STUDIES

IN INTELLIGENCE | Vol. 69, No. 2 (June 2025)

CI History
Strategic CI

Intelligence in Public Media

This publication is prepared primarily for the use of US government officials. The format, coverage, and content are designed to meet their requirements. To that end, complete issues of *Studies in Intelligence* may remain classified and are not circulated to the public. These printed unclassified extracts from a classified issue are provided as a courtesy to subscribers with professional or academic interest in the field of intelligence.

All statements of fact, opinion, or analysis expressed in *Studies in Intelligence* are those of the authors. They do not necessarily reflect official positions or views of the Central Intelligence Agency or any other US government entity, past or present. Nothing in the contents should be construed as asserting or implying US government endorsement of an article's factual statements and interpretations.

Studies in Intelligence often contains material created by individuals other than US government employees and, accordingly, such works are appropriately attributed and protected by United States copyright law. Such items should not be reproduced or disseminated without the express permission of the copyright holder. Any potential liability associated with the unauthorized use of copyrighted material from *Studies in Intelligence* rests with the third party infringer.

Requests for subscriptions should be sent to:

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

ISSN 1527-0874

Guide to Center for the Study of Intelligence and* Studies in Intelligence *web locations:

The homepage of the Center for the Study of Intelligence is at:
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 design: Doris Serrano. Photo: Karen Zhao, Unsplash.com, Oct. 11, 2019.

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 CIA's History Staff, Lessons Learned and Emerging Trends Programs, and the CIA Museum.

Contributions

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

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. An additional amount is available for other prizes.

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.

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 the 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 Editorial Board welcomes readers' nominations for awards.

CSI CENTER FOR THE STUDY OF INTELLIGENCE

Washington, DC 20505

EDITORIAL POLICY

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

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

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

EDITORIAL BOARD

John Charles (Chair)
Sheridan Bahar
Dawn Eilenberger
James D. Fitzpatrick, III
Steven Galpern
Brent Geary
Paul Kepp
Martin Kindl
Maja Lehnus
Manolis Priniotakis
Mark Sheppard
Monique N. Todd
Linda Weissgold

EDITORS

Joseph W. Gartin (Managing Editor)
Andres Vaart (Production Editor)
Doris Serrano (Graphics Design)

STUDIES IN INTELLIGENCE

Contents

Vol. 69, No. 2 (Unclassified Extracts, June 2025)

Counterintelligence

Intelligence in Public Media

Contributors

Article Contributors

Roald Moyers is a counterintelligence professional who served in the Departments of Defense and Homeland Security and in the US Army as a HUMINT collector.

Alexander Orleans is a cyber threat intelligence analyst and former US government contractor.

Reviewers

Graham Alexander is the pen name of a CIA operations officer.

John Ehrman is a retired Directorate of Analysis officer.

Resolute Lee is the pen name of an ODNI officer.

J. Daniel Moore is a retired CIA historian.

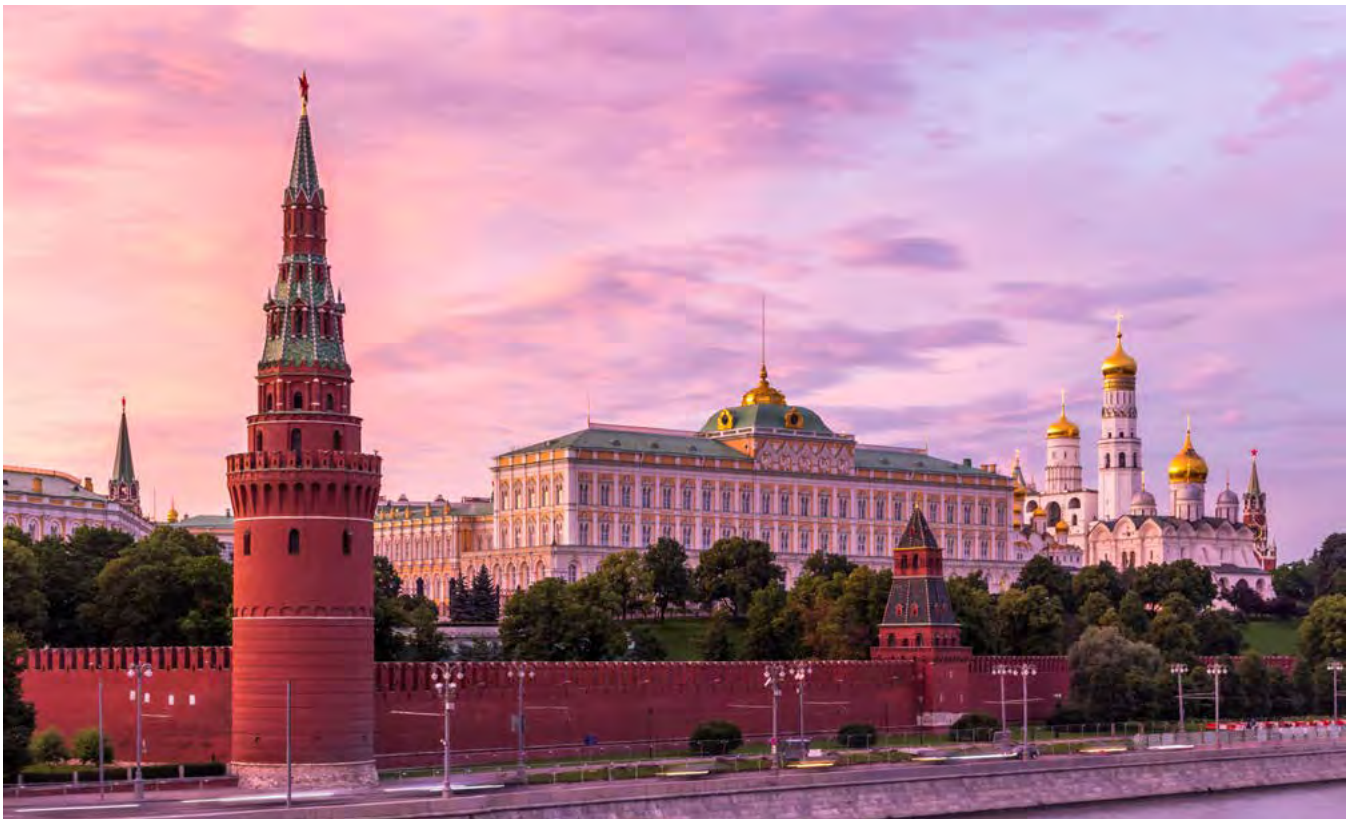
Hayden Peake served in CIA's Directorates of Operations and Science and Technology. He has contributed to the *Intelligence Officer's Bookshelf* since 2002.

Johnathan Proctor is a member of the J2's Defense Warning Staff.

David Robarge is CIA's chief historian.

JR Seeger and Ian B. Ericson: Seeger is a retired CIA operations officer; Ericson is the pen name of a CIA officer.

Anthony Sutton is an analyst in the Strategic Futures Group of the National Intelligence Council. ■



A view of the Kremlin in summer calls to mind fictional spymaster George Smiley's quip, "It would be beautiful in another context."

Beautiful in Another Context: A Counterintelligence Assessment of GTPROLOGUE

Alexander Orleans

Alexander Orleans is a cyber threat intelligence analyst and former US government contractor.

In the 1980s, the Soviet Union's Committee for State Security (KGB) launched a concentrated disinformation campaign as part of an effort to safeguard the identity of their CIA penetration agent, Aldrich Ames. Part of that campaign involved Aleksandr Vasilyevich "Sasha" Zhomov, dispatched as a dangle-type double agent by the KGB in May 1987 targeting CIA's Moscow Station and its Soviet and Eastern European (SE) Division. CIA assigned Zhomov the cryptonym GTPROLOGUE and accepted him as a source; he subsequently became a key disinformation and deception channel for the KGB. In a broader historical context, GTPROLOGUE exemplifies CIA's troubled experience with hostile double agents during the 1980s, when a few select services—particularly the Soviets, East Germans, and Cubans—badly burned the agency.

The views, opinions, and findings of the author expressed in this article should not be construed as asserting or implying US government endorsement of its factual statements and interpretations or representing the official positions of any component of the United States government.

Both the KGB's dispatch of Zhomov and CIA's handling of him as GTPROLOGUE are instructive. The former provides insight into the crafting of offensive counterintelligence operations, particularly underscoring how proper tailoring of a controlled source operation can manipulate a targeted service's attempts at asset validation and thus extend the lifespans of operations. The latter is a cautionary tale of counterintelligence flags that, when methodically inspected, could improve the likelihood of successfully unmasking future provocations.

This assessment is based entirely on publicly available material. To the author's knowledge, the primary source documents associated with this case remain classified, as do illuminating details they might contain. Also, the publicly available facts of the GTPROLOGUE case are rather disparate and occasionally contradictory. In attempting to reconcile such instances of contradiction, the author has preferred to use information that is supported by a preponderance of available research. With both of these qualifications in mind, what follows is an endeavor to present the first public, comprehensive, and contextual accounting of the case as well as its implications for running double-agent operations and conducting asset validation.

Contemporaneous KGB Perspective

On June 13, 1985, Aldrich Ames used his position as a counterintelligence officer in CIA's elite Soviet and Eastern European (SE) Division to sell the identities of more than a dozen Soviet agents—including military and intelligence officers—secretly working for the United States to the KGB for $2 million in an escrow account.[1] The losses resulting from Ames's betrayal played out over the rest of 1985 and 1986. CIA learned of them in sporadic bursts during that two-year period, finding itself by 1987 operating at a marked disadvantage. The '85–86 losses, as they became colloquially known within CIA, also signaled the need for a major KGB undertaking to deceive CIA as to the real reason for these losses. A multichannel KGB disinformation campaign, which operated from at least 1986, was launched to convince SE Division that its losses were the result of anything but a penetration.[2]

Two narratives were included in this campaign. The first was that the KGB had managed to secure a technical penetration of CIA's Moscow Station in the US Embassy. The second, which this author terms the "SCD [Second Chief Directorate] omniscience narrative," was that the operational brilliance and ingenuity of the KGB's SCD, abetted by poor CIA tradecraft, had exposed CIA sources in Moscow that in reality had been betrayed by Ames.

To make this campaign as effective as possible, the KGB relied on its traditional approach to counterintelligence operations. A guiding principle was a certain aggressiveness that emphasized seizing the initiative from the enemy and staying on the offensive.[3] For the Soviet Union, counterintelligence—both foreign and domestic—was the principal raison d'etre of its intelligence efforts both as a revolutionary movement prior to October 1917 and later as a government. Harry Rositzke, the first chief of CIA's original Soviet Division, summarized this legacy:

> *… there is an intangible quality of Soviet intelligence that is perhaps its greatest strength. It is the natural product of the origins and character of Soviet society, what I choose to call the clandestine mentality, the psychological tendency and ability to think and act in secret.… The clandestine mentality is rooted in a conspiratorial view of the world: the world is an unsafe place, for someone out there is plotting against me.… Since the world is a threatening place, only secret counter-action can guarantee survival.*[4]

The emphasis on counterintelligence, and an offensive conception of it, was deeply ingrained in the institutional and operational culture of the KGB. According

to the official KGB dictionaries of intelligence and counterintelligence terminologies, the three guiding principles of KGB operational culture were "clandestinity," "vigilance," and "aggressiveness."[5] Of the three, it was aggressiveness that was meant to suffuse the KGB officer's attitude toward operational action:

> [The style] *of counter-intelligence (intelligence) activity which is proactive and full of initiative, ensuring maximum success in the struggle against the enemy. It is a guiding principle which the intelligence and counter-intelligence agencies seek to follow in their work. In accordance with this, the side which takes the offensive will, all things being equal, achieve the best results.*[6]

The same terminologies defined "counter-intelligence" as:

> [The] *fight against the subversive activity of capitalist intelligence services, the organizations and individuals which they use and hostile elements within the country.… It is characterized by active measures designed to take the offensive against the enemy and to obtain information about his secret plans, intentions, and aspirations. This makes it possible to take steps in advance to forestall enemy subversive actions.*[7]

In attempting to forestall such adversary activity, the KGB "reflexively" favored the use of controlled source operations and mounted many dangle operations.[8] As the Cold War progressed, the KGB became known for extensively using double agents and dangles, most often for tactical counterintelligence (as opposed to strategic deception) purposes.[9] The use of dangles and double agents was considered to be valuable not only as a way to gain windows into an adversary services' motives and methods, but also to plant disinformation and tie down adversary personnel and resources in useless activity. This reflected a long-held preference to use disinformation to conceal real sources.[10]

By the 1980s, that norm of aggressiveness was tempered by two fears: potential punishment for over-disclosure of information during double-agent operations, and the risk that certain dangles would jump ship if given information significant enough to warrant substantial rewards from Western services. It was apparently "strict KGB doctrine that certain types of people and certain types of information would never be shared with CIA in double-agent operations."[11]

Within the KGB, the Soviet preoccupation with secrecy fostered an institutional bias against release of the sort of valid feed typically required to establish the credibility of a deception channel.[12] Stoking this bias among KGB officers running double-agent operations was the fear that someone higher up in the chain of command could decide later that passed information was in fact too sensitive to have been used as bait and then punish the officers involved. Ames himself said after his arrest:

> *Even if a document were of no real value, no one in the Soviet military was willing to sign off on releasing it, knowing that it was going to be passed to the West. They were afraid that a few months later, they would be called before some Stalinlike tribunal and be shot for treason.*[13]

As the pool of information available for use as valid feed was limited, so was the pool of available candidates for its delivery. The KGB feared using staff officers, who, given their rank and position, would have access to detailed knowledge of the KGB's internal workings—and should they defect would be worth their weight in gold to a Western counterintelligence service. Therefore, provocations dispatched by the KGB who actually worked inside the KGB typically presented themselves as having "peripheral or infrequent access" to information of particular interest to target services.[14] The KGB was still operating under both of these constraining policies when the decision was made to mount a disinformation campaign to conceal Ames's treachery. However, opportunities for innovation were provided by Ames himself.

Ames's initial betrayal to the KGB had been the identities of several sources whom CIA had accurately identified as KGB dangles but had chosen to run in order to monitor their production in an effort to ascertain KGB goals. Ames had chosen to expose these sources specifically because he convinced himself it was a moral way to make a quick buck, given that CIA was only receiving false information from them and that the KGB would not punish agents it truly controlled.[15] Yet, by revealing to the KGB which sources CIA knew to be dangles, he also was offering it vital details on how to craft future dangles in a way that would avoid detection.

At some point later in his career as a Soviet spy, Ames eventually provided explicit coaching to his KGB handlers on how to improve their dangle techniques and may have done so well that least a few subsequent dangles were taken by CIA as genuine.[16] This coaching likely included revealing the prevailing theories in the SE Division about how the Soviets ran double agents (discussed below).[17] It is possible that the nontraditional risks taken during the Zhomov case described below were, at least in part, a result of Ames explicitly providing such guidance. Similar guidance also may have been available to SCD via Edward Lee Howard, the former CIA officer who had previously betrayed CIA assets to the KGB and defected to the Soviet Union in 1985.[18]

Dispatching Zhomov

Sometime in 1986, Valentin Klimenko, chief of the SCD's First Department, was directed by either his immediate superior—legendary SCD chief Rem Krasilnikov—or KGB Chairman Viktor Mikhailovich Chebrikov to dispatch a dangle against CIA's Moscow Station with the apparent intent of feeding the SCD omniscience narrative to CIA.[19] On December 22, 1986, Klimenko allegedly met with Aleksandr Zhomov in private, off of official KGB property, and directed him to develop a "plan for something special for our American special service boys" within one month.[20] Zhomov, 32, broke the mold of previous dangles run by the KGB in several ways, all of which were designed to make Zhomov appear as legitimate as possible in the eyes of CIA.[21] These aberrations included several aspects.

Rank and standing

Zhomov was a staff officer in the First Department of the SCD, which was responsible for counterintelligence against Americans in Moscow, and he had served in the KGB for 10 years.

Responsibility

Zhomov was the direct supervisor for all surveillance teams tasked to follow CIA officers in Moscow on a day-to-day basis; he also later described himself as Klimenko's executive assistant. Both descriptions suggest he worked with the First Department's Second Section—the unit responsible for countering intelligence operations emanating from the US Embassy—and either duty would provide him access to a veritable gold mine of intelligence of value to Western services, particularly CIA.[22]

Training

Zhomov spoke English with near-native fluency, indicating a significant investment in him by the KGB, especially given the fact that he was a domestic counterintelligence officer, as opposed to a foreign operations officer.

To be selected as a provocation, an officer like Zhomov must have had Klimenko's absolute confidence and, given that Klimenko claimed he was directly tasked with running the operation, Klimenko must have had Cherbikov's absolute confidence as well.

Running the Provocation

Zhomov's primary mission appears to have been to convince the Americans that the '85–86 losses were a result of the SCD's skills in following CIA officers, combined with poor tradecraft on the parts of US case officers and sources.[23] That SCD omniscience narrative provided benign explanations for the losses that, if believed, would both have a demoralizing effect on

the CIA and deter it from looking inward for a mole.

Coincidentally, the narrative played into a growing paranoia in Moscow Station that the SCD had developed unshakable, "ultradiscreet surveillance" capabilities that CIA could not evade.[24] This paranoia was born of both the '85–86 losses and internal investigations, initiated on the basis of earlier KGB disinformation, that were in the process of ruling against the possibility of a technical penetration of Moscow Station. Available open sources do not indicate whether or not Ames shared those views with his KGB handlers prior to the development of the chosen deception narrative.

The entire operation was crafted to reinforce the SCD omniscience narrative, including the contact procedures Zhomov was to use and the feed he provided US intelligence. Zhomov's posting was to be his cover to contact CIA's chief of station (COS) in Moscow, Jack Downing. First, he would add to his portfolio the personal responsibility for monitoring Downing. This would ostensibly allow him to penetrate the tight KGB surveillance bubble around Downing and pass documents providing initial bona fides, a note outlining motivations for an offer of service to CIA, and instructions for future contact. This is precisely what happened one night in May 1987 in the last car of the *Red Arrow* overnight train between Moscow and Leningrad, which Downing was known to take on a regular basis.[25] Zhomov reportedly introduced himself as "Edwin" in his initial note to Downing.[26]

This first batch of documents included recent surveillance photos of Downing and his wife, along with a very long note by Zhomov. This note had three parts.[27] First was an accurate outline of Zhomov's position and responsibilities in the SCD, but without his name or a pseudonym. Second was an explanation of his purported motives: a mixture of growing frustration with the Soviet system and a failing marriage combining into a desire to leave for America, and thus an offer to spy for CIA to secure its good graces. Third was instructions for a communications plan ("commo plan") dictated by Zhomov: future contact was to be impersonal and at Zhomov's discretion but would utilize his role as Downing's surveillance officer.[28] Ironically, Zhomov's immediate and explicit willingness to spy for CIA, along with the offer of a thoroughly preconceived commo plan, would have been considered tell-tale signs of a dangle in the eyes of the SCD's foreign operations colleagues in the KGB's First Chief Directorate.[29]

This commo plan was designed by the SCD so it could control all aspects of Zhomov's contact with CIA personnel to the point of domination. In a double-agent operation, the concept of "control" can best be understood as:

> *… the capacity of a case officer (and his service) to generate, alter, or halt agent behavior by using or indicating his capacity to use physical or psychological means of leverage.… The degree to which an agent's communications can be controlled runs closely parallel with the degree to which he is physically controlled. Communications control, at least partial is essential: the agent himself is controlled to a considerable extent if his communications are controlled.* [30]

By that definition, the details of the commo plan ensured maximal SCD control over both the physical movements of, and communications between, Zhomov and Downing. Downing was to park his car at one of several restaurants or movie theaters listed in the note on each Friday night, leave his car unlocked, and go inside to the chosen establishment for a meal or film. Zhomov would enter Downing's car under the pretext of rifling Downing's briefcase for recently arrived diplomatic mail and deposit new documents in the briefcase. Should Downing wish to communicate with Zhomov, he was to include a specially marked envelope in his briefcase that Zhomov would know to take with him, effectively turning Downing's briefcase into a letter drop that was to be the primary channel of communication and contact. Brush

passes on the *Red Arrow* would be secondary, but still possible given Zhomov's knowledge of Downing's movements.

