announcement in a Tweet that he would be nominated to replace Rex Tillerson as secretary of state. (51) Pompeo accepted and secured approval of Gina Haspel as his successor.

Pompeo writes that at State, as at CIA, "There were scores of people focused exclusively on things not directly related to the core mission." He says he worked hard to correct that situation. (92) He mentions many efforts undertaken at State, such as the Abraham Accords (327) and some joint efforts that he addressed both as secretary of state and CIA director. He cites the bringing home of Americans held captive overseas as "perhaps the most satisfying" of these. (199)

Pompeo asserts that he always put America first and has "the scars to prove it," citing lines from the *New York Times* or *Washington Post* describing him as "a suck up, sycophantic, former-Trump-hating, power-hungry hack." (408) *Never Give An Inch* makes clear why he disagrees and retains hope for America's success.

History

Agents of Influence: How the KGB Subverted Western Democracies, by Mark Hollingsworth (Oneworld, 2023) 310 pages, endnotes, bibliography, appendix, photos, index.

British journalist Mark Hollingsworth has chosen a classic espionage topic for his latest book. With frequent Sun Tzu citations supporting several case studies, he argues that some agents are employed not to collect secrets but to influence the actions of others.

The first case tells how Hans-Peter Smolka, an NKVD (Soviet internal security service, 1934–46) agent recruited by Kim Philby, worked for the British Ministry of Information where he covertly influenced and manipulated public opinion. After the war, he was awarded an Order of the British Empire by King George VI. He then went to Vienna and helped Graham Greene write *The Third Man*. Although not a spy movie, at one point in the writing Greene included a scene in which the NKVD kidnapped a woman. Smolka, influenced the film's director to remove the scene from the movie script. As an interesting aside, Hollingsworth claims that Harry Lime—the movie's charismatic, morally squalid central character, played memorably by Orson Welles—was partly based on Smolka himself. (30)

A well-known variant performed by agents of influence involves sexual entrapment. Hollingsworth provides publicly known examples. The case of Conservative Party MP Anthony Courtney is unusual because he refused to cooperate with the KGB even after compromising photos were circulated in Parliament.

A much lesser known example concerns Helen O'Brien, who presided in the 1960s over a "unique den of political, sexual and espionage intrigue" in London—a night club called Eve. Frequented by government ministers, KGB officers, and MI6 agents like Greville Wynne, it was a prominent source of KGB compromising information, or *kompromat*. (168) Fluent in Russian, Romanian, French and English, O'Brien was "in fact a registered MI5 agent and informant, who was determined to discover the KGB's deepest secrets and counter their operations." (169)

Britain was not the only target for agents of influence. Hollingsworth notes that "French intelligence agencies were thoroughly penetrated by Soviet spies," (49) the most celebrated of whom was KGB agent of influence Victor Louis, who operated in Europe and America. (53)

Also mentioned is the book *Who's Who in the CIA*, a joint KGB-Stasi (East Germany's internal security service) operation, published in various languages, including English, and purporting to list names and duties of CIA officers. (92) A more direct attack was authored by Labor MP Bob Edwards and titled *A Study of a Master Spy*. It was exposed as "a vituperative attack" on former CIA Director Allen Dulles written by a KGB officer. (243) And much later, in an example of organizational influencing, the KGB would promulgate the lie that the CIA had spread the AIDS virus.

Hollingsworth concludes that in the modern cyberspace world, Russian influence operations will be enhanced by digital technology, and the West must develop means to deal with the resulting threat.

Agents of Influence is an interesting read, but it offers little that is really new.

Before Bletchley Park: The Codebreakers of the First World War, by Paul Gannon. (The History Press, 2020) 352 pages, endnotes, bibliography, photos, index.

The original edition of this book was published in 2010 as *Inside Room 40* (Ian Allen). Author Paul Gannon determined there was a need for an update when the British National Archives released materials correcting some of the previously accepted accounts of Room 40's codebreaking operations during WWI.