These restrictive contact methods not only played into Zhomov's role as chief of surveillance on Downing, but also eliminated any chance for Downing to carefully interrogate Zhomov in person. The denied-area operational environment presented by Moscow—a key element of how the SCD intended to ensure control over the entire operation—inherently precluded face-to-face meetings with sources exceeding about four to seven minutes. Also, any request Downing made for such a meeting elsewhere in Russia could be refused by Zhomov on the grounds that he, of all people, could not be expected to escape the surveillance at which he claimed the SCD so excelled, especially given that they were his people and would notice his absence. Zhomov's posting also precluded a meeting outside the USSR, as SCD officers had lacked occupational excuses for travel abroad. Through these measures, the KGB also reinforced its own defensive counterintelligence position: the risk of Zhomov actually attempting to defect was considerably mitigated through the SCD's control over the operating environment and subsequently the tempo and nature of contact.

Construction of the "bodyguard of truth"[31] designed to safeguard Zhomov against intense CIA scrutiny continued with his second batch of documents, delivered via the planned letter drop procedures one Friday in June 1987. These documents, meant to attest to Zhomov's access, described an upcoming offensive counterintelligence campaign by the KGB. In the coming months, the SCD was planning to dispatch a number of provocations against Moscow Station, specially selected for their attractiveness to US intelligence interests, in order to keep CIA so busy vetting false volunteers that it would be unable to make time for real sources that may volunteer.[32]

Beginning in July and continuing over four more months, the KGB dutifully ran dangles matching descriptions provided in Zhomov's production.[33] Zhomov thus was seen by CIA as having provided valid, valuable information along a plausible line of access. (It is unknown what tradecraft Moscow Station employed in handling these dangles, but it was likely low-level tradecraft that SE Division had reason to believe was previously exposed or could risk exposure.) Having thus established his bona fides via production, Zhomov finally passed along the lie of the SCD omniscience narrative. During another letter drop in June, Zhomov turned over a complete and accurate list of all CIA sources arrested by the KGB in 1985 and 1986, as well their fates, but attributing all losses to the SCD omniscience narrative.[34] Internal KGB assessments of Downing and his predecessor as Moscow COS were included as well.[35] Both pieces of information fit rationally into Zhomov's demonstrated access.

Contemporaneous CIA Perspective

At the time Zhomov appeared on CIA's radar, there was immense concern over determining the cause of the '85–86 losses. Beginning in January 1986, steps were taken within the SE Division to increase compartmentalization and to make inquiries, through offensive counterintelligence operations, into possible causes for the losses.[36] Those offensive operations returned only negatives, indicating that there had not been a penetration of the communication lines between the SE Division at headquarters and stations abroad.[37]

During 1986, two cases occupied much of the counterintelligence efforts regarding the '85–86 losses. First was Mister X, a self-declared—but anonymous—KGB officer who sent six letters to a CIA officer in Bonn between March and October 1986.[38] In these letters, Mister X claimed that a recently lost CIA source had been compromised by a technical penetration of Moscow Station. Mister X was later concluded to be fictional and his claims to be KGB were disinformation.[39] Second was Clayton Lonetree, a Marine Corps guard at the US Embassy in Moscow, who was caught in a

honeypot by the KGB in 1985.[40] However, Lonetree knew little of use to the KGB and turned himself in to the CIA station chief in Vienna in 1986. SE Division closely followed the Naval Investigative Service case against Lonetree and, following his court martial in August 1987, debriefed him extensively before determining that he did not facilitate a KGB technical penetration of Moscow Station.[41]

All of these efforts occurred in the context of CIA's decades-long recovery from the tenure of James Angleton as chief of counterintelligence. Beginning in the early 1960s and continuing until his forced retirement in 1974, Angleton formed and operated under an intricate set of hypotheses in which the KGB was nearly omnipotent, all Soviet volunteers and defectors were likely provocations, and the KGB had a highly placed penetration in CIA. This state of affairs and its effects at CIA were summed up by one of its former chiefs of counterintelligence, Paul Redmond, in 2010:

> *Because there was a belief that the Soviets had penetrated the CIA during the 1960s and the early 1970s,* [Angleton's Counterintelligence Staff] *reigned supreme, paralyzing operations against the Warsaw Pact by assuming that the KGB knew of and controlled all operations. During the tenure of* [Director of Central Intelligence] *William Colby in the mid-1970s, there was a reaction to this mindset that destroyed CI at the CIA and* [led] *to spies in the Agency going undetected and the flowering of opposition-controlled cases.*[42]

It was in this environment that, in July 1971, CIA case officer Burton Gerber published a study of sources and volunteers that had been condemned as provocations by Angleton; Gerber correctly determined that most of them had likely been genuine and not under opposition control.[43, 44] His study was part of an ongoing and fierce internal debate within CIA over the validity of Angleton's theories. Following Angleton's departure, Gerber's paper found strong support and became quite influential, contributing to a renewed willingness by the SE Division to engage the Soviet human intelligence target, and—as explored below—eventually contributed to the asset-validation philosophy of the SE Division as it related to the KGB.[45]

The ill effects of the post-Angleton period extended to asset validation practices within CIA and, according to Redmond, included a "refusal of officers to believe their cases could be a fabricator or controlled by the opposition, particularly when promotions were involved," often in cases involving Warsaw Pact and Soviet sources.[46] This hindered asset validation efforts and increased the likelihood that dispatched double agents could go undetected or that legitimate ones could be tripled and returned to Soviet control. At the same time, CIA was grappling with the challenges of asset validation within denied areas. Again, Redmond is instructive:

> *Asset validation is a very difficult task, particularly when the source is handled in a "denied area" and there are few, if any, other sources of "collateral" information on which to rely for comparison.… In the absence of any sources of its own within the opposition service to warn them, Western services running cases in denied areas have had to rely on the value of the intelligence provided, corroboration of its validity by other sources, if available, and the operational circumstances surrounding the case—particularly how it started.*[47]

The author believes that this statement can be taken as indicative of CIA's philosophy on asset validation in denied areas. While that philosophy is sound, it labors under constraints that are both self-evident and significant. Therefore, officers working denied area cases must be intimately familiar with the tradecraft, preferences, and foibles of the particular opposition service they are laboring to operate against. These tailored insights supplement the four methods of asset validation possible in denied-area cases—identified by Redmond as penetration of the opposition, value of intelligence produced by the source, corroboration of said intelligence by other sources, and analysis of the

case's origins—by making officers better able to detect patterns that could help determine whether or not a given source is under opposition control.

A relevant example of such a pattern in the case of GTPROLOGUE was foreshadowed by a key aspect of Gerber's 1971 study. One of the study's conclusions was that in none of the surveyed cases had the KGB dangled a staff officer, out of concern over the possibility of a real defection; as time went on, this conclusion became something akin to an operational rule of thumb within SE Division: the KGB did not dangle staff officers.[48] (Evidence also indicates that FBI agents during the Cold War separately arrived at, and also generally held, the view that the KGB "would never send a staff officer" as a dangle because of the risks involved if the officer chose to genuinely switch sides.[49])

By the time Zhomov's operation was conceived and launched by the KGB, the "staff officer theory" was apparently accepted, albeit informal, doctrine within much of SE Division. (However, it should be noted that nothing in open sources indicates that, in his 1971 study, Gerber ever suggested that the fact that the KGB had not previously dangled a staff officer could be treated as a guarantor of similar behavior in the future.) Given Ames's numerous postings within SE Division and his explicit coaching of the KGB on improving its provocation techniques, it is probable that he informed the KGB of the staff officer theory.

Shortly after Zhomov approached Downing for the first time in May 1987, the then-unidentified SCD officer was assigned the cryptonym GTPROLOGUE by SE Division.[50] Debate ensued over the new source's legitimacy that same month among SE Division's leaders at CIA Headquarters, mirroring similar debates probably taking place within Moscow Station. Despite the prevalence of the staff officer theory, some viewed GTPROLOGUE as unsettlingly well-timed and well-placed, particularly in light of CIA's desire for inside knowledge of the '85-86 losses.[51] The decision to run GTPROLOGUE and see where he took CIA was made by Gerber, who had been chief of SE Division since summer 1984, and his counterintelligence-minded deputy Redmond on the following explicit premise: if GTPROLOGUE were a legitimate volunteer, he would be a valuable source; conversely, should CIA determine him to be a dangle, his reporting would help indicate topics about which the KGB hoped to mislead CIA.[52]

CIA acquiesced to GTPROLOGUE's requested commo plan. In an effort to reduce the potential for compromise while maximizing opportunities for contact, Downing limited his trips on the *Red Arrow* to once every three months, and spent every Friday night at one of GTPROLOGUE's designated sites. While these logistics meant primary contact with GTPROLOGUE occurred through the letter drop, Downing discovered that GTPROLOGUE would make contact only about once a month, and that the Friday chosen for contact was unpredictable.[53] Available evidence indicates that no additional methods of contact ever were used between GTPROLOGUE and CIA.

When the SCD dangle campaign foretold by GTPROLOGUE's reporting came to pass, the SE Division's leadership directed Moscow Station to run the provocations, despite knowing their true allegiances. This decision was based on a desire to protect GTPROLOGUE: should the provocations be rejected, suspicion in the SCD could fall on him.[54] Soon, the running of these dangles occupied a majority of the station's resources, officers, and time—all with CIA knowledge that no reliable intelligence was being produced. This situation continued even though one instance of particularly sloppy tradecraft by the KGB blatantly revealed that two of the dangles were, in fact, provocations.[55] Had the KGB been taking those provocations seriously, rather than viewing them as ancillary aspects of the larger Zhomov operation, it should have taken steps to firm up the apparent legitimacy of the dangles in question in the aftermath of the error. However, there are no indications that the KGB made any

such efforts, and available information indicates that CIA continued to run both dangles involved, rather than dropping them as could have been justified by the information exposed through the KGB's error in tradecraft.

"Shopping lists" of desired intelligence and questions aimed to test GTPROLOGUE's legitimacy were passed via the letter drops, and apparently no long debriefings allowing for face-to-face assessment of the source ever occurred. After his initial production about the SCD dangle campaign and the SCD omniscience account of the '85–86 losses, GTPROLOGUE never again delivered intelligence that could be described as "certain to hurt [the KGB]."[56] For his efforts, CIA evidently paid GTPROLOGUE "a good deal of money," although there is no clear indication of how or how much.[57] Assertions that he was given upward of $1 million as part of a joint CIA-FBI program aimed at tempting KGB officers to provide intelligence on the '85–86 losses are unproven, and have been made on the basis of what could be interpreted as a post hoc fallacy.[58]

In light of GTPROLOGUE's material attributing the '85–86 losses to the SCD omniscience narrative, SE Division counterintelligence officers working on the losses began to push for questions to be passed to GTPROLOGUE that were designed specifically to test his legitimacy as a penetration. But it appears that the idea of putting such questions to GTPROLOGUE was resisted by elements of SE Division's leadership, which raised a concern common to sensitive cases that questioning the asset too sharply would "make him mad."[59] The questions that eventually were put to GTPROLOGUE were met with answers the wary counterintelligence officers found to be "vague or improbable."[60] Whenever a "hard question" testing his legitimacy did get put to GTPROLOGUE, he would demur and claim that he was holding out on providing his most sensitive intelligence until after CIA had safely extracted him from Russia.[61] However, at no point did he ever request a timeline or express an immediate desire for extraction—a significant red flag.

Uncovering GTPROLOGUE

Eventually, CIA learned GTPROLOGUE's identity through the debriefing of Sergey Papushin, a former SCD officer who defected to the FBI in New Jersey in November 1989.[62] Papushin, who had been acquainted with Zhomov during the former's KGB days, identified a photo of GTPROLOGUE as his former colleague during questioning by CIA, although he did not indicate an awareness of Zhomov's role as a double agent. But Papushin's knowledge of Zhomov did not gel with GTPROLOGUE's reporting about himself: while GTPROLOGUE claimed his marriage had essentially failed, and that this failure had contributed to his desire to defect, Papushin claimed that Zhomov was in fact happily married and doted upon his daughter.[63]

Over time, a combination of the drop-off in the quality GTPROLOGUE's production, poor answers to operational testing questions, and the discrepancies raised by Papushin's reporting all stoked the ongoing debate within SE Division (and the station) as to GTPROLOGUE's legitimacy as a bona fide volunteer versus a double agent. By April 1990, the five people on the GTPROLOGUE operational bigot list at CIA Headquarters were taking informal internal straw polls as to his true allegiance after each exchange between GTPROLOGUE and the new Moscow COS, Mike Cline. In these straw polls, a majority only declared GTPROLOGUE legitimate about 50 percent of the time.[64] Eventually, SE Division decided to deploy a "no exit" approach to determine GTPROLOGUE's legitimacy: attempting a mutually agreed exfiltration operation of Zhomov in July 1990.[65] On April 5, 1990, the final decision to go through with an exfiltration was made by Deputy Director for Operations Richard Stolz, supported by the recommendation of then-SE Division Chief Milt Bearden.[66]

Failure and Extraction

Before the April 5 decision, SE Division developed an exfiltration operation to take GTPROLOGUE out of Russia by having him travel to Estonia and pass from there to Helsinki by ferry on a US passport altered by CIA Technical Services.[67] Several weeks before, extraction had been floated to GTPROLOGUE along with a request for photos to be used in the passport. GTPROLOGUE agreed, provided the requested photos, and later was passed the passport via a dead drop in Moscow.[68]

GTPROLOGUE now was supposed to leave Russia for Estonia on July 10, 1990, but by July 14 he still had not arrived in Helsinki.[69] On July 14, Cline was asked to take the *Red Arrow* with his wife to Leningrad, on the off chance that GTPROLOGUE would attempt a brush pass to explain why he had not followed through on the exfiltration.[70]

A man, possibly GTPROLOGUE, did conduct a brush pass to Cline's wife that night aboard the *Red Arrow*. The passed note expressed "exasperation and rage," decrying the identity provided for the exfiltration as too risky to use and telling CIA that the writer was going to have to lie low and would initiate future contact when he felt it was safe.[71] After the *Red Arrow* arrived in Leningrad, the Clines found themselves under especially heavy surveillance and quickly noticed that GTPROLOGUE was blatantly part of their usual KGB surveillance team. Combined with the contents of the final passed note, these events led SE Division's leadership to conclude that GTPROLOGUE had been under KGB control for his entire operational life as a CIA asset, and effectively ended CIA's dealings with him.[72]

Ames' connections to GTPROLOGUE provide, at most, odd postscripts to the case. In 1989, some of GTPROLOGUE's reporting on dangles apparently led CIA to discard the reporting of a Russian volunteer (Sergey Fedorenko, a former academic who had been permitted to leave the Soviet Union) as possibly under KGB control, when in fact he was not.[73] Ironically, Ames was one of the few individuals in CIA at the time who disputed the applicability of GTPROLOGUE's intelligence to the defector.[74] Ames, acting as an unwitting playback mechanism for the SCD, later would pass information to the KGB throughout 1990 warning it of GTPROLOGUE's existence, but was apparently reassured by his handler that GTPROLOGUE would not betray Ames to CIA.[75] Ames's reporting on GTPROLOGUE may also have been viewed as something of a test of Ames by his handlers in Line KR of the KGB's First Chief Directorate (FCD). Knowing the true nature of GTPROLOGUE's activity, the KGB could compare operational details from SCD to material passed to FCD by Ames; discrepancies or alignments between these two data sets could be used to gauge Ames' access and continued willingness to (or not to) share information.

Missed Warning Signs

In hindsight, the GTPROLOGUE case presented a number of counterintelligence flags to CIA before he was offered exfiltration and its aftermath. Those flags, taken in sum and relation to one another, make the case useful as a cautionary tale. They also exemplify the complexity of asset validation, never a simple task even in the most straightforward of situations: a flag that is truly a cause for concern in one case may also appear in the case of a bona fide asset as well. And in the case of GTPROLOGUE, efforts to discern the truth behind such flags were complicated by a denied area operational environment, Zhomov's potential as a high-value counterintelligence asset, and contradictory data. The primary flags were:

Limited Production

Zhomov exhibited a continuing evasiveness regarding requests for certain information commensurate with his access. Despite the use of some valid feed and Zhomov's position as a staff officer, CIA counterintelligence officers would note later that Zhomov still had claimed the kind of limited reporting ability

that had characterized past KGB-controlled dangles. Namely, that he claimed to only have peripheral or infrequent access to information that should have been easily available given his rank and posting.[76]

Impeded Validation Efforts

CIA's efforts aimed at validating the case were substantially impeded and, at best, met with mixed results. These included Zhomov's poor responses to vetting questions and his limited production. This situation was compounded by the fact that CIA's ability to engage in a continuous and ongoing program of operational testing was severely limited in two ways. First, the impersonal commo plan dictated by Zhomov limited contact only to brush passes and letter drops. Second, the entire case took place within Soviet Russia (primarily Moscow), a denied area that presented all of the obstacles outlined by Redmond above, and also inherently precluded debriefings or long meetings. The fact that the denied area setting generally maximized the KGB's ability to contain the risks it faced in running the operation cannot be understated.

Lack of Operational Control

Zhomov insisted on controlling the initiation and tempo of all contact, which of course was to be run through the impersonal commo plan and already was constrained by the denied-area conditions of the environment. A key to running agents successfully is fostering emotional dependence on their handlers and for handlers to maintain sufficient capacity to exercise physical or psychological means of leverage over the agents.[77] But in this case, it was GTPROLOGUE's CIA handlers who were dependent on him; none of those handlers had any leverage over him except threats of compromise or noncooperation, neither of which had much utility.

Weakness of Alleged Motives

Zhomov appeared to lack a coherent account for the powerful motive necessary to cross the major psychological line of engaging in espionage against his own service. The defector Papushin's independent reporting directly contradicted Zhomov's own reporting on his home life, and thus undermined the credibility of Zhomov's alleged motive for spying. Also, while claiming both a desire to leave the USSR and to be saving information of further interest to CIA for his eventual debriefing in the United States, Zhomov never requested a timeline for his exfiltration.[78]

Topicality of Assignment and Production

That the SCD officer whom CIA would perhaps most have liked to run as a defector-in-place—not too high up in rank, with plausible access to intelligence of immediate interest, able to get close to CIA personnel without arousing suspicion—volunteered as a source was perceived by some as too good to be true. While "too good" and "true" are not by any means mutually exclusive characteristics of an asset, the former always heightens scrutiny to ensure the latter.

Errors in Opposition Tradecraft

As discussed above, a particular error in the KGB's handling of the SCD dangles that GTPROLOGUE "compromised" to CIA led to the blatant exposure of two of the dangles as under hostile control. If the KGB were taking its new dangle campaign as seriously as GTPROLOGUE claimed, that error should have further aroused CIA's skepticism. Instead, it seems that Moscow Station attributed the error to endemically poor SCD tradecraft, which should have appeared inconsistent with GTPROLOGUE's reporting of the SCD omniscience narrative that claimed that the SCD of recent years was at the top of its game.

To CIA's credit, neither the SCD omniscience narrative nor Zhomov's legitimacy were taken as de facto truths by its officers. But while the omniscience narrative was not taken as fact at any time by any member of the SE Division—at most, it was taken as an avenue of investigation worthy of attention as a possible explanation for the '85–86 losses—it still certainly reinforced how the operational risks of Moscow presented a possible explanation. Available accounts also clearly indicate that SE Division's

leadership harbored varying levels of suspicion toward Zhomov throughout the case and the division's counterintelligence staff regularly expressed their growing concerns.[79] At the onset of the case, then-SE Division chief Gerber and his deputy Redmond were suspicious of GTPROLOGUE, and as the case went on those suspicions never abated. When Gerber left his post as chief of the SE Division in 1989, he was still skeptical of GTPROLOGUE. By that time, SE Division counterintelligence officers also had begun to develop their own apprehensions about the case. While those counterintelligence officers' views were resisted by Gerber's successor, Bearden, even he and his senior staff clearly harbored their own concerns regarding Zhomov's true allegiances.

A potential reason for an apparent lack of harsher scrutiny of GTPROLOGUE is "the hunger": that driving desire of case officers for success in the form of a spectacular intelligence coup. That is, it is possible that there may have been a desire on the part of the case officers and managers to make the best of as potentially valuable a case as GTPROLOGUE, despite concerns over the source's legitimacy. According to a former Directorate of Operations division chief, this practice certainly is not unheard of.[80] (A possible parallel may be drawn with FBI cases where high-level criminals being run as confidential informants take advantage of the trust of their handlers in order to facilitate criminal agendas.[81]) As mentioned above, there also were indications during the latter stages of the case that the SE Division's leadership apparently felt that Zhomov was such a highly placed source that questioning him sharply could have risked withdrawal of his cooperation.

Offensive Resourcefulness

In the running of Zhomov, the KGB displayed significant resourcefulness by breaking from traditional constraints that CIA had detected in earlier Soviet operations—particularly using a staff officer as a dangle and using highly sensitive valid feed material—and the resulting provocation operation was exceptional. The operation was tailored to fill a gap in CIA knowledge that the KGB knew to be of pressing interest to its adversary. Zhomov was presented as having plausible access to relevant vital information, and his rank and posting played on the SE Division's internal preconceptions about volunteering KGB officers. That the KGB chose Zhomov in particular, given his rank and posting, was essential to the operation's success. Access to the sort of intelligence he provided would have seemed highly improbable otherwise, and such information coming from a less-qualified source likely would have been treated with greater suspicion. All of these elements fulfilled traditional key requirements for a successful dangle operation.[82]

The KGB effectively established the "bodyguard of truth" around the lie of Zhomov's true allegiance, by serving up an entire SCD dangle campaign to validate GTPROLOGUE's reporting. While costly, in a single stroke that campaign validated GTPROLOGUE to CIA and deftly tied down Moscow Station. Also, the operation was launched at a time when CIA was recovering from severe setbacks in its competition with the KGB, and thus was more likely to be susceptible to a well-crafted dangle.[83] Finally, the KGB ran Zhomov at CIA for several years, giving the operation plenty of time to bear fruit.

By the standards of former chief of CIA counterintelligence James Olson, Zhomov netted at least six types of positive results that a double agent operation can produce for a controlling service.[84] He was able to reveal CIA denied area tradecraft (including an exfiltration route); assess CIA personnel (particularly chiefs of station); serve as a deception channel regarding the causes of the '85–86 losses; expose CIA collection requirements; tie up Moscow Station resources through the futile activity of running dangles, including himself; and, more than likely, take CIA money.[85] The operation also presented the SCD with potential opportunities to arrest CIA officers or cast doubt on the validity and information of genuine volunteers through Zhomov's reporting. Conversely, during his time as GTPROLOGUE,

Zhomov's reporting was almost entirely unproductive for CIA, with two qualified exceptions: he did produce an accurate list of the assets CIA had lost during 1985 and 1986 (although that list was presented in the context of the SCD omniscience narrative), and he forewarned upcoming dangles in Moscow (that still resulted in a drain on CIA resources).

In its success as a counterintelligence effects-based operation, the dangling of GTPROLOGUE was also a textbook deception operation when measured against the standards of strategic deception operations mounted by the Allies during World War II.[86] The operation was ostensibly aimed at making CIA *do* something (i.e., not look inward for the source of the losses), rather than simply *believe* something. It was not mounted simply because the KGB had the resources to do so, but was part of a concentrated disinformation campaign with a simple unitary objective: dissuade, or at least distract, CIA from engaging in a mole hunt.

As noted, Zhomov claimed a limited reporting ability to his CIA handlers despite his rank and position within SCD.[87] In hindsight this is not terribly surprising. The KGB was taking a significant risk in dangling a staff officer, and apparently pursued every available means to mitigate that risk over the course of the operation. It is likely the KGB only felt comfortable engaging in such a gambit because it knew the SCD would have home field advantage in the denied area that was Russia, allowing the SCD to maximize its control over both the operation and Zhomov personally. That it supplemented such a safeguard by having Zhomov follow reporting habits that helped justify limited reporting, to avoid giving away more valid feed than absolutely necessary, makes sense. Perhaps the only glaring weaknesses in the operation from the perspective of the KGB's tradecraft was Zhomov's flimsy motives as GTPROLOGUE and the apparent lack of reinforcement of those motives through GTPROLOGUE's reporting to CIA.

Conditional KGB Success

Dangling Zhomov was largely a success for the KGB as an offensive counterintelligence operation. It clearly fulfilled its potential against CIA as an effects-based operation at the operational and tactical levels, and there is evidence, although ambiguous, that it fulfilled a strategic objective as well. Operationally, Zhomov's "revelation" of a dangle program cleverly tied up some CIA resources in Moscow while simultaneously contributing to both his bona fides and (indirectly) the credibility of the SCD omniscience narrative. Tactically, the impersonal commo plan allowed the KGB to introduce a degree of physical control over the movements of GTPROLOGUE's CIA handlers. In a broader sense, the counterintelligence benefits of running such a successful dangle helped increase KGB knowledge of CIA, as noted above.

At the strategic level, Zhomov's feed about the '85–86 losses and SCD omniscience was meant to serve as part of the bodyguard of lies the KGB was constructing around the truth of Ames's betrayal. There is no evidence to support the conclusion that Zhomov's reporting convinced CIA to seriously consider the SCD omniscience narrative as a more viable cause than a human penetration. But an argument could be made that the KGB's primary strategic aim was just to buy time by temporarily diverting counterintelligence attention from an active asset through presentation of an alternate narrative. If this was in fact the KGB's actual intention, then the operation would more properly be considered a strategic counterintelligence success, as opposed to a strategic deception. (In this case, a useful way to conceive of the difference between achievements in strategic counterintelligence and in strategic deception would be that the former amounts to more of an "operational deception" than the latter, which is closer in equivalency to a "national deception."[88])

As a matter of historical record, CIA counterintelligence did not begin to focus on Ames until November 1989, when he was still

one of several individuals under examination; a more exclusive concentration on him only developed in spring 1991.[89] The Foreign Intelligence Service (SVR), the post-Soviet successor to the KGB FCD, continued to run Ames until his arrest in 1994, the result of an intensive mole hunt by CIA and the FBI.

The two principal SCD officers involved in the GTPROLOGUE case went on to have long and successful careers within the Federal Security Service (FSB), the post-Soviet successor to SCD. Valentin Klimenko served in a variety of senior roles, rising to the rank of at least lieutenant general while in FSB-CIA liaison roles in Moscow and serving as the FSB representative in Israel in approximately 2003.[90] After retiring, he published in 2018 an autobiography titled *Notes of a Counterintelligence Officer*, which discussed the Zhomov case in some detail.[91]

Zhomov would become a prolific figure within the FSB and something of a perennial nemesis for CIA. He continued to serve in SCD's First Department through its transition into the FSB's American Department and its current incarnation as the elite Department of Counterintelligence Operations (DKRO) within the FSB's Counterintelligence (First) Service.[92] During this time, some of his known exploits include the arrest of Alexander Zaporozhsky (an SVR counterintelligence officer who helped CIA identify Ames as a penetration), serving as the FSB's liaison to CIA in Moscow, and playing a significant role in the 2010 Vienna spy swap between the United States and Russia.[93] For an undetermined period of time between approximately 2010 and at least 2019, Zhomov was the chief of DKRO; he eventually reached the rank of Colonel-General.[94]

In a broader historical context, GTPROLOGUE is an example of CIA's troubled experience with hostile double agents during the 1980s, when a few select services—particularly the Soviets, East Germans, and Cubans—badly burned the agency. As a result of earlier cases, in 1987 CIA had already begun to "[develop] a formalized counterintelligence review process, known as the Agent Validation System" to ensure thorough testing of sources for hostile control;[95] the AVS was formally introduced to the Directorate of Operations in 1991.[96]

Conclusions

Zhomov as GTPROLOGUE exemplifies an effective dangle. From operational setting to asset credentials to contact methods to feed, each aspect of the KGB's operation was structured with an innovativeness worthy of emulation. To quote John le Carré's fictional spymaster George Smiley, "It would be beautiful in another context."[97] The KGB successfully structured the operation to seize and withhold the initiative from CIA (within the context of the case), while still working to maximize Zhomov's attractiveness as a source. The operation also demonstrated the historical truth that if you can tell an adversary something it desperately wishes to know more about, it will listen even if it suspects you are lying. All of these elements are the clearest signs that Ames's reporting on CIA knowledge of past KGB double agents may have informed the planning of the Zhomov operation. The weakest aspects of the KGB's running of Zhomov were his alleged motives; more thoroughly backstopping those could have potentially further strengthened GTPROLOGUE's apparent legitimacy.

However, this case does not simply provide insight into the mounting of effective dangles. It also drives home the difficulty of asset validation. In particular, efforts to validate GTPROLOGUE grappled with the added complications of conducting the process in a denied area and conducting it when examining a potential high-value counterintelligence asset. The flags discussed above arose from, or were exacerbated by, these added layers of complexity. Operational and practical constraints created an inability to engage in preferred methods and amounts of testing. And particularly

in counterintelligence operations where the collection target is an aware and hostile actor, as much operational testing as possible is desirable to address doubts that may arise over time.[98]

Because a highly placed penetration poses a potentially significant weapon against the running service if doubled (as controlled at the outset of a case or later in the future), no single metric can be considered to excuse a CI asset from close scrutiny; production alone should not be taken as a solid indication of bona fides. All six traditional methods of asset validation—corroborating production through other sources; specific taskings and operational testing; collecting intelligence on the asset in question; polygraphing the asset; penetrating the local service to uncover potential information on the asset in question; and surveillance of the asset—should be considered carefully and pursued as necessary to return the strongest possible judgment as to an asset's reliability. That judgment then should be reevaluated constantly and actively, as it can never be taken for granted what has or has not happened to sources since they last established bona fides, with the intention of carrying out the sort of programmatic approach to evaluation tempered by officers' instincts meant to be realized by the AVS. In the case of Zhomov, the KGB wisely conducted the operation in the denied area it controlled, resulting in a blanket impediment to all avenues of asset validation.

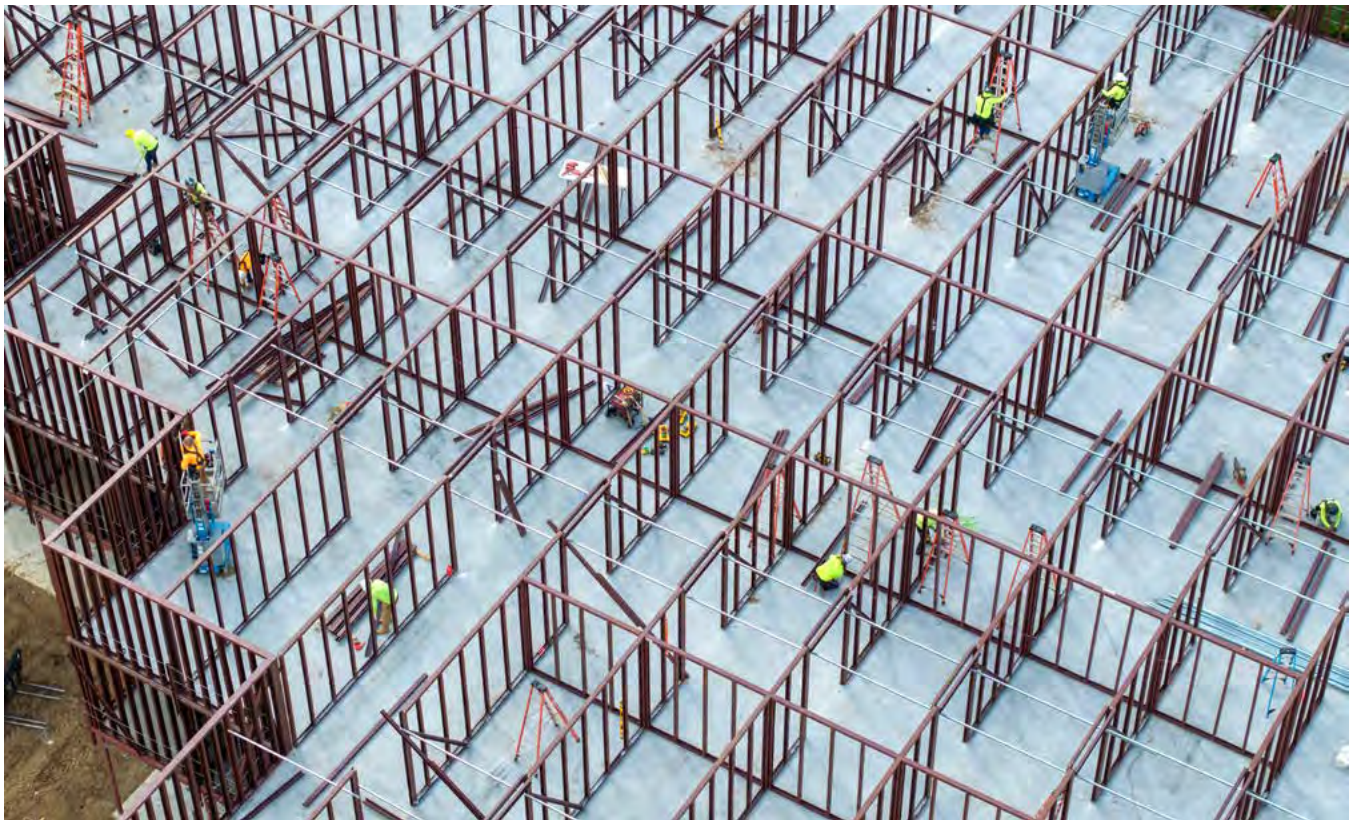
All intelligence professionals always must be ready to accept something entirely new, including in the tradecraft of adversaries, because everything happens once for the first time. This logic never should be far from a counterintelligence officer's mind. Detection of such critical anomalies in operations often arises as the result of spirited internal debates on delicate aspects of cases, including the reliability of assets. Concerns raised during these debates should be taken seriously by all parties involved. Discounting potential issues about a source's bona fides, whether from a fear of irking the source with additional operational testing or from a desire to believe in an asset's potentially high-value reporting; letting the hunger, no matter how well intentioned, override the necessary skepticism intrinsic to human intelligence operations may very well backfire. Such considerations should not be seen as valid reasons for reluctance to subject an asset to operational testing that is as vigorous as possible. ■

Endnotes

1. Michael Sulick, *American Spies: Espionage against the United States from the Cold War to the Present* (Georgetown University Press, 2014), 192–93.
2. Victor Cherkashin and Gregory Feifer, *Spy Handler: Memoir of a KGB Officer: the True Story of the Man who Recruited Robert Hanssen and Aldrich Ames* (Basic Books, 2005), 260; Sandra Grimes and Jeanne Vertefeuille, *Circle of Treason: A CIA Account of the Traitor Aldrich Ames and the Men He Betrayed,* (Naval Institute Press, 2012), 103; Sulick, 194.
3. Tennent H. Bagley, *Spy Wars: Moles, Mysteries, and Deadly Games* (Yale University Press: 2007), 105–106.
4. Harry Rositzke, *The KGB: The Eyes of Russia* (Doubleday, 1981), 48–49.
5. Vasiliy Mitrokhin, *KGB Lexicon: The Soviet Intelligence Officer's Handbook* (Routledge, 2006), 173, 231–32, 261.
6. Ibid., 261.
7. Ibid., 198.
8. Paul Redmond, "The Challenges of Counterintelligence," in *The Oxford Handbook of National Security Intelligence*, edited by Loch K. Johnson (Oxford University Press, 2012), 545.
9. William R. Johnson, *Thwarting Enemies at Home and Abroad* (Georgetown University Press, 2009), 92, 98, 113–14; Peter Deriabin and T.H. Bagley, *KGB: Masters of the Soviet Union* (Hippocrene Books, 1990), 251–52, 266–67; Richards J. Heuer, Jr., "Soviet Organization and Doctrine for Strategic Deception," in *Soviet Strategic Deception*, edited by Brian D. Dailey and Patrick J. Parker (D.C. Heath and Company, 1987), 35, 40.
10. Mitrokhin, 146–47.
11. John Diamond, *The CIA and the Culture of Failure: U.S. Intelligence from the End of the Cold War to the Invasion of Iraq* (Stanford Security Studies, 2008), 230.

12. Heuer, 41.
13. Pete Earley, *Confessions of a Spy: the Real Story of Aldrich Ames* (G.P. Putnam's Sons, 1997), 92.
14. Grimes and Vertefeuille, 21.
15. Diamond, 230; Earley, 139.
16. Earley, 139; Diamond, 230–31; David Wise, *Nightmover*, (Harper Collins, 1995), 114–15.
17. Cherkashin and Feifer, 261; Bagley 227.
18. Sulick, 115–23.
19. Milt Bearden and James Risen, *The Main Enemy: The Inside Story of the CIA's Final Showdown with the KGB* (Presidio Press, 2003), 197.
20. Ibid., 196.
21. Ibid., 196, 291; Cherkashin and Feifer 260–61.
22. John Barron, *KGB: The Secret Work of Soviet Secret Agents* (Reader's Digest Press, 1974), 81.
23. Grimes and Vertefeuille 118; Bearden and Risen, 295.
24. Bearden and Risen, 293, 299.
25. Ibid., 289–91; Grimes and Vertefeuille claim (117, 211) that the GTPROLOGUE case began in June 1988, but the preponderance of available information, including Bearden's and Risen's timelines, place its beginning in May 1987.
26. Andrei Soldatov, "Департамент контрразведывательных операций (ДКРО) ФСБ" Agentura.ru (2022). https://agentura.ru/profile/federalnaja-sluzhba-bezopasnosti-rossii-fsb/departament-kontrrazvedyvatelnyh-operacij-dkro/.
27. Bearden and Risen, 291; Grimes and Vertefeuille 119.
28. Bearden and Risen, 291–92.
29. Pete Earley, *Comrade J: The Untold Secrets of Russia's Master Spy in America After the End of the Cold War* (Berkley Books, 2007), 49–50.
30. F.M. Begoum, "Observations on the Double Agent," *Studies in Intelligence* 6, No. 1 (1962), 65, 66; available at https://cia.gov/resources/csi/studies-in-intelligence/archives/vol-6-no-1/observations-on-the-double-agent/.
31. Thaddeus Holt, *The Deceivers: Allied Military Deception in the Second World War* (Skyhorse Publishing, 2007), 72n.
32. Bearden and Risen, 295.
33. Ibid., 298–99.
34. Ibid., 295, 297; Grimes and Vertefeuille, 118.
35. Bearden and Risen, 297–98.
36. Grimes and Vertefeuille, 102–103.
37. Bearden and Risen, 153–56.
38. Ibid., 169–70, 190–91.
39. Grimes and Vertefeuille, 103-104.
40. Ibid., 108.
41. Ibid., 110–11.
42. Redmond, 540.
43. Bearden and Risen, 23–24.
44. David E. Hoffman, The Billion Dollar Spy (2015), 23–24.
45. Grimes and Vertefeuille, 24.
46. Redmond, 545.
47. Ibid., 545–6.
48. Grimes and Vertefeuille, 24; Bearden and Risen, 23, 296; Hoffman, 24; Cherkashin and Feifer, 261; Bagley 227.
49. David Wise, "When the FBI Spent Decades Hunting for a Soviet Spy on Its Staff," *Smithsonian Magazine* (October 2013). http://www.smithsonianmag.com/history/when-the-fbi-spent-decades-hunting-for-a-soviet-spy-on-its-staff-15561/.
50. Bearden and Risen, 296.
51. Ibid., 296–97.
52. Ibid., 297.
53. Ibid., 298.
54. Ibid., 298–99.
55. Ibid., 299.
56. Ibid., 422.
57. Grimes and Vertefeuille, 119.
58. Benjamin B. Fischer, "Spy Dust and Ghost Surveillance: How the KGB Spooked the CIA and Hid Aldrich Ames in Plain Sight," *International Journal of Intelligence and Counterintelligence* 24, No. 2 (2011), 287, 294; Fischer, "Doubles Troubles: The CIA and Double Agents," *International Journal of Intelligence and Counterintelligence* 29, No. 1 (2016), 51–52; Earley, *Confessions*, 259, 294.