Gannon first presents a summary of the events leading to World War I and Britain's need to intercept and decode enemy signals traffic. Next, he summarizes the traditional accounts of how Room 40 originated and the successes achieved in cooperation with its military counterpart MI1(b). Then he argues that the "standard account is in good part a cover story to explain leaks of codebreaking stories into the public realm after the war." Thus the acquisition of German naval codebooks was more "than immensely good luck." (20) And the official story that attributed codebreaking to amateurism and luck was "a comforting legend … part of a cunningly effective British plan to trick its enemies into underestimating its codebreaking capabilities." (86) Gannon even challenges the conventional wisdom that the selection of the first head of Room 40, Alfred Ewing, was the result of a chance encounter with the director of naval intelligence early in the war. (92)

Perhaps Gannon's most interesting revision concerns the Zimmermann Telegram, sent by German Foreign Secretary Arthur Zimmermann, proposing that Germany and Mexico join forces to wage war against the United States. Gannon asserts that William "Blinker" Hall (Ewing's successor) explained the decryption on the capture of a diplomatic codebook in Persia, resulting from "some good luck and some bad luck." In fact, however, it "was actually reconstructed, largely by [Nigel] de Grey" who worked in Room 40. (362) Gannon also charges that Hall gave at least two versions of how the telegram reached the United States and then was passed on to President Wilson the false claim about the way the telegram was discovered and decrypted. (374)

Before Bletchley Park draws on many primary sources that correct details in previous accounts of Room 40 operations. But the overall positive contribution of British codebreaking efforts in World War I is not changed.

Danger Zone: US Clandestine Reconnaissance Operations Along the West Berlin Air Corridors, 1945–1990, by Kevin Wright. (Helion & Company Limited, 2023) 80 pages, bibliography, photos, no index.

Tempelhof Airport opened for service in Berlin in October 1923. As air traffic increased, the Nazis built the iconic curved canopy terminal in the mid-1930s, and it operated until it was replaced in 2008.

Early during the Cold War, Germany was divided into four occupation zones: British, French, American and Soviet. Berlin was located in the middle of the Soviet zone and by agreement among the victors divided into sectors each controlled by one of the Allies. Auto and train access to Berlin from the Western zones required travel through East Germany and was allowed over designated routes. Air access was permitted in three air corridors with military and commercial flights coordinated among the occupying powers. Tempelhof served as the terminal for most US military intelligence collection flights discussed by British author Kevin Wright in *Danger Zone.*

Wright has assembled photographs and performance details of the various aircraft used throughout the Cold War beginning with modified B-26, B-17, and B-29 bombers. These are followed by the workhorse C-54 and

C-130 variants. Mission characteristics are supplied by former pilots and SIGINT ground stations are shown, for example the Allied listening station on Teufelsburg, built on Berlin war rubble. (19) Some Allied and Soviet aircraft that monitored operations in the corridors are also shown and described. Not all collection occurred in the corridors and Wright describes the small fixed-wing aircraft and helicopters used to patrol the Berlin zone.

The enclave of West Berlin contained the headquarters of the Four Power Control Commission, and Wright devotes a section to working with the Soviets on a day-to-day basis.

Double Agent Balloon: Dickie Metcalfe's Espionage Career for MI5 and the Nazis, by David Tremain (Pen & Sword Military, 2023) 246 pages, endnotes, bibliography, photos, index.

The MI5 double-agent operations against the Nazis in WWII were first revealed publicly by J. C. Masterman in his 1972 book, *The Double Cross System* (Yale University Press). Masterman described how the system operated and discussed the contributions of the principal agents, for example TRICYCLE, SNOW, GARBO, and TATE. BALLOON (Dickie Metcalfe), a sub-agent of TRICYCLE (Dusko Popov), was mentioned only a few times and then with sparse detail. British author David Tremain attempts to fill the gap with *Double Agent Balloon*.

Although thoroughly documented with primary sources, the result is a disjointed presentation of facts, often in the form of lengthy quotes, that leaves the reader puzzled. For example, one wonders why after Metcalfe was "passed out of the Royal Military College, Sandhurst," and stayed in the army, where he was "tried by general court martial and convicted of two of the six charges" and, forced to resign, was nevertheless recruited by MI5. (26)

Tremain explains how it happened. After finding work as an air raid precautions officer, Metcalfe wrote to his father's friend Sir Vernon Kell, MI5's first director. He was then interviewed by MI5 officer Thomas Argyll "Tar" Robertson in April 1939. (31) It is not clear when he was designated BALLOON, though Tremain writes he was formally recruited by MI5 in 1941, after working for them even earlier as an arms dealer. (70) There are references to his working for the Ministry of Supply while an MI5 double agent, but the relationship is not clarified.