59. Grimes and Vertefeuille, 118.
60. Ibid., 119.
61. Bearden and Risen, 423.
62. Ibid., 421, 395; Grimes and Vertefeuille, 118–9
63. Grimes and Vertefeuille, 118–9.
64. Bearden and Risen, 422.
65. Ibid., 422.
66. Ibid., 424.
67. Ibid., 435.
68. Ibid., 422, 435.
69. Ibid., 435.
70. Ibid..
71. Ibid., 436.
72. Ibid., 437.
73. Grimes and Vertefeuille, 123–24.
74. Ibid., 124; Earley, *Confessions*, 272.
75. Earley, *Confessions*, 276–77, 287; Wise, 191.
76. Grimes and Vertefeuille, 21, 24; Heuer, 36–40.
77. Begoum, 65.
78. Bearden and Risen, 423.
79. Grimes and Vertefeuille, 118–19; Bearden and Risen, 296–97, 422–23.
80. Author interviews with former CIA executive; spring 2014.
81. Author interview with Dr. John Fox, FBI historian; April 7, 2014.
82. Johnson, 106, 109, 113, 128, 197.
83. Holt, 58.
84. James M. Olson, *Fair Play: the Moral Dilemmas of Spying* (Potomac Books, 2006), 234n13.
85. According to a former CIA case officer with extensive Soviet operations experience, "Money paid is not money lost. It is money invested, even with a dangle. It sends a message to those witting back in the mother ship of KGB headquarters that the CIA is good to its word: they pay and they follow through—all attributes a volunteer wants to see before taking the step off the cliff." Author interview with former CIA operations officer, spring 2018.
86. Holt, 50–51, 53, 58, 71, 72.
87. Grimes and Vertefeuille, 21, 24; Heuer, 36–40.
88. Begoum, 62.
89. Grimes and Vertefeuille, 120–21, 125–26, 129–30, 142–43.
90. Bearden and Risen, 522; Rolf Mowatt-Larssen, "US and Russian Intelligence Cooperation during the Yeltsin Years" (February 11, 2011). https://www.belfercenter.org/publication/us-and-russian-intelligence-cooperation-during-yeltsin-years.
91. Filip Kovacevic (@chekistmonitor), "Valentin Klimenko was a top-ranking #KGB CI officer in the 1980s; in charge of the 1st Sec. of the 1st Dept. of the SCD, focusing on the U.S. Embassy & CIA station in Moscow.", Twitter/X, May 10, 2023, 11:00 AM, <https://x.com/ChekistMonitor/status/1656313194359709700>; Valentin Klimenko, Notes of a Counterintelligence Officer (International Relations, 2018). http://loveread.ec/view_global.php?id=85044. Klimenko's account of the Zhomov case contradicts available English-language sources in a number of critical aspects that are not corroborated by any other sources; for this reason, as well as Klimenko's affiliation and implied associated agenda, his statements regarding the case must be viewed with skepticism and were not treated as a reliable source of data for this analysis.
92. Joe Parkinson and Drew Hinshaw, "Inside the Secretive Russian Security Force That Targets Americans", *Wall Street Journal* (July 7, 2023). https://www.wsj.com/articles/fsb-evan-gershkovich-russia-security-force-dkro-e9cf9a49.
93. Gordon Corera, *Russians Among Us* (HarperCollins, 2020), 51–59, 114–16, 285–86, 297–98.
94. Kevin P. Riehle, *The Russian FSB: A Concise History of the Federal Security Service* (Georgetown University Press, 2024), 32; Soldatov.
95. Olson, 253n25.
96. Melissa Boyle Mahle, *Denial and Deception: An Insider's View of the CIA* (Nation Books, 2006), 231–32.
97. John le Carré, *Tinker, Tailor, Soldier, Spy* (Pocket Books, 2002), 332–33.
98. Beogum, 71. ■



An overhead view of a building construction site.

Deconstructing and Reconstructing Strategic Counterintelligence

Toward a New Model

Roald Moyers

Roald Moyers is a counterintelligence professional who served in the Department of Defense and Department of Homeland Security and in the US Army as a HUMINT collector.

The United States is actively engaged in combating what is being termed systems-destruction warfare, in a manner that Chinese military scholars refer to as unrestricted warfare. Within systems confrontation, conflict is waged in the traditional physical domains of air, land, sea, and space, but also the non-physical cyberspace, electromagnetic, and information domains. Systems-destruction warfare applies predominantly to the application of military resources and systems to wage war and dominate within these domains. China's vision of unrestricted warfare, however, relates to more overarching principles for new warfare that is omnidirectional, asymmetric, and unlimited in its application.

The views, opinions, and findings of the author expressed in this article should not be construed as asserting or implying US government endorsement of its factual statements and interpretations or representing the official positions of any component of the United States government.

Full-Spectrum Contest

Unrestricted warfare is executed across and through all the instruments of national power.[1] As a Defense Department report noted in 2023, international rivalry today is "far more complex than the 19th century's Great Game, the 20th century's Cold War, or the beginning of the 21st century's War on Terror. It transcends traditional diplomatic and military solutions to yield a full-spectrum contest of powers vying for strategic advantage through diplomacy, military strength, and economic and technological superiority."[2]

In particular, China views and applies its instruments of national power (diplomatic, informational, military, and economic) as operational systems to achieve its national interests. Beijing's intent is to degrade, deny, and disrupt the United States first and foremost, but also Western-dominated international norms and systems by applying all facets of China's instruments of national power in a directed effort. Today's battlefield is not confined to traditional force-on-force conflict; it comprises the breadth of instruments and systems that the United States depends on for everyday life, including the military systems and instruments that underpin military capability and the interstitial spaces that bridge them together.

The complex blending and interrelation of national power dimensions and the strategic battleground has proven to be a very difficult concept for the counterintelligence (CI) community to adapt to. For decades, our broader CI community has suffered in both identity and responsibility in its mission. Underlying CI's "fractured, myopic, and marginally effective" report card is CI's continued lack of operationally minded philosophy, and established theory, which lead to misfocused practices and priorities.[3,4] Counterintelligence professionals such as Michelle Van Cleave, Paul Redmond, John Ehrman, and James Olson, among others, have called to revitalize and refocus CI toward strategic counterintelligence and to operationalize CI. Some 40 years ago, George Kalaris and Leonard McCoy called to redefine CI considering the growing technical threats across the intelligence disciplines, where CI must learn to adapt, understand, apply, and professionalize in.[5]

Despite encountering and struggling to combat systematic unrestricted warfare, the CI community remains locked in a mental model where CI serves as a security function, as opposed to a strategic intelligence discipline. To be sure, there have been CI successes and the CI community appreciates the daunting challenge of its mission. On balance, however, the CI community fails to break down, analyze, and rebuild new models to succeed in today's complex operating environment. Using a grounded theory of CI, this paper deconstructs the current CI model and reconstructs it to propose a more effective and operationally relevant model of CI for the current and future operating environment.

Literature Review

There is much in the current body of CI literature on practitioners writing about their experiences. Although these provide breadth and depth on CI's application and challenges, they generally focus on the more traditional roles associated with CI functions such as counterespionage, insider threat, and the nexus of security, analysis, and classic offensive operations. Academics have also greatly contributed to the discipline of CI by heeding the calls of practitioners to develop a theory to better define, understand, and apply CI. What remains to be written and established for strategic CI, however, is grounding the theories with practice.[a] This paper leaves ample space to continue grounding practice and theory through the application of strategic CI theory and policy.

This paper builds on Prunckun's (2011) theory of

a. See, inter alia, Executive Order (EO) 12333, CI Enhancement Act of 2002, and Intelligence Community Directives (ICDs) 750 and 700. See also Department of Defense Manual (DODM) 5240.01, DOD Directive (DODD) 5240.02, DOD Instruction (DODI) 5240.10, among other Defense policies.

Evolution of Counterintelligence

The current CI model has been shaped through continual reforms over the past 25 years, beginning in earnest with Presidential Decision Directive *75*, *US Counterintelligence Effectiveness – Counterintelligence for the 21st Century* promulgated in December 2000. PDD-*75* called for a predictive and integrated CI system. Over the next 25 years, the IC took steps to continue strengthening US capabilities and effectiveness by integrating CI into and across the national security enterprise and into US industry. These steps also include the establishment of functional and mission managers within the Office of the Director of National Intelligence (ODNI). Functional managers were charged with the authorities for developing and implementing strategic guidance, policies, procedures for activities related to a specific intelligence discipline, or set of intelligence activities; set training and tradecraft standards; ensure coordination within and across intelligence disciplines and intelligence community elements and with related non-intelligence activities.[20] In 2010, DNI James Clapper merged the CI and security offices into the Office of the National Counterintelligence Executive (later the National Counterintelligence and Security Center). Intelligence Community Directive (ICD) *750* on counterintelligence programs was implemented in 2021.

counterintelligence, which leans on Johnson's (1987 and 2009) and Ehrman's (2009) earlier efforts to develop a CI theory.[6] Although Wettering (2000) addresses organizational, behavioral, and institutional challenges, his focus remains on CI as a security, and counter-espionage function of intelligence which perpetuates the mental models this paper calls to break down and reconstruct.[7] This paper also leans on John Boyd's work on deconstructing and reconstructing mental models.[8] As outlined by EO 12333, CI means information gathered and activities conducted *to identify, deceive, exploit, disrupt, or protect against* espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities.[9]

Bedrock Of Intelligence

CI is the bedrock of intelligence and operational functions. Sound CI processes and activities applied to the collection and analysis of information (including its own counterintelligence information) for intelligence purposes lends credibility to intelligence which supports the development and execution of policy, strategy and operations. Prunckun (2011) lists four principles of CI: deter, detect, deceive, and neutralize. In addition, Prunckun lists three axioms, or conditions of CI: surprise, data collection, and targeting.[10]

This paper modifies this to five CI principles based on CI as defined through EO 12333: *identify, deceive, exploit, disrupt,* and *protect*. The five CI principles have both an *offensive* and *defensive* focus. As Prunckun argues, for intelligence, military, or even strategic business operations to be successful, they must achieve an intended degree of surprise. CI enables surprise at all operational levels by establishing and maintaining secrecy.

Data Collection

In order for CI to establish and maintain secrecy for its supported organization and missions, CI must collect data. An adversary, or competitor's intelligence functions will use all available means (legal, illegal, technical, non-technical) to collect information on its competitor. Simply put, an adversary will conduct reconnaissance on its target to collect intelligence. That reconnaissance can occur through a myriad of means purpose built or assembled to specifically target the information needed to develop operational and strategic intelligence

and to enable the adversary's own surprise.

To establish and maintain secrecy, CI must understand the range of means and methods available to collect information, what can be targeted, how, and why, and what information, through what means can be collected against its supported element. In other words, CI must conduct counterreconnaissance. To be effective, CI must collect information across the breadth of its operating environment. CI must be where adversarial foreign intelligence entities (FIE) operate and are attempting to collect on, penetrate, and exploit.

Third, adversary intelligence activities and national and military strategies focus on targeting information that enables it to disrupt, deny, degrade, or exploit its target, and its target's vulnerabilities, sphere of influence, operations, capabilities, and intentions—present and future. This means CI must continuously collect and analyze data across the scope of its operating environment on both friendly and the adversary to develop an understanding of CI vulnerabilities, threats, and opportunities to provide effective mitigation measures.[11] In other words, to enable security and secrecy.

Deterrence

CI's axiom of secrecy is where CI and security converge. CI supports security through the defensive counterintelligence principle of deterrence.[12] There are three premises to deterrence.

Unacceptable Damage

The premise of unacceptable damage holds that there must be some form of retaliation against the adversary or their intelligence organization. Retaliation may also extend into the domain of international relations. For example, political demarches, public expulsion of intelligence officers and or political officers, arrests, or conversely, dismissal from national security positions for security infractions.

Perception

The second premise is perception by an adversary. The adversary must perceive that a threat has been communicated to it.

Credibility

The third premise, credibility, requires both capability and intent. An adversary must perceive the threat of retaliation to be credible and that it would jeopardize the success of their capability, operations, and or strategy.[13] Another aspect of this is the capability and intent to identify an adversary's penetration (e.g. the CI insider threat) and exploit it to the adversary's disadvantage, which ultimately leads to deterrence.

Current Application

So how does theory shape the practice of strategic CI? Today's model is fragmented, with an over-emphasis on security-focused policies and processes. It lacks a coordinated whole of government effort enabled by baseline professional expertise and acuity. It severely limits effective responsiveness to adapt preemptively and recursively to adversarial threats. As a result, CI struggles to achieve the desired objectives and results of the national counterintelligence strategies.

Currently, CI is outlined in DODD 5240.02, which breaks CI into distinct mission areas: 1) countering espionage, international terrorism, and the CI insider threat; 2) support to force protection; 3) support to the defense critical infrastructure program; and 4) support to research, development, and acquisition. CI activities—analysis, collection, investigation, operations, production, and functional services—are applied toward a distinct mission area. Functional services are the combined application of CI activities.[14]

DODM 5240.02 also directs CI to be integrated into all operations, programs, systems, exercises, planning, doctrine, strategies, policies, and information architectures. This is also consistent with ICD 750. In keeping with its security centric mental model, CI approaches this directive through

the lens of support to security whereby CI, as a second tier system seeks to integrate its resources into existing operational security, information security, personnel security and physical security processes and technologies in an effort to passively bolster security as a deterrent, thereby enabling its principle of deny (focused inwardly) across the security architecture.[15] However, its protection measures are hollow and without real authority, as they are inherently the protection measures afforded by and through the security architecture when and where they are integrated. As outlined in ICD 750, Defense Department policies, and DHS policies, CI is also responsible for CI training as defensive measures and in some cases perceive training as a proactive CI measure.

Organizational CI efforts are focused on one or more functions. Additionally, the application of the functions are siloed, resulting in a stunted understanding and awareness of the full breadth of CI. Moreover, most CI organizations are not imbued with full authorities under EO 12333, and even when CI organizations have full authorities under EO 12333, they choose to further constrict themselves to functional services consistent with the prevailing model, which further reduces the overall application of CI functions. These factors exacerbate a constrained mental model where CI only operates and applies to narrowly defined mission areas that are easily conceivable. Additionally, with ICD 750 and the merger of CI and security, countering insider threats and espionage have blurred into CI as security. This approach focuses resources and policies inward and subordinates them to the security mission.

In short, security enables secrecy and CI assesses whether secrecy remains feasible. Secrecy is enabled through security-oriented policies and procedures such as security classification guidance, information security, and operational security. CI supports security by deterring potential security violators through the subjection of punishment under espionage-related statutes.[16] Deterrence is also achieved through its defense measures of training.

Despite policies explicitly directing the incorporation and support of CI activities into the security framework, the implementation of CI for deterrence remains a secondary security priority, as it creates a redundancy of security processes at an increased cost to security. The prevailing CI model also presents significant gaps in CI collection across the larger national security framework due to increased costs for the required intelligence architecture required for limited perceived benefits. These gaps are the results of the fragmented approaches and integration of CI with security and redundant security measures since security and cyber security incidents are generally reported through respective reporting channels.

Well-established CI programs incorporate a CI review process in the security and information technology architectures, but the degree of incorporation is not equal across the executive agencies. The organizational integration of CI and security divorced from the intelligence architecture limits CI's ability to collect relevant information. The fragmentation of CI and mental models of integrated CI/SEC functions exaggerate these issues, where IT systems are distinct, and CI takes on more of an educational and consultative role as presupposed through ICD 750 and patchwork of fragmented CI policies throughout the national security enterprise.

Security is derived from CI. In this model the execution of CI leads to the implementation of defensive security measures and postures. The defensive activities and postures are the security policies and measures implemented resulting from the execution of CI. In this model, CI executes what it perceives as its three primary principles of deny, through CI as a deterrent, proactively identify through the security architecture (and in the case of the larger CI model, through fragmented relationships and coordination measures), protect by bolstering the security architecture across operations, programs, systems, exercises,

planning, doctrine, strategies, policies, and information architectures. Protection is afforded through the collection of information, which enables the feedback to defensive measures. They are considered offensive, in that they are directed and engage directly with an adversarial FIE through controlled operations.

In this limited model, security supports CI as a mechanism to detect, in order for CI to carry out the classical principle of exploitation. The limited model of CI attributes deception through the principle of exploitation. In this context, deception enables controlled double- agent operations against an adversary. The prevailing Defense model of CI, however, has distanced itself from the general principle of deception and left it to develop into its own discipline of military deception. The divergence of deception from CI and the importance of its role in offensive and defensive CI was and remains a crippling blow to strategic counterintelligence. Deception is a fundamental principle of counterintelligence.

Toward A Strategic Model

China has taken on a system-of-systems worldview and has aligned its instruments of national power to pursue a system of systems approach to becoming the preeminent global power. The battlefield comprises all operational domains. Within this framework, China has developed a multidimensional and multifunctional operational system to be employed against all domains. Yet, it must also be flexible to incorporate new technologies and new functions over time. What this system of systems affords is a modular approach of applying any combination of elements, components, and systems in an integrated fashion to achieve dominance over an opposing system.[17]

For CI, this means the current fragmented and security-focused model of CI is ineffective at identifying and countering the CI threats across the instruments of national power. Moreover, the fractured nature of the CI discipline, where a limited application of CI functions are applied to one problem set at a time, will never effectively identify and counter the FIE threats across the modern warfare domains. To be effective, it must take on a strategic system-of-systems perspective toward CI authorities, institutions, and threat landscapes. Moreover, CI must take on an operational model freed from its self-imposed shackles of constraints and restraints.

Strategic CI is both offensive and defensive. Its state in support of a particular operation, activity, domain, or intelligence function comprises both offensive and defensive properties. Much like light is both an electromagnetic wave and a particle, CI depends on how it is approached. The current mental models associate offensive activities with clandestine activities and are distinct from defensive activities. It also associates intelligence activities in confrontation with FIE to require approaches and methods equal to those of clandestine intelligence activities.

However, as an intelligence discipline, CI leverages its fundamental authority and responsibility derived from EO 12333 to seek out and collect targeted information to identify adversarial reconnaissance and collection efforts. Strategic CI leverages this fundamental responsibility to proactively seek out across all possible threat domains (internal and external) information of intelligence value for CI to identify, deceive, exploit, disrupt, and protect. It is through the intelligence authorities imparted upon CI through EO 12333, the CI Enhancement Act of 2002, and the successive intelligence legislation that enables strategic CI to exert its intelligence authorities across all domains. The limiting factors are which organizations can apply clandestine intelligence activities, and the full scope of CI investigative activities to independently prosecute identified FIE threats.

Offensive Counterintelligence

Offensive CI comprises those activities that are executed proactively through counter-reconnaissance and counter-collection efforts across the operational

domains that actively seek out FIE reconnaissance and collection activities. Offensive activities can either use existing security functions, processes, and technologies to seek out and collect adversarial collection and reconnaissance efforts related to penetration (i.e., CI insider threats), or through targeted collections across the operating domains to identify adversarial collection and reconnaissance efforts.

Within the strategic model, offensive activities do not equate to clandestine activities, but rather proactive targeting of intelligence information within the breadth of the mission space to actively seek out to identify FIE collection and reconnaissance activities. In other words, preemptively and proactively conducting counter-reconnaissance and counter-collections to identify FIE collection and penetration attempts and, or activities. Additionally, defensive measures include vulnerability assessments, and the implementation of security procedures to mitigate vulnerabilities, and conducting CI overwatch, or countersurveillance of friendly forces, or of other intelligence activities. The prevailing fragmented CI model distinguishes these CI activities as distinct functional services (CI support to HUMINT, CI Support to Force Protection, etc).

Surprise

Surprise in strategic CI is more effectively achieved by its role as an intelligence discipline where it stands outside security, and not as a sub-function of security. Timely information is key to maintaining and generating surprise. Organizations create and architect intelligence assets in a manner that affords timely and efficient collection and reporting of information. For the sake of achieving operational surprise elements of security can be sacrificed. Moreover, at times, security must be deceived for the sake of exploiting opportunities to achieve or maintain surprise. Positioning CI within security (unless done for clandestine purposes), denies our own ability to enable surprise.

Surprise is also more effectively achieved when CI and security are distinct from one another, by allowing for the use of the breadth of intelligence authorities that are bestowed upon intelligence functions. Secrecy is achieved in strategic CI by employing the espionage statutory frameworks to compel and bind others to secrecy. This facet also creates effective deterrence by directly compelling and subjecting others to the espionage criminal statutes for the purpose of protecting intelligence sources, methods, and activities. CI merged with, or subordinated to security architectures loses this critical and effective facet of deterrence thereby hollowing out CI as a credible deterrent.