At one point BALLOON and GELATINE (Friedl Gartner) were both TRICYCLE's subagents in what Tremain calls "The TRIBARGE Organization" apparently intended to add credence to TRICYCLE's bona fides for the Germans. Although the chapter with that title does not mention the organization, there are long quotes indicating but not explaining, its activity. (253)

Tremain goes on to acknowledge that "BALLOON was, in his own way, a colorful character, but he pales in comparison to TRICYCLE. Together they succeeded in deceiving the Germans in the 'great game' of double-cross." (352)

Double Agent Balloon provides some interesting new material while creating doubt as to how it all ties together. A disappointing account.

Forging Secrets: Faces and Facts Inside the Nazi Operation Bernhard Scheme, edited by Kiel Majewski et al (The Florence and and Laurence Spungen Family Foundation, 2022) 250 pages, photos, index.

In early 1940, Nazi SS officer Reinhard Heydrich established a counterfeiting unit in Berlin in which the Nazi intelligence service produced British £5 notes to be used in an to attempt to destroy the British economy. The project was named Operation Andreas. After printing some £3 million in counterfeit notes, it was abandoned after Heydrich was assassinated in May 1942.

In July 1942, the operation was resurrected by Reichsführer Heinrich Himmler and given the name Operation Bernhard. Its objective was the financing of German espionage operations. *Forging Secrets* tells that story.

Based on accounts from historians, descendants of Holocaust survivors, and the granddaughter of the Nazi who ran Operation Bernhard, *Forging Secrets* tells how the Nazis forced Jewish prisoners to forge the money while working in special workshops in various concentration camps. Some 140-plus prisoners produced enough fake currency to equal the face value of all reserves in the vaults of the Bank of England.

Compelling eyewitness accounts by the forgery workshop's survivors are combined with historical analysis of new information on the counterfeit notes They also tell of attempts to forge other material, including US dollars. The detailed descriptions reveal how the forgeries were made and how some were eventually recovered. Photos document many of the individuals and steps in the counterfeiting process.

Several espionage agents and supporters were paid with the counterfeit bills. Most notable was CICERO (true name Elyesa Bazna), played by James Mason in the 1952 film *Five Fingers*. Others mentioned include British double agent Dusko Popov (codename TRICYCLE), German SS officer Walter Schellenberg, and a "black market runner known as George Soros."(31)

Foreign Secrets is a limited edition book and each copy contains a counterfeit "Operation Bernhard" £5 note produced by the prisoners of Block 19 in Sachsenhausen. A movie version of the operation, *The Counterfeiters*, won the Academy Award in 2007 for best foreign film, but it contained many inaccuracies that the book corrects.

An interesting bit of intelligence history that documents Operation Bernhard.

Hitler's Trojan Horse: The Fall of the Abwehr, 1943-1945, Vol. II, by Nigel West (Frontline Books, 2022), 272 pages, endnotes, photos, index.

The Abwehr was the German Army organization responsible for intelligence and security from 1920 until the end of WWII. British historian Max Hastings, commenting on the Abwehr's performance, wrote that its "wartime shortcomings were the product of indolence and incompetence."[a] Nigel West's two-volume study of the Abwehr, based largely on newly released archival records, supports that view with examples of how initial organizational and operational successes crumpled into failure.

In the first volume, *Hitler's Nest of Vipers: The Rise of the Abwehr*,[b] West describes the types of files discovered, the early Abwehr cases, and how they changed the early postwar assessments of Abwehr performance from the late 1930s to1943.

In *Hitler's Trojan Horse*, he deals with its decline and abolition by completing descriptions of operations begun in volume I and adding ones that occurred after 1943. Intertwined are the bitter disputes with other Nazi intelligence organizations and personnel that eventually resulted in the demise of the Abwehr and its leader, Wilhelm Canaris.