Deterrence

Deterrence is more effectively achieved by its role as an intelligence discipline. CI is inherently a unique intelligence discipline, in that it is afforded the option of pursuing its responsibilities and authorities under intelligence legal frameworks, or under federal criminal statutes. However, they are not strictly mutually exclusive. Strategic CI allows for the full breadth of intelligence partnerships and sharing of authorities to achieve the most effective use of resources, while ensuring and enabling surprise and secrecy. Leveraging whole government authorities and partnerships as intended allows the greatest opportunities for deterrence by uncovering a greater extent of FIE espionage and intelligence networks, activities, and methods.

Deterrence from a strategic perspective also does not simply equate to public charges or dismissal of intelligence or political figures, or of political responses. Deterrence can also be achieved by leveraging the exploited networks to exploit the opportunities they present and offensively attack and penetrate the FIE's intelligence systems at a time and place of our choosing. This positions strategic CI as a critical enabler of surprise, by enabling other operational attack systems (kinetic, and non-kinetic) to penetrate adversarial networks across the warfare domains.

Recommendations

All the of the necessary legislative requirements and authorities are already in existence to

reconstruct CI toward a strategic model. Additionally, the institutional systems and mechanisms for both overt and clandestine activities are already present, to include the sharing of resources and authorities, coordination and deconfliction, and referrals of intelligence activity opportunities. Strategic CI is also already doctrinally established and can be observed through joint warfare doctrines such as command and control warfare and irregular/unconventional warfare doctrines.[1819] Historically, strategic CI can also be observed in the obsolete US Army Counterintelligence Field Manual, where CI was applied through the full range of operational planning and intelligence activities.

A successful strategic CI model for the national security enterprise requires policies that reinforce CI as an intelligence discipline distinct from organizational positions subordinate to security architectures. It will require in policy that organizational CI functions incorporate the respective intelligence oversight required of intelligence activities and functions to ensure the appropriate protection of civil protections, while enabling protection of sources, methods, and activities.

While this may seem an unnecessary statement, many non-Title 50 executive branch departments that maintain small national security elements for intelligence and counterintelligence do not possess the basic oversight structures required of a functioning intelligence and counterintelligence activity. Strategic CI requires a more concerted national mission management role for CI within ODNI for the vast CI missions across the US government. This would entail stronger representation and coordination of intelligence priorities and missions from the disparate CI missions across the executive offices of the US government and among the IC.

Increased professional training and standardization of training and certifications will also be a requirement. Current training standards and baselines are already in existence; however, the IC should seek to improve standardizations amongst the broader CI community and elevate the baseline CI certifications to more advanced levels of CI to ensure equal integration and transferability amongst the broader CI community.

Our adversaries have been studying our systems and our methods and technologies of warfare over the course of the 21st century. In response to our strengths, they have advanced forms and domains of warfare that we have been slow to accept, adapt, and respond. If the United States is to succeed in this era of unrestricted warfare, the CI community must deconstruct and reconstruct CI as a singular, holistic, and adaptable intelligence discipline. An offensively postured mindset would continuously look across all domains, disciplines, and functions to proactively identify, deceive, exploit, disrupt, and protect. We must be adept at recognizing opportunities and knowledgeable in leveraging the whole of government to exploit opportunities. In this way, the CI community can adapt to the changing threat environment. ■

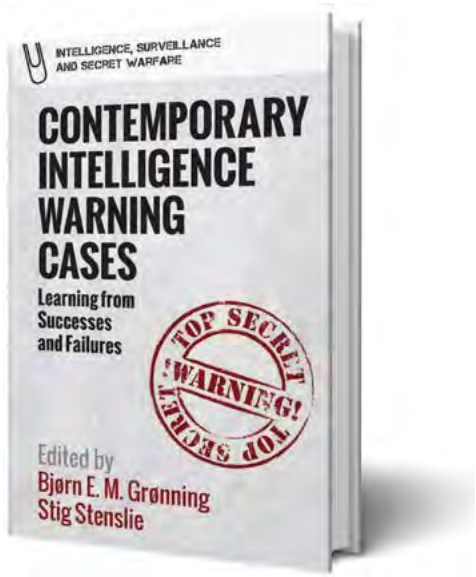
Endnotes

1. Qiao Liang and Wang Xiangsui, *Unrestricted Warfare* (People's Liberation Army, 1999).
2. Defense Counterintelligence and Security Agency, *Targeting U.S. Technology: A Report of Threats to Cleared Industry* (2023), 3.
3. Michelle Van Cleave, "Strategic Counterintelligence: What Is It, and What Should We Do About It?" *Studies in Intelligence* 51, No. 2 (June 2007).
4. John Ehrman, "Toward a Theory of CI: What are We Talking About When We Talk About Counterintelligence?" *Studies in Intelligence* 53, No. 2 (June 2009).
5. George Kalaris and Leonard McCoy, "Counterintelligence for the 1990s," *Studies in Intelligence* 32, No. 1 (Spring 1988).
6. William Johnson, *Thwarting Enemies at Home and Abroad: How to Be a Counterintelligence Officer* (Stone Trail Press, (1987; Georgetown University Press, 2009).
7. Wettering, "Counterintelligence: The Broken Triad," *International Journal of Intelligence and CounterIntelligence* (2000):13, published online October 29, 2010.
8. John Boyd, "Destruction and Creation" (1976). https://www.coljohnboyd.com/static/documents/1976-09-03__Boyd_John_R__Destruction_and_Creation.pdf.
9. President, United States of America. "EO 12333, As Amended." Federal Register. Vol. Vol. 46. Washington D.C., 8 December 2008.
10. Hank Prunckun, "A Grounded Theory of Counterintelligence," *American Intelligence Journal* 29, No. 2 (2011), 8–10.
11. Ibid., 10.
12. Ibid.
13. Ibid.
14. Department of Defense, Department of Defense Directive 5240.02, Counterintelligence (Government Publishing Office, 2018).
15. Ibid., Section 3.d., 2.
16. 18 U.S. Code Chapter 37 Part I – Espionage and Censorship.
17. Engstrom, 2018.
18. Milan Vego, Joint Operational Warfare: Theory and Practice (Naval War College, 2009). Command and Control Warfare, (C2W) as defined by Joint Operational Warfare "is understood as integrated use of information operations, security, military deception, psychological operations, electronic warfare, and physical destruction all supported by intelligence to influence, degrade, deny information to or destroy an adversary C2 capabilities while protecting one's own or against similar actions applicable across the entire spectrum of conflict" (VIII-45). C2W is both offensive and defensive and is employed simultaneously across the operational spectrum (tactical to strategic).
19. For more on the application of CI in irregular warfare see Aden Magee, "Counterintelligence in Irregular Warfare: An Integrated Joint Force Operation," *American Intelligence Journal* 29, No. 2 (2011): 16–23.
20. 108th Congress. Intelligence Reform and Terrorism Prevention Act. Public Law 108-145. US Federal Register, 2004.
21. For a timeline of CI events see: ODNI. Time-Line of CI Milestones. n.d. 2024. https://www.dni.gov/index.php/ncsc-features/203-about/organization/national-counterintelligence-and-security-center?start=36.

intelligence in public media

Contemporary Intelligence Warning Cases: Learning from Successes and Failures

Reviewed by Johnathan Proctor



Author:	*Bjørn E. M. Grønning and Stig Stenslie (eds.)*
Published By:	Edinburgh University Press, 2024
Print Pages	376, index
Reviewer:	Johnathan Proctor is a member of the JCS/J2's Defense Warning Staff.

Case studies have been a mainstay of intelligence education and research for decades, starting with and exemplified by Rebecca Wohlstetter's *Pearl Harbor: Warning and Decision*, published in 1962. However, in their 2017 series of case studies, *Intelligence Success and Failure: The Human Factor*, Rose McDermott and Uri Bar-Joseph pointed out what they perceived to be gaps in the literature of intelligence case studies. First, they argued these case studies, focusing primarily on failures, do not pay enough attention to successes. Second, they said that most studies focus on the US experience, specifically on Pearl Harbor and 9/11.[a] *Contemporary Intelligence Warning Cases* fills both of these gaps in the literature, while simultaneously providing a series of case studies recent enough to resonate with the current and next generations of intelligence professionals, many of whom served, or were at least alive, during the events explored.

Contemporary Intelligence Warning Cases is a compilation of 16 short studies written by a diverse group of scholars and edited by Bjørn Grønning and Stig Stenslie, the deputy research director and head of The Center for Intelligence Studies at the Norwegian Intelligence School, respectively.

While the full list of authors represents several nationalities, most are connected through King's College London—specifically the Department of War Studies or Center for the Study of Intelligence—or the Norwegian Intelligence School, where many authors are full-time or visiting faculty. Chapters written by three American

a. Rose McDermott and Uri Bar-Joseph, *Intelligence Success and Failure: The Human Factor* (Oxford University Press, 2027), 2–4.

All statements of fact, opinion,or analysis expressed in this article are those of the author. Nothing in the article should be construed as asserting or implying US government endorsement of its factual statements and interpretations.

authors provide the exceptions to this rule, including two biographies that cite US Intelligence Community experience within CIA: John Gentry and Soo Kim.

While the roster of authors slants more toward academic experience over current or former practitioners, each author is well established through career experience or publication history. The variety of intellectual backgrounds is a strength of the book, with authors focused on events well within their specific fields of expertise. For example, Aaron Brantley, who explores the 2015 Russian cyber attack on Ukraine's power grid, has published four books on cybersecurity, intelligence, decisionmaking, and cyber deterrence.

Contemporary Intelligence Warning Cases explores warning failures and successes, but it does not concur with the idea that only intelligence failures and policy successes exist. A central premise of the book, clearly articulated by the editors in the introductory chapter, is that warning is a "joint venture in the intelligence-policy nexus" with two elements: the intelligence services' responsibility to "detect, discern, and alert decisionmakers" and the "decisionmaker's preventative response" to the threat warning. (1–5) The idea of warning as persuasive communication is acknowledged by other authors from the King's College school,[a] but Bronning and Stenslie imply that there are limits to the responsibility of intelligence services to persuade, challenging the idea expressed in Henry Kissinger's reported statement, "You warned me, but you did not convince me."[b] They divide warning failures into two types: *Type A* failures are those in which an intelligence service does not detect and communicate a threat warning; *Type B* failures occur when policymakers do not act on the threat warnings.

In addition to Type A and Type B successes and failures, the authors include two other critical distinctions in their case studies. First, they look at both traditional and nontraditional warnings. Traditional cases focus, as expected, on military attacks, terrorism, and cyber-attacks. Nontraditional cases examine such events as the 2008 financial collapse, ISIS's destruction of world heritage sites in Palmyra in 2015, the COVID-19 pandemic, extreme flooding in Pakistan in 2022, and a national intervention in the sale of a private company to a Russia-connected firm in 2022.

Second, the authors distinguish between strategic and tactical failures, defining each primarily by time frame and the ability to act on warning. They characterize strategic warning as longer-term, broader, and often less actionable. Tactical warning, by contrast, is more specific, in timing and scope, and is thus generally more actionable. The authors cite Gordon and Gentry's *Strategic Warning Intelligence* and Erik Dahl's *Intelligence and Surprise Attack* in their definitions.[c] However, the picture of strategic and tactical warning emerging from the 16 individual case studies most closely aligns with the late CIA analyst Jack Davis' strategic and "incident" warning framework.[d]

The editors establish the overall framework and relevant definitions in the opening chapter, and the case studies that follow use them consistently. Each chapter provides background information and a narrative of the event, discusses the type of success or failure, and closes with a series of lessons and recommendations for intelligence practitioners. Four major themes emerge from the case studies:

- the importance of the intelligence-policy nexus and the relationship between the two elements;
- the critical role that bias and politicization play in both intelligence and policy circles;
- an emphasis on cooperation, both inter- and intra-governmental; and
- the importance of expressing warnings directly and clearly, often recommending dedicated warning products over the practice of embedding warnings in standard production.

While one of the book's core strengths is its exploration of a wide variety of cases, the inevitable

a. Christoph Meyer et al., *Warning About War: Conflict, Persuasion, and Foreign Policy* (Cambridge University Press, 2020), 6.
b. Roger George and James Bruce, *Analyzing Intelligence: National Security Practitioners' Perspectives*, 2nd ed. (Georgetown University Press, 2014), 366, accessed March 20, 2023. ProQuest Ebook Central.
c. John Gentry and Joseph Gordon, *Strategic Warning Intelligence* (Georgetown University Press, 2019), 11–17; Erik Dahl, *Intelligence and Surprise Attack: Failure and Success From Pearl Harbor to 9/11 and Beyond* (Georgetown University Press, 2013), 2–4.
d. Jack Davis, *Improving CIA Analytic Performance: Strategic Warning* (CIA, Sherman Kent Center for Analysis, 2002), 2–4.

trade-off is that no chapter goes into significant detail on any one, particularly when they are compared to case studies from World War II, the Korean War, the first Yom Kippur War, or 9/11. The average chapter runs approximately 14 pages, with an additional two to three pages of citations and endnotes. Another strength is each event's contemporary nature. However, the resulting trade-off in this event is a lack of detailed information on intelligence collection and production, much of which has yet to be declassified and made public. Several authors acknowledge their reliance on publicly available information and its effect on their chapters.

Chapters are standardized with lessons and recommendations at the end of each, but not all chapters clearly state the type of problem (i.e., traditional or nontraditional) or the specific nature of each failure (i.e., strategic or tactical, Type A or Type B). While some cases are very clearly one type or another—tactical or strategic, or traditional or nontraditional—there are cases in which the types of failure are more difficult to discern or more debatable. In such instances, clear articulation of the authors' overall assessments and reasoning might help individual readers, especially those with less knowledge or experience in intelligence. However, for academics or instructors in a classroom environment, this creates an opportunity for classroom discussion and debate on the categorizations that might be appropriate in each case.

None of these issues detracts from the book's quality and relevance for intelligence practitioners or scholars. It is also an excellent read for decisionmakers looking to understand their roles in the warning equation and the challenges intelligence faces in working to provide warning. The length of each case study does not detract from their overall accuracy or the relevance of the lessons and recommendations. Their conciseness does, however, make the chapters more digestible, indeed optimal for use in undergraduate, graduate, or professional training environments.

Likewise, a reliance on OSINT does not allow for information on what intelligence services knew, when they knew it, and the form of collection that provided, or failed to provide, that information. While some might argue that these are necessary elements of any complete case study, their absence does not affect the value and applicability of each chapter's conclusions and recommendations.

Finally, one of the book's most important contributions to intelligence studies is its consideration of strategic warning. Several authors cite Dahl's work and his theory of preventative action, which emphasizes the importance of detailed tactical warning in preventing threats, despite the usual calls from decisionmakers for more and better strategic warning.[a] None of the cases presented contradict Dahl's findings and generally support his emphasis on tactical warning and receptivity from decisionmakers. However, the Bergen AS case study (Russian acquisition of critical technology through a business transaction) demonstrates that strategic warning can also be highly effective. In the Bergen AS case, strategic warning on the threats posed by business acquisitions enabled the establishment of the legal framework eventually used to act on tactical warnings. As the editors state, "strategic warning requires strategic response."[b]

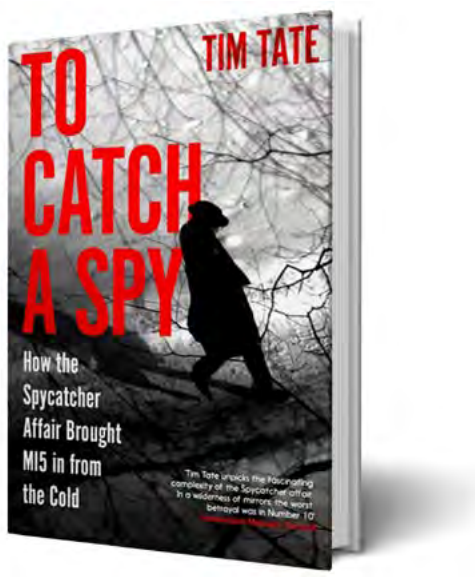
Overall, *Contemporary Intelligence Warning Cases* is an excellent addition to the scholarly literature on warning and deserves a place in organizational and personal libraries. It performs an essential service, filling gaps in the case study literature by adding a series of contemporary cases explored from various intellectual and national perspectives and touching on topics not commonly associated with intelligence warning. Furthermore, it adds distinct value to the field through its framework of intelligence success and failure, its discussion of strategic warning's importance, and its emphasis on the importance of the intelligence-policy relationship. Intelligence officers would do well to understand the policy space in which decisionmakers operate, and those decisionmakers need to form realistic expectations of what intelligence can provide with high levels of confidence, particularly against lingering and complex issues. ■

a. Dahl, *Intelligence and Surprise Attack*, 23–24.
b. Bronning and Stenslie, *Contemporary Intelligence Warning Cases,* 298.

intelligence in public media

To Catch a Spy: How the Spycatcher Affair Brought MI5 in from the Cold

Reviewed by David Robarge



Author: *Tim Tate*
Published By: Icon Books, 2024
Print Pages 386, index
Reviewer: The reviewer is CIA's chief historian.

Charles Dickens's 1853 novel *Bleak House* centers around an interminable probate case, *Jarndyce and Jarndyce*, that bleeds the estate in question of all its value and leaves the eventual inheritor with nothing. The campaign of Margaret Thatcher's government during 1985–91 to use the Official Secrets Act to prevent publication, and even public discussion of, the memoir of retired MI5 officer Peter Wright, *Spycatcher: The Candid Autobiography of a Senior Intelligence Officer*, has a similarly ironic outcome and produced a backlash akin to the British government's failed attempt in 1960 to ban *Lady Chatterley's Lover* under the Obscene Publications Act.

Motivated by the desire to prevent unauthorized disclosure of classified information and to protect MI5 from criticism, the effort must rank as one of the most counterproductive exercises in official censorship ever attempted. It cost the British government £3,000,000 pounds (over $10,000,000 today) and caused it severe domestic and international embarrassment. In *To Catch a Spy: How the Spycatcher Affair Brought MI5 in from the Cold*, investigative journalist and documentarian Tim Tate cogently and comprehensively lays out the inconsistency, duplicity, stubbornness, and shortsightedness of London's wasteful and futile effort to suppress Wright's book.

The damage done went far beyond discrediting the Thatcher government. It also resurfaced allegations of high-level Soviet penetration of MI5 and demonstrated that the service, because it was officially unacknowledged, essentially operated without legal restraints or parliamentary oversight. Despite doggedly resisting the patent need to hold MI5 accountable in some fashion, in the end the Thatcher government had to allow the service to be statu-

All statements of fact, opinion,or analysis expressed in this article are those of the author. Nothing in the article should be construed as asserting or implying US government endorsement of its factual statements and interpretations.

torily recognized and placed under ministerial review. That was only one of the ironies of the *Spycatcher* affair. Another was that the unsuccessful pursuit of the down-at-heels Wright turned his book—eventually translated into 11 languages—into a blockbuster bestseller that made him a millionaire.

Tate ably tells two stories in *To Catch a Spy*. The first is biographical; it recounts Wright's early life, limited education—he was expected to get a scholarship to Oxford or Cambridge until a family crisis forced him to find a job—work with the Royal Naval Scientific Service (RNSS) during and after WWII, courtesy of a family friend's intervention, and then in 1955 starting with MI5. He was a gifted but prideful and irascible technologist who contributed to advancements in electronics, but he also resented established scientists who viewed him as an impertinent outsider.

Wright's introduction to the world of counterintelligence had come before he joined MI5, when the head of the RNSS chose him to join a technology advisory committee. He found RNSS surveillance equipment and capabilities to be backward and was soon working on modernizing them. During this time he figured out how the never-before-seen microphone the Soviets had implanted in a wooden replica of the Great Seal of the United States hung in the US ambassador's office in Moscow worked—the device had baffled American scientists who examined it.