An example of a case partially treated in volume I is the story of Erich Vermehren and his eventual defection to the Allies in Turkey. When interviewed in London in May 1944, he discussed "several members of a very determined plot determined to overthrow the government." (246ff)

Operations that came to Allied attention after 1943 included the story of Abwehr agent Otto John—codenamed WHISKY. West reveals John's role in the July 20 plot to assassinate Hitler, noting also that WHISKY's contribution was excluded, for unexplained reasons, from the SIS (MI6) official history, published in 2010. (243ff)

Another interesting case not mentioned in volume I concerned Halina Szymanska, Abwehr chief Canaris's Polish mistress. West tells how she helped establish links with the Abwehr officer Hans Bernd Gisevius, OSS, MI6, and Canaris. (187)

A final example, in what West terms "the Klatt Mystery," is alluded to only briefly in Volume I but is examined in detail in Volume II. Klatt refers to Abwehr officer Richard

a. Max Hastings, *The Secret War: Spies, Ciphers, and Guerrillas* (New York: HarperCollins, 2016), 64.

b. See Graham Alexander review of *Hitler's Nest of Vipers* in *Studies in Intelligence* 67, no. 2 (June 2023).

Kauder, who claimed to head the long running (1941–45) MAX agent network that supplied important military intelligence on the Soviet Union to the German Army. West explains why some thought MAX was an NKVD deception campaign, while others were convinced it was an undetected spy-ring benefiting the Allies. West acknowledges that a degree of uncertainty remains.

Despite increasing high-level bureaucratic problems, the Abwehr, in conjunction with the Sicherheitsdienst (the SS intelligence element), prepared extensive plans for stay-behind operations across France, Belgium, and the Netherlands. West tells how, thanks to the 212 Double Agent Committee (a duplicate of the Double Cross Committee) and the OSS, all stay-behind nets were penetrated.

Hitler's Trojan Horse provides documented detail about Abwehr personnel, operational units, and the many cases in which they were involved. In fact, there is so much detail—unit designations and lengthy quotations from reports—that in reading the narrative one can lose track of the subject at hand. It would have been helpful had comments been included that better explained the detail while establishing context.

Nigel West has presented the most complete account of the Abwehr to date. It will serve as a valuable reference work.

The Lion and the Fox: Two Rival Spies and the Secret Plot to Build a Confederate Navy, by Alexander Rose (Mariner Books, 2022), 270 pages, photos, index, bibliography.

Alexander Rose's engaging, readable volume recounts a tale of covert operations and diplomacy during the Civil War. Rose's book is worthwhile if only for a glimpse into the time before national intelligence organizations had been created and when important covert operations were performed by diplomats, who often had little or no experience in directing such history-changing operations. Similarly, Rose shines light on the Union naval blockade, a vital reason behind the Union victory that has too long been given short shrift by historians in favor of emphasizing the more easily digested accounts of land battles and political struggles.

Rose focuses on the operational duel between two Americans who in 1861 found themselves on differing sides. Ship captain James Bulloch ("the Fox") became the covert operative charged with securing new, highly advanced steam vessels with which the Confederacy could strike Union ships forming a floating barrier at sea designed to starve the South of imported goods—particularly weapons—and choke its economy. Confronting him was US State Department diplomat Thomas Dudley ("the Lion"), a Quaker lawyer who opposed slavery before destroying the institution became a Union strategic objective, who was charged with uncovering and stopping Bulloch's covert operations. This struggle was carried out in Liverpool, England, a thriving shipbuilding center in the 1860s and hotbed of pro-Southern sentiment that was fueled by British desire for profit and indulgence in self-propagating fantasies of the "sunny South." Further complicating Dudley's work was that the British government remained uncertain which side it would support, ambiguity that helped Bulloch and the South.

Although Bulloch's efforts were initially successful—launching British-built Confederate raiders Florida, Alabama, and Shenandoah—these ships served not as blockade-busters battling Northern warships but as "commerce raiders," harassing unarmed Union commercial shipping. That they became storied vessels whose myth considerably outweighed their impact on the war was due in part to Dudley's enduring diplomatic pressure on London, which in turn kept Richmond from striking the blockade in favor of "running" its curtain. To accomplish their respective covert missions, both Bulloch and Dudley recruited assets to collect intelligence and uncover the opponents' efforts, let secret contracts or tried to expose and stop these commercial deals, and collaborated with shady characters of often-swiveling loyalties. In short, Rose tells a story of the sort that were it not true, would make good fiction.

Rose does an excellent job throughout weaving an often-complicated story into a coherent narrative that both experienced intelligence officers and the public will find compelling and entertaining. He particularly excels

in taking readers deep into side issues or quirky personal stories, only to neatly return to the main narrative and explain why he led readers into the rabbit holes in the first place. He also vividly brings to life the seedy, Dickensian world of mid-nineteenth century Liverpool, which is central to how both the crafty Bulloch and the stolid Dudley were able to operate successfully.

The Lion and the Fox might have been an even better work of history had the author stuck to his guns, rather than bowing to the publisher's marketing will (I confess to having heard Rose discuss this in a podcast). The subtitle indulges in commercial hyperbole as neither Dudley nor Bulloch were "spies" and the latter's objective was never to "build a Confederate navy," which existed quite apart from his covert operations in England. Similarly, rather than conventional endnotes the volume presents references in entire chapter-covering collections at the end, making the reader do the work of figuring out where material in the text came from. Even so, intelligence readers will find an enjoyable and informative read in *The Lion and the Fox.*

The reviewer: David Welker is a member of the CIA History Staff.

The Madam and the Spymaster: The Secret History of the Most Famous Brothel in War-time Berlin, by Nigel Jones, Urs Brunner, and Dr. Julia Schrammel (Pegasus Books, 2023), 304 pages, bibliography, photos, index.

The "Madam" was Kitty Schmidt who ran a brothel in Berlin for VIP clients during the Weimar Republic. The "Spymaster" was SS General Reinhard Heydrich, who after Hitler came to power, the authors argue, ordered his chief of foreign intelligence, Walter Schellenberg, to take over the brothel for espionage purposes. There they used a combination of hidden microphones and prostitutes to collect information from clients during their erotic engagements. The establishment was called Salon Kitty.

In telling the story of Salon Kitty, The Madam and the Spymaster gets off to a candid, though curious start, stating that "The truth about the establishment's history and functions has proved tantalizingly elusive." (ix) At the end of their story the authors can only conclude, "We can also be fairly certain that some sort of espionage operation did indeed take place in Salon Kitty." (256) But none are described. The authors also remain "uncertain whether 'Madam Kitty' was a 'trusted informant' or a willingly cooperative agent of the Nazis." (253)

Despite claiming that to tell the story they had to assemble a puzzle from "official documents, and from literature, films, documentaries and photographs, as well as from personal interviews and memoirs," no source notes are provided. (254)

The authors do provide historical background and comments on the morality of various characters from Hitler, Heydrich, Kitty, and even Nazi martyr Horst Wessel, but they include no evidence of any actual espionage. (117)

The Madam and the Spymaster relies on Walter Schellenberg's memoir (also undocumented) to establish the existence of Salon Kitty. But its actual contribution, if any, remains in doubt. Caveat Lector!

The Peacemaker: Ronald Reagan, The Cold War, and the World on the Brink, by William Inboden (Dutton, 2022) 592 pages, endnotes, bibliography, photos, index.

Before Ronald Reagan became president, he visited the North American Air Defense Command (NORAD) complex in Colorado's Cheyenne Mountain. The commander explained that if the Mutual Assured Destruction (MAD) policy failed, an incoming ballistic missile could be detected and give the president time to launch a counterstrike. When Reagan asked what could be done to stop the attack, he was told that it was not possible.

As historian William Inboden points out in *The Peacemaker*, Reagan recognized that this was an unsatisfactory situation, especially since he had been informed

that "the Soviet nuclear arsenal had eclipsed America's and several Soviet officials had voiced the belief that the USSR could survive—and win—a nuclear exchange." (32–33) Reagan later expressed the view that "we should have some way of defending ourselves against nuclear missiles" before they can do damage. (202) At that moment, the seeds of the Strategic Defense Initiative (SDI) were sown.

The SDI story is just one of the issues dealt with in Inboden's lucid account of the Reagan presidency's failures and successes in international policy. In each instance, he includes the influence of intelligence in its various forms. SDI stirred fierce opposition in the Soviet Union and among the Western allies, but Reagan relied on CIA's assessment that the Kremlin was hemorrhaging its cash reserves on "skyrocketing imports from the West—especially grain—and a soft world market for Soviet oil." (122) This was subsequently reenforced by a CIA report saying, "No amount of capital that the Soviet Union can invest would permit them to compete successfully with the United States in terms of SDI." (311)

At the same time he ignored CIA analysis predicting overall Soviet economic growth. Where CIA's Soviet analysts "saw growth and resilience, Reagan perceived decline and weakness." (301) Inboden argues that Reagan's insights gave him critical negotiating leverage with Gorbachev that he used to good effect.