After joining MI5, Wright became involved in a series of counterespionage and security investigations that demonstrated the service's special powers and ability to operate on the edges of the law and beyond "in the defence of the realm," as its operating directive stated. A main target was the Communist Party of Great Britain. Since the 1930s, MI5 officers and agents had infiltrated party branches to find out what members were doing to aid the Soviets. Break-ins, phone taps, and surveillance were standard methods. "And we did have fun," Wright recalled in his memoir. "For five years we bugged and burgled our way across London at the State's behest, while pompous bowler-hatted civil servants in Whitehall pretended to look the other way." (52)

At the same time, Wright continued devising ingenious technical modifications to MI5's equipment. Despite the advances and initial successes against Soviet Bloc facilities, however, nothing worked well for long for most of the 1950s, leading Wright to conclude that Moscow had a mole inside MI5 who was blowing the operations. This assessment led to the most contentious and divisive episode in Wright's career. Energized by revelations and allegations of Soviet espionage against the UK, he joined some like-minded MI5 colleagues in inconclusive investigations of MI5 Director Roger Hollis and Deputy Director Graham Mitchell. Former MI6 officer Kim Philby's defection to the Soviet Union in 1963; the exposure of Anthony Blunt, the Surveyor of the Queen's Pictures, in 1964 as a member of what would come to be known as the Cambridge Five; and information shared by CIA's Counterintelligence Staff reinforced Wright's suspicions of treachery. In the course of his inquiries, he encountered distressing evidence of MI5's slovenly security practices, nurtured by a culture of Oxbridge clubiness and an abject fear of controversy, all of which Tate depicts exceedingly well. Wright also led an extraordinarily bizarre and illegal effort by a cabal of rogue MI5 officers to blackmail Labor Prime Minister Harold Wilson into resigning because they thought he was a Soviet agent.

Wright retired in 1976 in an highly conspiratorial frame of mind with none of the numerous MI5 officers he suspected of espionage having been caught. His last official act was signing an acknowledgment that in retirement he was still bound by the Official Secrets Act and prohibited from disclosing in any form any classified information he had learned in his 20-year career. He also discovered that MI5 would not honor an agreement made when it hired him to include his 14 years with the RNSS in his pension calculation because the benefit supposedly could not be transferred to a service that did not officially exist. That left Wright with only 60 percent of what he had been promised—not enough to live on, so in desperation he looked for other sources of income.

At a point Wright agreed to partner with the well-connected national security journalist Chapman Pincher. By then, having emigrated to Australia and living in a run-down dwelling in Tasmania hoping to become a horse breeder, Wright had composed a discursive, unpublishable memoir; Pincher would

use its information in a book and split the proceeds. Victor Rothschild, the fabulously wealthy Third Baron Rothschild who worked for MI5 during WWII, loomed in that relationship as a benefactor and middleman. Tate is unsparing in his evaluation of the trio, especially Pincher, as they connived to expose MI5's shady past: "Rothschild and Wright were professional dissemblers, willing and able to lie without remorse in the course of their duties or in pursuit of their individual goals; but of the three conspirators, it was the journalist whose duplicity and ruthless self-interest would cause the greatest trouble." (135)

The result of their dubious collaboration was Pincher's soon-to-be-notorious exposé of communist infiltration of Britain's society and government, *Their Trade is Treachery*. In the House of Commons, Thatcher denied the book's claim that Hollis was a Soviet agent. That exoneration and her assertion that Soviet infiltration of MI5 had been thoroughly investigated infuriated Wright. Around that time, two developments occurred that changed his life and turned *To Catch a Spy* into a captivating legal drama, which Tate relates with verve: the British government took steps to stifle public discussion of its intelligence services, and English television producer Paul Greenglass approached Wright for an interview about the Hollis matter. It aired in July 1983 and gave Wright a platform for accusing Hollis of espionage and Thatcher for misleading Parliament. As Tate observes, "Peter Wright was an unlikely whistleblower. Virulently right-wing and rabidly anti-communist.… It was an unseen irony that a man whose every political instinct and prejudice matched that of the Iron Lady in Number 10 was now marked out by her advisors as her enemy." (1, 166)

After Wright had Greenglass ghost-write *Spycatcher* and an Australian publisher agreed to print it, Thatcher's suppression operation would play out in courts around the world with Australia at center stage as she and her advisers sought to enjoin not just its publication but any open discussion of it in the UK and, later, parts of the British Commonwealth. In addition to Wright, the *dramatis personae* were his counsel, future Australian Prime Minister Malcolm Trumbull, and Thatcher Cabinet Secretary Robert Armstrong. Trumbull was then a brash, new lawyer, who was helped by a filing blunder by Her Majesty's lawyers that placed the trial in Sydney, a more liberal venue than Melbourne, where it should have been held. Also helping was the oversight of Justice Philip Powell, who would grow increasingly frustrated by the British government's legal tactics, procrastination, and double standards.

Trumbull's target was the smug and arrogant Armstrong, reluctantly dispatched to Australia along with a cohort of bewigged government lawyers and well-tailored Whitehall bureaucrats to defend London's flimsy case. Perhaps its most fundamental flaw was that for years former intelligence officers had discussed their work publicly, and books of their recollections or interviews with them had been published without sanction—including the memoir of former MI5 Director Percy Sillitoe, Nigel West's *A Matter of Trust: MI5, 1945-72*, and Pincher's *Their Trade is Treachery*, the latter two containing much of what was in *Spycatcher*. Trumbull also had other points in his favor, including that an Australian court ruled in 1980 that an official claim of confidentiality could only succeed if the information was truly confidential—hardly the case after the publication of Pincher's book. Tate's narrative then builds in suspense as he describes the trial, including details of Turnbull's courtroom theatrics, which he used to eviscerate London's case. Tate effectively addresses Turnbull's week-long inquisition of Armstrong that would leave the latter's reputation in tatters.

The affair would turn into a farce outside of the court, as a US edition of *Spycatcher* became readily obtainable in the UK even though it was officially banned and public libraries had to remove imported copies of it from their shelves. Yet, Tate acerbically notes: "One of these imported copies was formally placed in the House of Commons library, ensuring… that MPs could enjoy Wright's dangerous memoirs over restorative drinks in one of the House of Commons' many bars. Less privileged institutions, however, found themselves unable to share the book with their readers." (305) Tate adds several more ludicrous examples.

Powell's 85,000-word, 286-page decision, handed down in March 1987 and upheld on appeal, categor-

ically rebuffed London's position. "[W]hen one observes all the information [in *Spycatcher*]—much of it derived from, and some of it directly attributed to 'insiders'—which because of the British Government's acquiescence or inaction, has already been made available, the claim now that the republication of such information at the hands of an 'insider' will cause detriment sounds decidedly hollow…" More rejections of the Thatcher government's position followed in Powell's ruling. "As the day wore on," Tate notes, "it was clear that the British Government was receiving a historic judicial spanking." (277, 281)

Undeterred, the Prime Minister had her Attorney General seek to enjoin three prominent British newspapers from publishing details from Wright's book (two other newspapers had already been similar prohibited from reporting on it and the trial) and to curtail publicity about it and the Australian proceedings in the Hong Kong and New Zealand press. Appeals, counterappeals, and other of the government's legal maneuvers eventually lost it the backing of the Tory press. The *Times of London* told its readers that "No-one except Britain's enemies can take comfort from the sight of Mr. Peter Wright growing in international respectability…as his governmental pursuers fall over their own feet in embarrassment and failure." (309)

The Law Lords, Britain's highest judicial body, ended *Spycatcher*'s legal travails in October 1988. After upbraiding Wright for "heinous treachery" and a "flagrant breach of [his] duty of confidence," they declared that "It seems…to be an absurd state of affairs that copies of the book…should now be widely circulating in this country, and that at the same time other sales should be restrained. This simply does not make sense.…[We] do not see why anybody in this country who wants to read it should be prevented from doing so." (314) Further consequences to 10 Downing Street soon followed. Injunctions and contempt of court proceedings against some British newspapers were either lifted or rendered nugatory. In November, the Queen's Speech—the traditional opening of a new Parliament—included the announcement that MI5 would be given legal standing for the first time in its history. In addition, a new Official Secrets Act relaxed government secrecy strictures and provided a public-interest defense for whistleblowers, although the intelligence and security services were exempted from that provision. Lastly, the Intelligence Services Act of 1994 finally acknowledged the existence of MI6 and brought it, MI5, and the SIGINT service GCHQ under parliamentary control. A senior executive from Wright's Australian publisher later concisely summed up the whole fiasco: "Everything the British government was ostensibly trying to do, it achieved the opposite." (317)

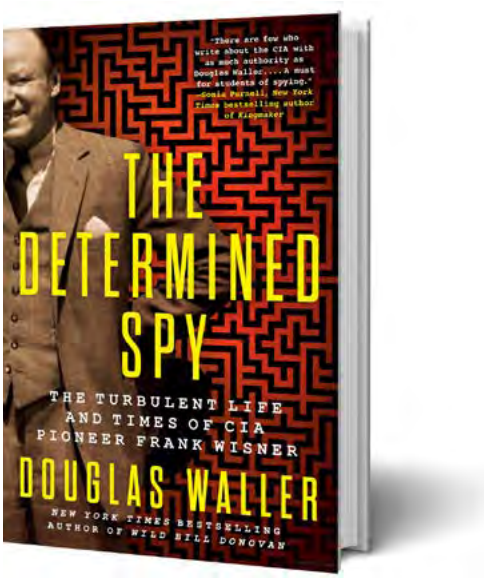
Tate's book makes easy reading, as he has the documentarian's narrative flair for clear prose and teasers and grabbers to close and open successive chapters. His sympathies clearly lie with Wright, whom he too often calls "the old spycatcher," while no one in Thatcherite officialdom evades his sharp pen. Sometimes he overdoes it, as when newspapers and judges "thunder" and "growl." For material about MI5, he frequently relies on Christopher Andrew's official history, published in the United States in 2009 as *Defend the Realm: The Authorized History of MI5*, but Andrew never cites specific MI5 documents, referencing only "Security Service Archives," so Tate's readers cannot independently evaluate some of his sources. Also, he too often uses Wright's memoir as his sole direct source about the service's activities. Tate has uncovered a wealth of documentation, much of it only recently declassified, but in his Epilogue and Acknowlegments he is unsparing in his criticism of British records-management officials and practices.

To Catch a Spy should resonate with information management officers in the US Intelligence Community today because it describes a conundrum they wrestle with constantly when reviewing current and former officers' writings and statements: how to evaluate the national security implications of information that is known to the public. The *Spycatcher* affair, so well recounted in Tate's book, offers observations and insights for those who labor in this arena. ■

intelligence in public media

The Determined Spy: The Turbulent Life and Times of CIA Pioneer Frank Wisner

Reviewed by JR Seeger and Ian B. Ericson



Author:	Douglas Waller
Published By:	Dutton, 2025
Print Pages	645, index
Reviewers:	JR Seeger is a retired CIA officer. Ian B. Ericson is the pen name of a CIA officer.

Frank Wisner was a consequential figure in the history of CIA and covert action, as this pair of reviews by veteran intelligence officers makes clear. – The editors.

By JR Seeger

In its first decade of existence, CIA faced numerous challenges, from worldwide Cold War conflicts to the hallways of power in Washington, DC. During this time, the majority of CIA leaders were veterans of the Office of Strategic Services (OSS). Their world view was shaped by seeing firsthand the devastation of total war and the transformation of the USSR from ally to adversary. One of these leaders was a young lawyer from Mississippi named Frank Wisner. In his short life of 56 years, Wisner created CIA covert action capabilities that remain in CIA today. This monumental biography by the author of *Wild Bill Donovan* delivers an understanding of the man, his times, and his covert action operations. It is a must read for anyone interested in the history and culture of CIA.

A deep understanding of Frank Wisner requires knowledge of the man who lived inside and yet apart from two great US intelligence organizations, OSS and CIA. Both organizations were filled with sons and daughters of privilege. Almost all the early leaders were often labled "male, pale, and Yale." Wisner grew up the son of a Mississippi industrialist and went to the University of Virginia for his undergraduate and law degrees. He was already a US Navy reserve intelligence officer when Imperial Japan attacked Pearl Harbor. He thrived in Naval intelligence, where his legal mind and commitment to detail brought him to the attention of early OSS leaders. Wisner attended a brief OSS training program in October 1943 and received orders for OSS/Cairo. He arrived in December 1943 as the station's chief of reports.

All statements of fact, opinion,or analysis expressed in this article are those of the author. Nothing in the article should be construed as asserting or implying US government endorsement of its factual statements and interpretations.

Not long after his arrival, Wisner again came to the attention of OSS leadership through his work in Cairo. According to Waller, he transformed the station reporting both on the collection and production sides by designing collection requirements and by demanding clear and concise reports. His successes in Cairo led to reassignment in June 1944 to Istanbul and then to a command position in Bucharest three months later.

In Bucharest, Wisner came in contact with the Soviet military and intelligence establishment for the first time and came to learn the Soviet tactics designed to make certain that Romania would become a client state. Wisner worked with OSS/X2 (counterintelligence) officer Robert Bishop to understand and counter the Soviet effort. In this first battle against the Soviets, Wisner began to understand better than many in OSS that the Soviet Union was in transformation from a reluctant ally to an implacable adversary.

Waller reports:

Until the end of his mission, Frank Wisner continued to send Donovan's headquarters cables that Moscow was intent on establishing pro-Soviet regimes in all of Eastern Europe.… For the rest of his life, he held a personal grudge against the Russians. In Romania, he began a long cold war against the Soviet Union. (99)

After VE Day, Donovan named three OSS officers to lead collection in Germany: Allen Dulles became the chief in Berlin and the commander of OSS in Occupied Germany; Richard Helms and Frank Wisner took over the operational component responsible for collection in Germany, Poland, and Czechoslovakia. Helms and Wisner left Germany in December 1945 after OSS had been disbanded. At that point a much smaller, more bureaucratic Army Strategic Services Unit took on intelligence collection in Germany as the Soviets were ramping up their efforts to control Eastern Europe.

Wisner tried to return to civilian life, but by October 1947 he had joined State Department as the head of a joint military-civilian "coordinating committee on Europe." It was at this time that Wisner became a member of the Policy Planning Staff, which was run by George Kennan. Kennan's May 1948 State memorandum on political warfare sent Wisner down that path for the rest of his federal career.[a] As part of Kennan's plan, Wisner offered a program titled BLOODSTONE, which would become the Office of Policy Coordination (OPC), which Wisner managed under the joint command of State, Defense, and the newly formed CIA.

Wisner was known for his ambition and his work ethic. By 1948, he offered a plan for OPC to conduct the following covert action programs: psychological warfare, political warfare (specifically subversion), economic warfare (manipulating adversary banking), "preventative" direct action (paramilitary operations), and a catch-all program titled "miscellaneous." Wisner operated in an administrative shadow world in which few of his supervisors knew anything about OPC activities and President Truman's White House offered little resistance, and even less guidance, on how OPC would counter the Soviet and, by 1949, Communist Chinese threats.

The book's third of four parts[b] (by far the largest), outlines the projects OPC initiated, the bureaucratic challenges Wisner faced, and the eventual fusion in 1951 of OPC with the Office of Special Operations (human intelligence [HUMINT] operations) into a new entity, the Directorate of Plans. The merger had been ordered by Director of Central Intelligence Walter Bedell Smith, who during his tenure as DCI (1950–53) restructured and rationalized an organization that had been largely ignored by the first directors. While Wisner's days of working the "gaps and seams" between State, Defense, and CIA were over, his operational role increased under the first DDP, Allen Dulles, and after August 1951, when he replaced Dulles, who had been made deputy DCI.

a. Archived Department of State memorandum. George Kennan, Policy Planning Staff Memorandum, May 4, 1948. "The Problem: The inauguration of political warfare." Archive.law.upenn.edu

b. Parts one and two address Wisner's youth and activities during World War II, respectively. The final part focuses on Wisner's mental illness and last years of life.

Wisner's covert operations defined the first decade of the Cold War. Waller takes the reader through each effort and details why they succeeded or failed. He manages to do so without being either a cheerleader or a hostile prosecutor of Wisner or his programs.

Part Four, which goes into the late 1950s and the first five years of the 1960s, Waller describes Wisner's tragic descent as DDP into manic-depression—now referred to as bipolar disorder. Genetically predisposed to the illness, and after some time in a mental health institution where he received electro-shock therapy, he briefly returned to CIA and a post in London before he retired. About three years after his retirement he committed suicide in 1965.

As with his biography of Donovan, Waller's work on Wisner is thoughtful and exceptionally well-researched. He is a master of blending archival research with letters and papers of his subject as well as of his subject's peers and even adversaries. Waller brings to light the Cold War complexities that faced four presidents and five DCIs during Wisner's career. Even if a reader is not interested in Wisner's life or CIA covert action, this book is a must read for anyone interested in the early Cold War and the creation of the intelligence establishment that remains critical today. ■

By Ian B. Ericson

The legend of CIA was built thanks to a founding generation of officers who cut their teeth in the OSS during World War II and leveraged that experience to confront a bold and aggressive new Soviet adversary. Frank Wisner, OSS veteran and inaugural head of CIA's Directorate of Operations, personifies the OSS's reputation for daring and indefatigable devotion to mission. Douglas Waller's new biography of Wisner, *The Determined Spy*, is an invaluable addition to the literature on this remarkable, tragic figure without whom the early history of CIA could not be written.

Wisner was born in 1909 and raised in Laurel, Mississippi. His father was a wealthy lumber entrepeneur who had married into the business. Waller's description of Wisner's childhood, education, and overall formation is thorough, perhaps even too thorough, given some of the gaps in the author's account of Wisner's work at CIA. Wisner excelled athletically and academically at the University of Virginia, receiving his bachelor's degree in 1931, followed by a law degree in 1934, both with top academic honors. He continued to shine as a New York attorney at the law firm of Carter, Ledyard, and Milburn, and in 1936 married Polly Knowles, the daughter of a New York shipping magnate. Wisner was flourishing professionally and personally.

Like so many of his generation, however, it was during WWII that Wisner found his purpose. In part due to his New York law connections, Wisner obtained a position in the OSS in 1943. He served with distinction in Cairo, Bucharest, and finally Berlin after Germany's surrender in May 1945. Waller's account of Wisner's time in OSS is detailed and compelling, especially his descriptions of Wisner's tours in Romania and Germany. Wisner became intimately familiar with the intelligence business, particularly as it related to covert action—activities intended to secretly influence the political, military, or economic conditions of a foreign country. He also saw firsthand the depravities of the Red Army and the communist system it forced upon the citizens of Eastern Europe. Wisner grew to love Romania and its people during the war, and watching the Soviets snuff out Romania's independence profoundly affected him and influenced his aggressive anti-communist efforts while at CIA.

Wisner returned to the practice of law—an industry that no longer suited his temperament —with the OSS's dissolution at the end of September 1945. In 1948, George Kennan, Director of the Policy Planning Staff at the State Department, recruited Wisner back into the fight as the first head of CIA's covert action arm, the inconspicuously named Office of Policy Coordination (OPC). Wisner's boundless—almost maniacal—energy perfectly suited him to the task. Waller notes that the impetus for OPC's frenetic pace came from policymakers, including Kennan, looking for a third option to confront communism that went beyond diplomacy but did not involve full-scale war.

Wisner was certainly eager to launch operations against the Soviets, but he was sensible enough to

realize that he needed to organize OPC first. Kennan and others at State and the National Security Council would hear none of it, however, fearing that delay on the covert policy side would blunt the effectiveness of the Marshall Plan. Kennan reviewed Wisner's plans for covert operations in 1949 and 1950 and added to the list. Kennan's later insistence that he never intended OPC to cast such a wide net and that he deeply regretted the existence of OPC ("the worst mistake I ever made") is disingenuous to say the least in light of his contemporary marching orders to Wisner. His later misgivings notwithstanding, Kennan's de facto orders to intensify covert subversion of the Soviet bloc set the tone for OPC activity in the 1950s.[a]

Waller does an excellent job analyzing CIA's various covert activities in the late 1940s and early-to-mid 1950s. Wisner immersed himself in the minute details of each operation, working at a pace that would have broken just about anybody and that most likely exacerbated his genetic predisposition to bipolar disorder, or what was then called manic depression.

Waller skillfully describes the historical background and details of CIA's covert efforts to overthrow the governments in Albania (late 1940s), Iran (1953), and Guatemala (1954), well known operations that nonetheless remain poorly understood. Waller is mostly fair in his descriptions of the events, recognizing for example that it was internal opposition to Iran's mercurial Prime Minister Mohammed Mossadegh and not CIA machinations that played the decisive role in Mossadegh's removal. In his epilogue, however, he cannot resist repeating the canard that CIA overthrew the "democratic regime" in Iran. In fact, the shah exercised his constitutional prerogative to remove Mossadegh, who illegally refused to leave office.

The chapters that describe Wisner's mental breakdown, his temporarily successful convalescence at Sheppard and Enoch Pratt Hospital in Maryland, the toll the disease took on his family, and Wisner's suicide in 1965, are movingly written and among the book's best. Waller writes of the support Wisner received from friends and colleagues at CIA, especially as his condition became impossible to ignore during the twin international crises in Hungary and Egypt in 1956. Waller received invaluable assistance from Wisner's children to fill out this part of the narrative, and even decades later it is clear the memories are bitter.

The book's flaws relate mainly to what it omits. Beginning in 1952, when OPC and the Office of Special Operations merged to form the Directorate of Plans, Wisner was in charge of traditional HUMINT as well as counterintelligence (CI), in addition to covert action. Waller is almost completely silent on CIA's HUMINT and CI efforts, ignoring for example CIA's recruitment and handling of GRU officer Pyotor Popov in 1953 and the appointment of James Angleton as CI chief in 1954. Insights into how Wisner approached operating behind the Iron Curtain or vetted agents would have filled out the narrative considerably.

Wisner's tour as CIA's chief of station in London was also far more eventful than Waller acknowledges. While Wisner was there, CIA passed leads from it's Polish source, Michael Goleniewski, that led to the identification of numerous Soviet spies operating in Britain, including MI6 officer George Blake. Wisner would have been intimately involved in joint efforts to run to ground Goleniewski's information, but the threadbare chapter on Wisner's time in London focuses instead on the return of his mental instability, which only reappeared nearly two years into his tour.

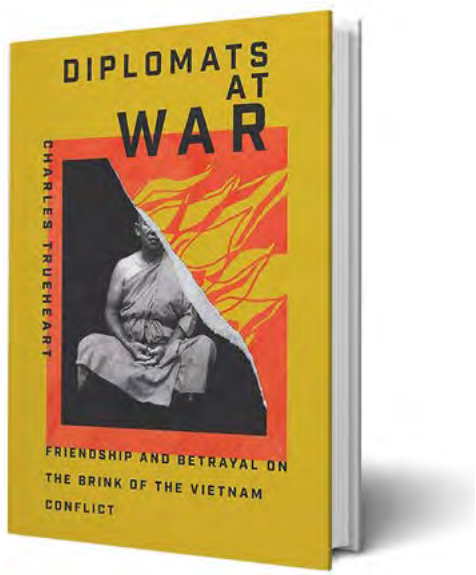
Despite these deficiencies, Waller's book remains an important contribution to the intelligence literature on CIA's formative years. Waller's prose is crisp and compelling, and the volume never bogs down despite its hefty 526 pages, plus index and endnotes. It is an achievement and a fitting tribute to its legendary subject. ■

a. US Army historian Thomas Boghardt addressed one product of this strategy in this journal: "Liberation: US Operations to Counter Soviet Occupation of Ukraine, 1949–1953," *Studies in Intelligence* 67, No. 3 (September 2023) [Classified U//FOUO]. See also Frank Costigliola, *Kennan: A Life Between Worlds* (Princeton University Press, 2023) and Benjamin Nathan's review of the book, "The Enigma of George Kennan," in *New York Review of Books*, April 24, 2025.

intelligence in public media

Diplomats at War: Friendship and Betrayal on the Brink of the Vietnam Conflict

Reviewed by J. Daniel Moore



Author: *Charles Trueheart*
Published By: University of Virginia Press, 2023
Print Pages 368
Reviewer: Daniel Moore is a retired CIA historian.

Author Charles Trueheart writes in the Prologue to *Diplomats at War*: "The origin of war, like the origin of a personal conflict, is almost always murky." He eloquently proves the point in this winner of the 2024 Douglas Dillon Award from the American Academy of Diplomacy. This important book is rich in insights and analysis. It details the critical events and decisions in the months leading up to the Vietnam War, especially with respect to US policy and among key diplomatic actors and journalists in Vietnam and Washington. The author demonstrates the refined research and analytical skills one expects from an accomplished historian: a mastery of primary and secondary sources—various archives, state department records, oral histories, personal interviews, and letters written by his mother, to name just a few. He throws in ample doses of effective humor as well.

A distinguished former correspondent of *The Washington Post* and former associate director of the Institute of Politics at Harvard, Trueheart calls *Diplomats at War* a "work of memory hiding inside a work of history." (11) The son of William Trueheart, the US Embassy's deputy chief of mission in South Vietnam in the early 1960s, Charles was a young witness to the crucial events that led to the US-engineered downfall of Republic of South Vietnam President Ngo Dinh Diem in November 1963.

On the personal side, he observed the crumbling of his father's longtime personal friendship and close professional association with his boss in Saigon, Ambassador Frederick "Fritz" Nolting. The two families had been close for years—Nolting was Charles's godfather. William Trueheart and Nolting attended the University of Virginia together before World War II. They had planned

All statements of fact, opinion,or analysis expressed in this article are those of the author. Nothing in the article should be construed as asserting or implying US government endorsement of its factual statements and interpretations.

for academic careers but served in the military during the war and later joined the foreign service.

But Trueheart and Nolting came to bitter loggerheads over whether the United States should stand by Diem or encourage Diem's generals to do the dirty work of removing him from power. Sixty years on, the author's quest to understand how and why their relationship fractured to the point that they never spoke again after leaving Saigon—other than during a brief, chance meeting years later at the Metropolitan Club in Washington, DC—constitutes the backstory that propels this powerful narrative.

Charles Trueheart makes America's drift toward a decade of war seem almost inevitable. He details how Washington policymakers turned against Diem in favor of a military junta more favorable to US geostrategic policy aims. Importantly, the "hawks," who included key presidential adviser and Undersecretary of State Averell Harriman, NSC staff member Michael V. Forrestal, and Bureau of Intelligence and Research Director Roger Hilsman at State, had the ear of President Kennedy.

Collectively, they gradually persuaded an indecisive and hesitant Kennedy that regime change was necessary. The president had had a keen interest in South Vietnam since the partition of 1954. In a 1956 speech to the Conference on Vietnam in Washington, then-Senator Kennedy said, "If we are not parents of little Vietnam, we are the godparents. We presided at its birth, we gave assistance to its life, we helped shape its future." Indeed, South Vietnam had been a dependent client of the United States from its very beginning.

Throughout 1963, US journalists David Halberstam of the *New York Times*, *The Associated Press*' Malcolm Browne and Peter Arnett, and *Time* correspondent Stanley Karnow exposed the failures of South Vietnam's military to stop communist insurgent gains and highlighted the US Embassy's unsuccessful efforts to paint more positive pictures of events. Press reports followed closely by the president contradicted and undermined more optimistic narratives from Nolting and US Military Assistance Command Vietnam (MACV) Gen. Paul Harkins. Trueheart similarly describes CIA intelligence as too optimistic, offering an overly optimistic view of the situation in the countryside. Collectively, the journalists corroborated the hawks' view that the Diem regime would be unable to contain the growing insurgency in the countryside.

The Buddhist uprising against Diem in the summer of 1963 and the resultant harsh government crackdown was the last straw for Diem's detractors in Washington. They argued that Diem's removal—and that of Nolting—was necessary for the success of US objectives in Vietnam and, more importantly, to stop the spread of communism in southeast Asia. In the end, after some handwringing, Kennedy acceded to regime change, and Nolting was replaced by hawk Henry Cabot Lodge.

Nolting left his post in mid-August 1963, leaving Trueheart as charge d'affaires. He departed still believing in supporting Diem and vainly argued his case in Washington. In his absence, Trueheart joined the chorus of the hawks in Washington, which led Nolting to view his former deputy as a traitor to their shared mission and friendship.

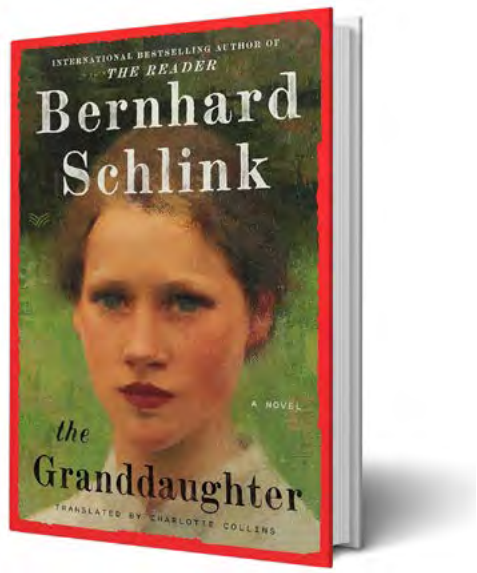
President Kennedy was assassinated three weeks after the coup in Saigon and Lyndon Johnson, who had supported Diem, found himself steering the deepening US involvement in Vietnam. Diem's replacement by a South Vietnamese military junta, beholden entirely to US support, set the stage for the introduction of US military forces in early 1965.

Looking back years later, Nolting observed: "We do not overthrow governments. We keep our word to our allies. We are loyal to our friends." In an interview later in life, William Trueheart agreed with Nolting in principle, with one exception, Vietnam in 1963: "We [the United States] felt we had a broader commitment than just Diem. We had a commitment ... to the Vietnamese people. To do anything to perpetuate the Diem regime was not in the interests of the United States." (360) His son, the author, takes exception. Overthrowing governments, he concludes, is not worth the cost. On that principle, he concludes, William Trueheart and Fritz Nolting would likely agree. ■

intelligence in public media

The Granddaughter: A Novel

Reviewed by Graham Alexander



Author:	Bernhard Schlink (Charlotte Collins, trans.)
Published By:	HarperVia, 2024
Print Pages	336
Reviewer:	Graham Alexander is the pen name of a CIA operations officer. Here he reviews the original German-language version first published in 2021.

Bernhard Schlink, a lawyer, academic, and novelist, uses his latest novel, *The Granddaughter,* to assess the ramifications—cultural, political, and familial—of Germany's experiences with right- and left-wing authoritarianism during the 20th century, a formula deployed in many other German works, including his own. Throughout the novel, Schlink displays an admirable ability to shape and mold prose on top of a narrative that is uniquely German. Numerous scenes are instantly memorable, not only because Schlink has a knack for crafting dialogue, but because he has the ability to frame thoughts through silence while transmitting to readers a sense of the sights, smells, and sounds that are often indelible atmospheric elements in human interactions.

The Granddaughter is a speedy and worthwhile read, especially for those interested in the ramifications of two failed German police states for the current climate in Germany. Schlink's work deserves respect for his willingness to explore the idea of how successor generations cope with and interpret the past: a term Germans know as *Vergangenheitsbewältigung*. Schlink's knack for precise prose succeeds in making these complicated questions of morality, guilt, and motive more accessible to readers than authors like Gunter Grass or W.G. Sebold, who have also covered this ground.

Schlink's own political biases are clear as the novel unfolds and gradually evolves into a parable. He argues between the lines that the ability of the German people to jump out of the long shadow of their 20th-century past hinges upon their willingness to adopt a centrist political ideology linked to Enlightenment values. He is admittedly passionate and eloquent in pushing this argument,

All statements of fact, opinion,or analysis expressed in this article are those of the author. Nothing in the article should be construed as asserting or implying US government endorsement of its factual statements and interpretations.

but his message is bound to land more persuasively on some readers than on others. This understood, *The Granddaughter* succeeds on the same terms as Schlink's first novel to explore this terrain, *The Reader*, in sparking both debate and reflection among readers far beyond the borders of the Federal Republic. Since it was first published in German in 1995, *The Reader* has been published in some 40 languages and won literary awards in numerous countries.

The Granddaughter chronicles the experiences of a 70-something German widower named Kaspar, who tries to understand the life experiences and enigmatic behavior of his late, alcoholic wife, Birgit. Living in modern Berlin, Kaspar seeks to complete Birgit's autobiographical novel, which he discovers only after her unexpected death. In the book, Birgit had meditated on her life in East Germany, a life he helped her escape in the 1970s, and the consequences of East Germany's dissolution in 1990. Most poignantly, Kaspar learns that Birgit had given birth to a daughter just before she defected. Birgit's ignorance of the child's fate tormented her silently in the years that followed. Kaspar eventually succeeds in locating the grown daughter, Svenja, and discovers that she is living in a segregated, neo-Nazi community in eastern Germany. He forms an immediate attachment to Svenja's 15 year-old daughter, Sigrun, and persuades both Svenja and her suspicious husband to permit Sigrun to visit him semi-annually in Berlin.

Schlink plays skillfully through this narrative in his descriptions of Kaspar and Birgit. Kaspar is clearly an intelligent, cultured man and a subconscious product of the cosmopolitan, *weltoffenes* image that underpinned the Federal Republic since its inception in 1949. Birgit, in contrast, is a product of the authoritarian Marxist Germany into which she was born and matured, even as she formed an identity in silent rebellion against it.

Schlink's own experiences living in a divided Germany help him frame these characters in ways that are convincingly authentic. Kaspar, like many West Germans, regards Easterners as hopelessly indoctrinated and narrow-minded, an afterthought banished to history after 1990. Birgit, for her part, suffered both the anguish of having abandoned her daughter and seeing her own land disintegrate. Many East German readers likely will nod emphatically reading long passages from Birgit's incomplete novel. They do not mourn the death of a state whose legitimacy was never real, but at the same time, they are never truly reconciled to their roles in a reunited Germany or to adopting collective amnesia about East Germany's legacy.

Schlink is on sound footing through the first half of the novel, but its complexion changes once Svenja and Sigrun emerge. Where Birgit is a three-dimensional character tormented by mistakes and ambivalent about her identity, Svenja and especially Sigrun present as two-dimensional caricatures of what German and foreign media commentators have labeled "the far-right." Schlink uses the Sigrun character to voice a number of platitudes pushed by persons of this political persuasion.

Kaspar is clearly the most sympathetic actor, however, since Schlink uses his words on several occasions to rebut the rightist arguments and demonstrate how Sigrun is utterly defeated in response. Kaspar's goal throughout this section of the novel is clearly to conduct a covert battle for Sigrun's liberation, so as not to alienate Sigrun's increasingly suspicious parents. As noted, the reader may wholeheartedly detest the objectives of Germany's far-right and applaud Kaspar's motives, but stylistically, Schlink's abandonment of neutrality toward the East Germans and his own sympathy for Kaspar conspire to engineer a palpable shift in tone. To Schlink's credit, the novel ends ambivalently, without a resounding triumph for any side. This ultimately makes *The Granddaughter* a worthwhile read and one worth pondering as a paradigm of the modern Federal Republic, where competing historical narratives and their legacy still vie for supremacy within millions of hearts and minds. ■

intelligence officer's bookshelf

Compiled and reviewed by Hayden Peake, Anthony Sutton, John Ehrman, and Resolute Lee.

Contemporary Issues

Authoritarianism: A Very Short Introduction
By James Loxton
(Oxford University Press, 2024), 89 pages, index.
Reviewed by Anthony Sutton, an analyst in the Strategic Futures Group of the National Intelligence Council

Intelligence officers are often proud experts in a field, yet new problems and new assignments ask officers to build competence without time for a full course of study. James Loxton, a senior lecturer in comparative politics at the University of Sydney, offers a boon to officers newly encountering autocratic regimes. He delivers on the subtitle's promise, providing "a very short introduction" that makes the reader conversant in authoritarianism after an evening's effort.

Following modern convention, Loxton defines authoritarianism as everything other than democracy in the form of competitive elections decided by inclusive voter rolls. He subdivides autocracies into military, party, and personalist systems, modifying the most-popular typology by folding monarchs into the personalist set.

Readers glimpse how autocracies come about, especially through democratic breakdowns enabled by polarized citizenries or semi-loyal opposition parties that tolerate antidemocratic wings. Authoritarian regimes typically struggle to maintain popular legitimacy, collect accurate information, prevent elite defections, and manage leadership successions. Nonetheless, autocracies can endure, especially those with centrally controlled resources such as oil or revolutionary heritages that destroy rivals and bind elites.

Autocracies become more likely to evolve into democracies amid certain structural changes, like socioeconomic modernization, as well as more specific events, such as crises, mass mobilizations, and pacts with opposition leaders. Dying autocracies commonly bequeath constitutional carve-outs and successor parties that protect the interests and individuals that made up the predecessor regimes.

Loxton encapsulates his topic with breezy prose that invites straight-ahead reading. Yet the book earns shelf space as a reference, given its descriptive subheadings, tidy index, and generous guide to further reading. Loxton name-checks the giants of the field and conveys a sense of historical trends, preparing the reader to engage with specialists. He hints at the statistics underlying his summations but rarely slows to present numbers and never offers a chart. Instead, he relies on pithy lines like, "People loyal to democracy do not make deals with Nazis."

Loxton's work competes well with earlier introductions to authoritarianism. Erica Frantz's slightly more academic overview features more data, more depth on subcategories of autocracy, and more details about the fates of autocratic leaders.[a] Milan Svolik's opus provides a stronger organizing principle, inviting readers to derive authoritarian tendencies from the fact that leaders cannot credibly commit to share spoils with supporters, leaving potential or actual violence as the only arbiter of power struggles.[b] Ultimately, all three books are compatible. Loxton's introduction has the advantage of being newer, and —considering the relatively little time needed to take in 89 pocket-sized pages— he offers a great return on investment. ■

a. Erica Frantz, *Authoritarianism: What Everyone Needs to Know* (Oxford University Press, 2018).
b. Milan Svolik, *The Politics of Authoritarian Rule* (Cambridge University Press, 2012).

All statements of fact, opinion,or analysis expressed in this article are those of the author. Nothing in the article should be construed as asserting or implying US government endorsement of its factual statements and interpretations.

The Academic-Practitioner Divide in Intelligence Studies
Edited by Rubén Arcos, Nicole K. Drumhiller, and Mark Phythian
(Rowman & Littlefield, 2022) 318 pages, index.

Will students taking intelligence courses benefit more from a teacher who has learned the subject in academia or from one who has experience working in the intelligence profession? This formulation of the academic-practitioner divide in intelligence studies has no simple answer. In the early 1980s the question wouldn't have received much attention, at a time when there were few intelligence courses being offered at the college level. The circumstances are much different now, as the 31 contributors—four with prior service in intelligence organizations—from institutions teaching intelligence in Europe, North and South America and Australia make clear in 14 chapters.

Contributors David Omand (former director of GCHQ, now Teaching at Kings College) and Nicholas Dujmovic (former CIA analyst and historian and professor at Catholic University) discuss their experiences as practioners-turned adademics. Omand's purpose is "to describe the nature of the inevitable and necessary divide there has to be between the worlds of the practitioner and of the academic studying the specialized subject of secret intelligence, and to add my own testimony on how I made that transition myself and how best to construct secure connecting bridges across that divide." (4) Dujmovic views "the question of the academic-practitioner divide in the study of intelligence at colleges and universities is really the question of "who is teaching this subject?" and explains why. (59)

One view from an academic-only is given by Damien Van Puyvelde, a lecturer in intelligence and international security at the University of Glasgow and a research fellow at the Institute for Strategic Research (IRSEM, French Ministry for Armed Forces). He discusses the divide between academics and intelligence practitioners in France from the establishment of the "French school" of intelligence studies in the 1990s to today. (179)

The other contributors argue issues like who can best teach intelligence-related subjects and what should be the purpose of teaching or studying intelligence? Some insist that little can be learned "from intelligence studies faculty who lack a prior employment history with a three-letter agency or other organization that conducts intelligence." Others take the position "that faculty members without direct intelligence work experience can add value to the field, develop its conceptual underpinnings, research and explain aspects of its history, address problems of practice, and effectively teach intelligence-related topics." (1) The Army War College contribution (Genevieve Lester, James Breckenridge, Thomas Spahr) discusses these and related issues from the positions of a former intelligence officer and those from academia only.

The sourcing is excellent and includes mention of publicly available journals (e.g., *Studies in Intelligence*, and the *Romanian Intelligence Studies Review*). (254)

The Academic-Practitioner Divide in Intelligence Studies doesn't provide single best answers to the questions raised. But it does offer "a menu of ways in which the academic-practitioner divide can be mitigated … in pursuit of shared goals based around increasing knowledge and improving understanding of intelligence." (253).A valuable contribution. ■

History

Anti-American Terrorism: From Eisenhower to Trump—A Chronicle of the Threat and Response, Volume III The Clinton Administration
By Dennis A. Pluchinsky
(World Scientific, 2025) 984 pages, index.