The Peacemaker also comments on CIA efforts to improve the analytic product and revitalize the Directorate of Operations. (87) On other fronts, Inboden describes the contributions to and consequences of CIA operations in Nicaragua and Afghanistan, the SALT talks, and CIA's role in the Iran-Contra affair.

But, Inboden notes, "the Kremlin could still hit back" and did so with the KGB. He discusses the impact of the CIA agent losses due to Aldrich Ames and Robert Hanssen. (359) And to some extent, Inboden suggests these losses were compensated by the defection of KGB officer Vitaly Yurchenko and the revelations of the French agent in the KGB, Vladimir Vetrov, who exposed KGB efforts to steal Western technology and gave CIA an opportunity to reply with "just the sort of tradecraft that Casey and Reagan loved." (122)

Valuable contributions to foreign policy also came from cooperation from the Vatican and Ryszard Kuklinski, the Polish army colonel who became a CIA agent and reported on the communist regime's intentions. (113) But the most important KGB defector, from a foreign policy perspective, was Oleg Gordievsky who counseled Prime Minister Thatcher and met with President Reagan. (181)

The title for the book comes from a comment made by Mikhail Gorbachev, who said Reagan had decided at the right moment "to be a peacemaker." (475) Inboden discusses their relationship in detail, while showing how intelligence was an important factor in the Reagan presidency. Inboden doesn't claim that Reagan won the Cold War, only that he "oversaw the American strategy for the successful end of the Cold War." (476) *The Peacemaker* illustrates how intelligence functions for a US president.

The Soldier Statesman in the Secret World: George C. Marshall and Intelligence in War and Peace, by David Robarge (Center for the Study of Intelligence, Central Intelligence Agency, 2023) 241 pages, footnotes, bibliography, photos, index.[a]

Gen. George Catlett Marshall, US Army chief of staff during World War II, and later secretary of state and defense, is well known for his military achievements and the postwar European economic program that bears his name. He has been the subject of several well-regarded biographies that, with one exception, portray his many accomplishments. The exception is his contribution to the profession of intelligence. CIA Chief Historian David Robarge treats that topic in *The Soldier Statesman in the Secret World*.

Robarge tells how Marshall confronted tactical intelligence for the first time during World War I when, as a lieutenant colonel, he was assigned to General Pershing's

a. The book is available to the public at https://cia.gov/resources/csi/books-monographs/the-soldier-statesman-in-the-secret-world-george-c-marshall-and-intelligence-in-war-and-peace/

staff in France. Tasked to prepare a plan for the reducing the St. Mihiel salient, he found the US Army intelligence section inadequate and turned to the headquarters of the 2nd and 8th French Armies for the necessary data. (2)

Marshall had encountered a problem with military intelligence that would not be solved until 1962: the US Army had no intelligence branch that trained personnel. Unit intelligence positions were filled with officers of other branches—often combat arms—and required to learn on the job. The result was not always positive, and intelligence assignments were not considered career enhancing. Robarge shows that Marshall never addressed the issue comprehensively. And though he dealt with intelligence-related issues before and during EEII, he was less proficient managing them "than any other area of responsibility he had as Chief of Staff." (8)

The Soldier Statesman in the Secret World presents examples that support that view, keeping in mind that his primary responsibilities were leading an army fighting on two fronts while coordinating with the Navy and responding to Congress.

Robarge shows how Marshall had continuing difficulties with the heads of Army intelligence (G-2) and in achieving integration among service intelligence components. He did strongly support cryptographic matters and encouraged cooperation with British counterparts. He also recognized the need for better strategic intelligence. Robarge also describe Marshall's support, with some reservations, for William Donovan in the creation of OSS. (39) Tactical intelligence was left to the theater commands.