After graduating from Madison College (now James Madison University) with a BA in Sino-Soviet Relations, Dennis Pluchinsky studied Russian at the Defense Language Institute, earned an MA in International Affairs from George Washington University, and in 1976, joined the US Department of State's Threat Analysis Group, one of the first government units to monitor terrorism.

For the next 28 years, he studied the anti-American terrorist threat and how the US government responded to it. From 1990 to 2015, he also taught counterterrorism-related courses at universities in the Washington area, at CIA's Kent School for Intelligence Analysis, and DIA's Joint Military Intelligence Training Center. In 2004, he was selected for the Director of Central Intelligence's Exceptional Intelligence Officer program, during which he conducted research on terrorist surveillance

methods, ruses, and disguises. He retired from the State Department in 2005.

Pluchinsky then became an adjunct professor, teaching terrorism courses at several private institutions, including George Washington, George Mason, and Georgetown Universities. While preparing for these courses, he "discovered that there was no single work that addressed the threat and response in terms of terrorism in the U.S. and overseas in the post-World War II era." He decided to write one that turned into five volumes. Three volumes, including this one have been completed. The first two were: *Volume I: The Eisenhower Through Carter Administrations*, which was published in March 2020, and *Volume II: The Reagan and George H.W. Bush Administrations*, which. appeared in June 2020. (16) Volume IV will examine the George W. Bush administration, and Volume V will cover the Obama and first Trump administrations. His goal is to create a work that will become a standard reference for future scholars, intelligence analysts, policymakers and historians.

As terrorist activity increased in each administration, so did the involvement of intelligence agencies. Volume III discusses the sometimes overlapping roles of the FBI, NSA, and CIA as they responded to three suicide terrorist operations against the United States. It also treats the growing role of CIA in monitoring al-Qa'ida, including the establishment of Alec Station, the unit created to track Usama bin Ladin. (647)

Each volume is thoroughly documented and includes Pluchinsky's assessment of actions discussed and opportunities missed. After noting that the "Clinton administration was the first to confront the global jihadist terrorist threat," Volume III adds it should have realized sooner that the United States needed to get much more aggressive and lethal with al-Qa'ida and the Taliban (933) The solution to that problem is left to Volume IV ■.

Book and Dagger: How Scholars and Librarians Became the Unlikely Spies of World War II

By Elyse Graham
(Ecco, 2024), 376 pages, index.

The first US centralized intelligence orgnization, the Office of the Coordinator of Information, was created on July 11, 1941. It was succeeded by the Office of Strategic Services (OSS) on June 13, 1942. OSS has been the subject of many books, but Stony Brook University historian Elyse Graham, who holds degrees from Princeton, Yale, and MIT, takes the position in *Book and Dagger* that OSS "reinvented intelligence" (xiv) But, like a pilot's first solo flight, things can only be invented once, and Graham would have been closer to the truth if she had merely pointed out that the OSS Research and Analysis Branch (R&A) was the first of its kind in an intelligence agency.

Graham makes two other claims about R&A worth noting. First, she writes that R&A would "reshape the global system of espionage," employing "scholars and the wonders they could work in the world of books and paper." (xiv) Second, this "Chairborne Division—depended on and produced hair-raising adventures in the field.... The war may have been fought on battlefields, but it was won in libraries." (xv) *Book and Dagger* does not support these assertions. It focuses instead on how, with the exception of Yale historian Sherman Kent, scholars with expertise were recruited, trained and sent overseas to conduct espionage, not what they did inside R&A or what intelligence they provided.

Book and Dagger, for example, describes the activities of several officers, including Joseph Curtiss—the "mild-mannered English professor from Yale"—and Adele Kibre—"dark-haired, wicked-eyed, a classicist by training" with a PhD in Latin from the University of Chicago. (4) To improve "reader understanding," of the events Graham describes, she admits to adding fictional material to her purported history, justifying the tactic by noting that for "the sake of continuity, I have included occasional imagined scenes in this book." (3, xx)

Graham spends considerable time commenting on OSS and its British and German counterparts. Before discussing any operations, she notes that the British SOE and "the OSS didn't yet know it, but the very weaknesses that made their own governments look down on them—they had to pull recruits out of libraries, for heaven's sake—would force them to introduce methods of information gathering and analysis that were so good they forever transformed the world of spycraft." (45) Neither assertion is accurate. Information gathering, gradually improved by technology, had been around for centuries, and analysis was a matter of adapting scholarly methods by specialists. Graham never realizes that academics and librarians were recruited only because they had needed expertise whether as an analyst or in field work.

The operations mentioned in *Book and Dagger* raise other issues. One example is the comment that "the most

famous deception operation of the war [was] the British-run Operation Mincemeat." (213) Many would argue that the D-Day deception, Operation Fortitude, deserves this honor. Another example is Graham's discussion of the Vermehren defection in Turkey. It was, as she notes, a very public embarrassment for Germany, but it didn't involve OSS.

Graham reaches some other conclusions that are not documented. For example she writes that "In the right hands, paper could be more effective than bombs as a weapon in the war." (85) And later clams that "because they weren't tied down by established ways of doing things, the professors and librarians of the OSS, and the refugees who joined them, were able to create something new." (297) But she doesn't say what was new.

Book and Dagger, in short, tells a little about what a few OSS officers did during WWII but almost nothing about the value of their work. Moreover, while most of the academics and librarians in OSS worked in the R&A Branch, she discusses many who performed clandestine operations overseas. Graham provides a mix of organizational confusion and operational misjudgments. Caveat Lector. ■

The Invisible Spy: Churchill's Rockefeller Center Spy Ring and America's First Secret Agent of World War II
By Thomas Maier
(Hanover Square Press, 2025), 479 pages, index.

The Invisible Spy accurately describes the book's central figure, Ernest Cuneo, as an ex-NFL player, attorney, and "liaison between White House and Churchill's spies." He was all those things and more, but his liaison work with British intelligence in New York did not make him a spy and certainly not "the first American spy of World War II." (13) And his wartime liaison work with OSS and the FBI didn't make him a spy either. But he was an interesting figure, and journalist/TV producer Thomas Maier tells his story well.

Ernest Cuneo was born in New Jersey on May 27, 1905, the son of Italian immigrants. He graduated from Columbia University and earned a law degree at St. Johns University. After a short professional football career with the Brooklyn Dodgers, he went to work for Congressman Fiorello LaGuardia, a job that started his lifelong devotion to politics, though he also retained private clients such as columnists Walter Winchell and Drew Pearson. Both played roles in Cuneo's liaison work.

Cuneo was also friends with several Columbia graduates were members of FDR's so-called "Brain Trust" and by the mid-1930s, he was appointed associate general counsel of the Democratic National Committee. He soon became a political operative for FDR, traveling back and forth between New York City and Washington, DC. (50)

Then, according to Maier, shortly before the United States entered WWII, the British sent William Stephenson to establish an intelligence station in New York. Stephenson's mission was to quietly promote US support for the war against Germany. Cuneo served as "Roosevelt's secret go-between the White House and the British … [and] formalized Cuneo's 'unofficial status as a spy for the president.'" During the war, Cuneo's liaison role was extended to the FBI and OSS. As liaison for Donovan, he dealt with the military, the Justice Department, Congress, and the press. (83)

The Invisible Spy relates anecdotes about the intelligence officers Cuneo met, some of them, like Ian Fleming, would later become famous. Maier provides detailed, though not always accurate, background on each one. In Fleming's case, he is given credit for "Operation Mincemeat," the British deception using a "corpse … to fool the Nazis" prior to the invasion of Sicily. Fleming had no involvement in "Mincemeat." (142)

For historical context, Maier also comments on intelligence operations occurring before, during, and after WWII, operations that did not involve Cuneo and don't do credit to Maier's grasp of his subject. For example, he labels Soviet agent Kim Phiby and Hitler's spy chief Wilhelm Canaris as double agents. (18) And then he misconstrues the message of a genuine double agent, Dusko Popov, when claiming Popov warned the FBI about the pending attack on Pearly Harbor. (108) A final example, when discussing Soviet defectors, he writes that Elizabeth Bentley turned herself into an "FBI satellite office in New Haven, Connecticut." (328) The event occurred in New York City.

The Invisible Spy summarizes Cuneo's postwar life and at one point quotes him as saying "I actually think I have cracked the code of history." (407) But Maier concludes that "spying remained the most enigmatic part of Cuneo's life, the most difficult to track, document and understand." (409) If fact, though much is revealed about those Cuneo knew, the specifics of his liaisons are not discussed, and no evidence of any spying is presented. And Maier himself seems unsure, when he concludes

that Cuneo knew that "a nebulous status as 'liaison' to a foreign intelligence agency … left him bereft of any recognition." (414)

Ernest Cuneo died in March 1988, leaving the details of his liaison work a mystery. ■

An O.S.S. Secret Agent Behind Enemy Lines: The Second World War Exploits of Lieutenant Leif Bangsbøll
By Brook G. Bangsbøll
(Frontline Books, 2024), 308 pages, no index.

After the death of Leif Bangsbøll, Lt. Col. (USA, Ret), in 2001, his son Brook discovered evidence of his father's military career during and after WWII of which he had been unaware. Before joining the Office of Strategic Services (OSS), Lief had been a pilot, learned several languages, served in the Royal Danish Navy, the Royal Norwegian Air Force, and the US Army. He would end his WWII service in OSS, supporting the Danish Resistance. His postwar career saw service in Korea, the 82nd Airborne Division, and as a Special Forces Green Beret. There was too much material for one book, so Brook decided to tell his father's story in two volumes. The first, *An O.S.S. Secret Agent Behind Enemy Lines*, deals with Leif's WWII service. The second, *U.S. Special Forces Commando*, will be published later.

Brook Bangsbøll acknowledges that his book lacks source notes, but he adds that, with one exception, "all the central events described in the book are in some way corroborated … by extracts from military records or other documented media or reference materials, including medal citations, letters and photographs with handwritten notes on the back." He explains the exception by writing: "I have taken literary license to generate much of the dialogue between the characters, but the entire storyline of events is firmly based on historical facts." (xv)

An O.S.S. Secret Agent Behind Enemy Lines tells how Lief began his military service, the unusual circumstances that led to his OSS recruitment, his training in Canada, and his "night parachute mission behind enemy lines in the European theater of war as an agent in the OSS." (xxiii) His most important operation as an "OSS field agent, codenamed Alexander Hudson," (170) was to support the Danish resistance. One operation involved sabotaging German supply trains and freeing a group of Danish Resistance members. (219)

Although a better chronological fit for the second book, Brad includes a moving chapter on his father, "the Danish descendant of Vikings and the patriarch of the Sørensen-Bangsbøll clan," and his burial service in Arlington National Cemetery. ■

The Umbrella Murder: The Hunt for the Cold War's Most Notorious Killer
By Ulrik Skotte
(WH Allen, 2024), 323 pages, index.

After defecting to the United Kingdom in 1969, Bulgarian writer Georgi Markov worked for the BBC. On September 7, 1978, while waiting for a bus on the Waterloo Bridge, Markov was injected with a pellet containing ricin poison administered by a modified umbrella. According to Danish journalist Ulrik Skotte, the murderer was not identified until 2021. *The Umbrella Murder* tells his story.

After the collapse of communism the Bulgarian intelligence service on orders from the new Bulgarian president, told Scotland Yard it had located several file folders on the agent who appeared to have been given the job of killing Markov. This agent's codename was "Piccadilly," and he was living in Denmark. His name was Francesco Gullino, sometime called "The Italian."

Scotland Yard assigned two detectives to the case. They learned the suspect was living in Copenhagen and made arrangements with the Danish security service to interview him in 1993. After the interview, the detectives concluded they had little evidence of guilt, and Gullino was freed. But Gullino knew he needed help, and while he could have turned to any number of people, he chose film maker, Franco Invernizzi. (57)

A colleague of Danish journalist Ulrik Skotte at the Danish Broadcasting Corporation, told him about Franco's new contact and put them in touch. When Skotte asked Franco why they should meet, Franco said "all you need to know for now is that I have cracked the case." (7)

The Umbrella Murder discusses the history of the Markov assassination, and the slow accumulation of evidence that eventually convinced Skotte that Gullino was guilty. He acknowledges that his evidence is persuasive but not conclusive and that Gullino would never be formally charged. (302) An interesting contribution to a famous still unsolved case. ■

Fiction

Counterfeit Spies: How World War II Intelligence Operations Shape Cold War Spy Fiction

By Oliver Buckton
(Rowman & Littlefield, 2024), 267 pages, index.

In the introduction to his 1998 book, *Counterfeit Spies*, intelligence historian Nigel West writes that the 17 books he discussed in it "are based on nothing more substantive than a fertile imagination." In his study of how "actual World War II espionage and deception operations influenced postwar spy fiction," Florida Atlantic University English Professor Oliver Buckton applies a different and puzzling definition of *Counterfeit Spies*. In Buckton's view, it is the "authors who produced 'the bodyguard of lies' surrounding the truth of wartime espionage, intelligence, and deception [that] may be considered counterfeit spies." (19) Why the authors and not their fictional creations are so designated is discussed but not clarified. (20)

For reasons never explained, Buckton acknowledges at the outset that he begins each chapter with a fictional scene "featuring speculative dialogue that represents an imagined version of how a significant documented episode in the life of the subject of the chapter might have unfolded." (10) These speculations are not delineated as such, thus the reader must decide when the fiction ends and the non-fiction narrative begins; the distinction is not always clear.

Buckton's method is straight forward. Most of his subject authors are well known, for example John Bingham and Ian Fleming. Buckton cites traces in Fleming's novels of his involvement in wartime deception operations, citing Operation Mincemeat as one example, a poor choice since Fleming was not involved.

Buckton's method is straight forward though his contextual comments are frequently wrong. For example the statement that Felix Cowgill was head of Section IX; that was Philby. (78) Most of the authors discussed are well known, for example John Bingham and Ian Fleming. Buckton cites traces in Fleming's novels of his involvement in wartime deception operations, citing Operation Mincemeat as one example, a poor choice since Fleming was not involved.

A better example is the work of novelist Graham Greene, who served in MI6 under Kim Philby during WWII. Buckton discusses a number of Greene's books in which he finds connections to his wartime experiences. In the case of *The Third Man,* he finds echoes of a relationship to "double agent" Philby, though that book is not a spy story. Greene's *Human Factor* is a better example. Buckton also sees elements of the wartime Garbo deception network in "his brilliant satire of British intelligence and debunking of the myth of Bond, *Our Man in Havana*." (14) He argues that "Greene's merciless satire of the incompetence and gullibility of British intelligence surely pulls the rug from under the illusion that the British were the best at the Great Game."

Counterfeit Spies also explores the "writings of a new generation of spy novelists who missed wartime service but served in British intelligence after World War II, whether in SIS or MI5," who benefited from the "enduring influence of World War II counterfeit spies working in deception, propaganda." They include John le Carré, John Bingham (model for George Smiley), and Helen MacInnes. Buckton makes this claim despite asserting that the "focus of this book has been on a specific group of British writers who served as agents and officers in British intelligence during World War II and went on to make use of these wartime experiences in writing postwar spy fiction." (287)

It is very likely that espionage-related books by former intelligence officers turned writers draw on their own experiences. *Counterfeit Spies* offers some speculative examples amidst a profusion of confusion and factual errors. Only the authors know whether Buxton is right. ■

The Snares: A Novel

By Rav Grewal-Kök
(Random House, 2025) 320 pages
Reviewed by John Ehrman.

Neel Chima, a deputy assistant attorney general in the waning days of the second George W. Bush administration, gets a call one day. "Are you happy where you are? Toiling in the trenches of the Justice Department?" asks the caller, who works at the highest-levels of the CIA and is known simply as "the priest" because of his single-minded dedication. "You're a good lawyer but…you're never going to be a great one," the type who makes it to the top at Justice, the priest tells him. Perhaps, instead, Neel would be interested in a job that will enable him to "vault past all the timekeepers at Main Justice"?

The answer, of course, is yes, and soon Neel, anxious to make his career mean something, finds himself the

principal deputy director of the Freedom Center. It's a counterterrorism fusion center of sorts, loosely modeled after National Counterterrorism Center. In the Freedom Center analysts pore over reports from other agencies to search for intelligence nuggets others may have missed. The analysts then add the names to an ever-growing threat matrix, with "every name implicating more names…[as] the lists grew longer, and the matrix deepened." Names of people in the United States go out for investigation and surveillance, while those outside the country are ranked for strikes in the wilds of the Middle East and South Asia. Neel takes to his work diligently, if with some confusion in his new surroundings. "He had to find his way in a world of bureaucrats and operators he only dimly understood. Most of all, he had a career to make."

But Neel has a problem: he doesn't fit in. He's the son of Punjabi immigrants who has married the daughter of a wealthy WASP Republican lawyer; he's no longer part of one community but not accepted by the other. At work, he's a lawyer among intelligence officers and operators, and does not understand their tribal ways. "You want, on an almost primal level, to belong," the priest tells him, but it's not happening. It's no surprise that Neel drinks too much or, late at night, watches porn videos on his computer while his wife and daughters are asleep.

And that's not the least of Neel's problems. Sam Jones, a mysterious CIA officer has been watching Neel for months and occasionally taunting him over the phone. After Neel comes under investigation for a security violation while on TDY in Bangkok, Sam emerges from the shadows with an offer to make the inquiry go away. All Neel has to do is remove from the threat matrix a young American in Chicago who looks to be self-radicalizing so that he'll be forgotten by the bureaucracy and Sam's hit squad can quietly kill him. At the same time, a drone strike in Waziristan goes wrong, and a dogged reporter uncovers Neel's role in identifying the target and planning the attack, spreading his name across the national media. Meanwhile, Neel's marriage collapses under all the pressure.

Grewal-Kök is an editor and writer primarily of short fiction; *The Snares* is his debut novel. Rather than a conventional tale of espionage, he gives us a story about the intersection of the politics and bureaucracy of intelligence and how it chews up one man. This is Graham Greene territory—one thinks of *The Human Factor*—and Grewal-Kök creates a layered and subtle narrative that looks at questions of identity, choice, and morality. He writes with a deft touch, telling his story in spare prose that nonetheless gives depth to his characters and situations and draws in the reader. Neel's plight may be extreme, but you'll still sympathize with him because you can see how something like this could happen to you. *The Snares* will keep you turning the pages as quickly as any thriller. ■

The Spy Coast

By Tess Gerritsen
(Thomas & Mercer, 2023), 347 pages.
Reviewed by Resolute Lee.

The Spy Coast is internationally bestselling author Tess Gerritsen's first foray into the espionage thriller genre. Gerritsen is a veteran author whose writing credits span drama and thriller genres, including the Rizzoli and Isles crime thriller series. In *The Spy Coast*, her writing is crisp and well-paced, weaving together exposition and prose into a well-crafted and thoroughly engaging narrative that pulled this reader through its pages—in one sitting!

The Spy Coast uses a common plot device of espionage novels in which a protagonist, in this case a retired CIA officer named Maggie Bird, finds a "visitor" from her past, a corpse, laid out in the driveway of her retirement home in a sleepy, fictional seaside village of Purity, Maine. Maggie, who had hoped to leave behind ghosts of a mission gone tragically wrong years earlier, soon recognizes the body as someone involved in that operation.

Until that discovery, Maggie had been living quietly on her chicken farm, socializing with neighbors and a local circle of other CIA retirees who call themselves the "Martini Club." She, of course, calls on club members to help her uncover why the past has returned.

Using flashbacks, Gerritsen adds dimensionality to Maggie as she steadily reveals the complexities of her past decisions and unveils the painful events that have brought Maggie to the present. Gerritsen also achieves authenticity, weaving realistic spy tradecraft into the story and offers glimpses into the challenges of human intelligence operations, which in this story mixes Maggie's operational relationships and personal relationships, including love interest, in an effort to take down a notorious international money launderer. At times the scenario stretches credulity, but in the end it addresses a main theme of the novel, do we really know who people are, even those most close to us?

Of note, Gerritsen acknowledges in an author's note that *The Spy Coast* was inspired by her discovery years ago that a good number of neighbors in her own then sleepy Maine town, Camden, were retired CIA and Foreign Service officers. The notion of unassuming retirees with secret past lives and dusty old skills made for fascinating characters to explore.

In sum, *The Spy Coast* is a well-crafted and engaging story, and, as Gerritsen continues her new series, I look forward to reading further into the past secrets—and the mysteries solved—of Maggie and her Martini Club friends. ■