On the domestic front, Robarge describes how Marshall handled a "turf dispute" with the FBI (26) and later the Army's Counter Intelligence Corps (CIC) that created a problem involving First Lady Eleanor Roosevelt. The president was much concerned, and Marshall took decisive action. (29) After the war, President Truman sent Marshall to China to seek an agreement between the warring Nationalist Party and the Communist Chinese, a mission doomed to failure. The intelligence situation there was also unsatisfactory since Truman had abolished OSS and several competing agencies were producing poor quality and untimely results, some of which irritated Zhou Enlai, Marshall's principal contact. Robarge explains how Marshall resolved these issues and why he ended up complimenting his intelligence support in China. (128–29)

It was also in China that Marshall had a curious experience with espionage. Robarge tells how Marshall obtained Zhou's notebook naming a communist agent spying on the Nationalists. He returned the notebook to its owner, who assumed it had been copied, but Robarge found no indication that it was. (132–33)

In January 1947, Marshall was recalled to Washington and nominated to be secretary of state. Robarge emphasizes how, during Marshall's two-year tenure, he improved the department's intelligence capabilities and assured they would not be undermined by the new CIA while cooperating on covert action programs. Marshall advocated that the CIA should have the preeminent role in foreign clandestine operations; he believed that a "'neutral,' nonmilitary agency was needed to avoid disputes between the Army and the Navy." (140)

Marshall retired in January 1949, only to be recalled to duty in September 1950, as secretary of defense. During his one-year tenure, two areas of concern were the Korean War and CIA. Robarge describes how Marshall dealt with his dissatisfaction with CIA's intelligence reporting on the the Chinese role in Korea. Marshall was also concerned with CIA's strategic estimates, the "Agency's roles in foreign espionage and counterintelligence, and in covert action." (169)

The final issue Robarge examines is Marshall's response to the so-called Red Scare, or communists in the US government, which overlapped his service at State and Defense. Senator Joseph McCarthy would accuse Marshall of being a communist appeaser among other scurrilous charges.

The Soldier Statesman in the Secret World is a thoroughly documented account that tells how a very remarkable man contributed to the evolution of US intelligence. It adds previously unknown details and is an important contribution to the literature.

Spy Ships: One Hundred Years of Intelligence Collection by Ships and Submarines, by Norman Polmar and Lee J. Mathers (Potomac Books, 2023) 305 pages, endnotes, bibliography, appendices, photos, index.

Norman Polmar is an analyst and consultant specializing in the naval, aviation, and intelligence. His coauthor, Lee J. Mathers, is a retired naval surface-warfare officer with an intelligence specialty. In *Spy Ships*, the authors begin with a short review of ship and small-craft intelligence collection up to the twentieth century. This is followed by a discussion of how the inventions of radio and radar spurred signals collection by ships and submarines during the world wars.

The principal emphasis of the book is on spy ships—including submarines—of the Cold War to the present, as operated by the Soviet Union/Russia, Japan, and the United States, with special attention in the latter case on episodes involving Israel and North Korea. One of the appendixes treats China, Norway, France, Germany and several other countries.

After World War II, the Soviets used East German–built fishing trawlers for SIGINT collection. *Spy Ships* describes the evolution to more sophisticated collection operations using diesel and nuclear submarines under the control of the GRU (Russian military intelligence). (60–62)

The Soviets also employed ships of the line for SIGINT collection and the authors mention a famous example, the cruiser Ordzhenikidze that carried Premier Nikita Khrushchev to England in April 1956. The ship had a team of electronic intercept specialists, and while the ship was docked at Portsmouth, British Cmdr. Lionel "Buster" Crabb, a diver operating for MI6, was decapitated, apparently while examining the ship.

Turning to the United States, *Spy Ships* discuses several SIGINT collect operations. They include the joint efforts of CIA and the seldom-mentioned National Underwater Reconnaissance Office. Their main mission, only partially successful, called Project Azorian, was the recovery of the nuclear warhead in the sunken Soviet nuclear submarine, the K-129, using the CIA-sponsored ship *Glomar Explorer*. (42)

The authors also provide a short discussion of the use of submarines for intelligence purposes, citing the 1971 program known publicly as Ivy Bells—actually named Declension. In this case, the submarine USS *Halibut* was employed to install a recording device on a Soviet underwater communications cable. (44)

US surface ships were also used as collection platforms. (94) *Spy Ships* gives detailed accounts of two operations. The first involved the NSA controlled SIGINT ship, the USS *Liberty*—a converted merchant ship—that was attacked and nearly sunk by the Israelis in 1967. The Israeli government admitted the error and issued an immediate apology. But the authors discuss why some still think the attack was deliberate. (126ff)

The other case study is the seizure of the USS *Pueblo* by the North Koreans in January 1968 with much of its classified equipment intact. This enabled the Soviets to read US encrypted communications for some time because a KGB spy inside the US Navy, John Walker, had provided details about the equipment. (37) The ship remains in North Korea. (180ff)

The authors conclude with the comment that today the sobriquet "spy ships" is "most accurately applied to the specialized intelligence collection ships sent to sea by the Soviet Union/Russia and the United States during the Cold War and after." (209) *Spy Ships* provides well-documented and illustrated evidence that the authors have it right.

Intelligence Abroad

Revealing Secrets: An Unofficial History of Australian Signals Intelligence & The Advent of Cyber, by John Blaxland and Clare Birgin (University of New South Wales Press, 2023) 457 pages, endnotes, bibliography, index.

Initially commissioned in 2019 as an official history of the Australian Signals Directorate by then Director-General Mike Burgess, the ground rules for *Revealing Secrets* were changed by his successor, who denied access to archival documents originating after 1945. The result is an unofficial history with the chapters covering the post-World War II years based on open sources.

After a discussion of cryptological history from its origins in the ancient world, *Revealing Secrets* offers history of Australian SIGINT and cybersecurity, from 1901 to the present as it developed under a number of leaders. The authors explain why Australia has a national signals intelligence agency and its sometimes troublesome relationships with its counterparts in the United States, the United Kingdom, Canada, and New Zealand.

During World War II, Australian SIGINT was subordinated to the Central Bureau under General MacArthur's command, and the authors make clear that while the Australian SIGINT contribution to the Allied victory is virtually unknown, its role was important. A key example, they assert, is Australia's unrecognized contribution to the Battle of Midway. Citing Australian sources, they claim Australian SIGINT identified Midway as the Japanese target before the United States and the latter only confirmed it. (197)

In the post-war era, *Revealing Secrets* conveys the dramatic transformation of Australian SIGINT. The authors discuss Australia's military commitment in Vietnam, the impact of the internet, challenges of the cybersecurity era. Of particular concern are the new SIGINT organizations created and how they dealt with the security leaks that threatened to exclude Australia from the close-knit Five Eyes intelligence relationship. (260)

It was also during this period that the US-Australian Joint Defence Space Research Facility was created at Pine Gap (276) and that according to media reports a sophisticated joint US-Australian operation bugged the Chinese embassy in Canberra with fiber-optic devices. (305)

Revealing Secrets concludes with the proclamation that the "book opens the door to a deeper understanding of Australia's role in world history" and shows how "SIGINT influenced, some-times determined, major events." (332) It is a positive contribution to the literature.

Fiction

Citizen Orlov, by Jonathan Payne (CamCat Publishing, 2023) Kindle Edition, 288 pages in print.

We all know the first law of horror movies: never open the door. Now we can add a corollary, this one for espionage novels: never answer someone else's phone. That simple act, by the eponymous protagonist in first-time novelist Jonathan Payne's *Citizen Orlov*, starts the action in a tale that is as witty as it is engaging.

The story begins when Citizen Orlov, a simple fishmonger, hears a telephone ringing through an open window as he walks down an alley between two office buildings. Unknown to him is that the buildings are occupied by the Ministries of Security and Intelligence. Unsure at first whether to answer, Orlov eventually reaches in the window and winds up taking an urgent, life-or-death message for an Agent Kosek. In an attempt to find Kosek, Orlov climbs through the window and enters the building, where he is immediately drawn into a bewildering world of plots and counterplots.

Citizen Orlov is a picaresque take on the classic spy story of the innocent outsider who lands in the conspiratorial world by accident. Payne, who formerly worked for the UK Home Office, sets his tale presumably the interwar years in an unnamed mountainous central European

country in a manner recalling early Graham Greene and Eric Ambler, with a little of Vladimir Voinovich thrown in. In an echo of George Orwell, moreover, Payne never tells us the characters' given names—they address one another formally, as Citizen, Comrade, Agent, or His Majesty

Orlov himself, however, is anything but the simple man he appears to be. He proves to be a shrewd and resourceful fellow, quickly learning how to manipulate those who are manipulating him and, eventually, outwitting them. The reader will enjoy following his adventures and rooting for him.

Orlov also learns a lot about the intelligence world. "It occurs to Orlov that the security business is complicated and sometimes taxing on the brain," writes Payne about two-thirds of the way through. "He cannot imagine why anyone would want to do this sort of thing for a living. It must be exhausting." No argument there.

The reviewer: John Ehrman is a recently retired CIA analyst.

❖ ❖ ❖