STUDIES

IN INTELLIGENCE | Vol. 70, No. 1 (March 2026)

Espionage in Our Future

Why Human Intelligence Still Matters

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.

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

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 Program, and the CIA Museum.

Contributions

Studies in Intelligence welcomes articles, book reviews, and other communications. Detailed guidance, along with exemplars of articles and reviews can be found on CSI's pages on CIA's public web site (https://cia.gov/resources/csi/).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

STUDIES IN INTELLIGENCE

Contents

Vol. 70, No. 1 (Extracts, March 2026)

(Continued on following page.)

❖ ❖ ❖

Contributors

Article Contributors

Thomas Mulligan is a researcher at the RAND Corporation and former CIA officer.

Reviewers

Graham Alexander is the pen name of a CIA officer.

Sean Barnes **is a retired CIA officer and tradecraft instructor.**

Rovert Coventry III **is a defense technology entrepreneur and a candidate for a commission in the US Navy Reserve (intelligence).**

John Ehrman is a retired CIA officer and frequent contributor.

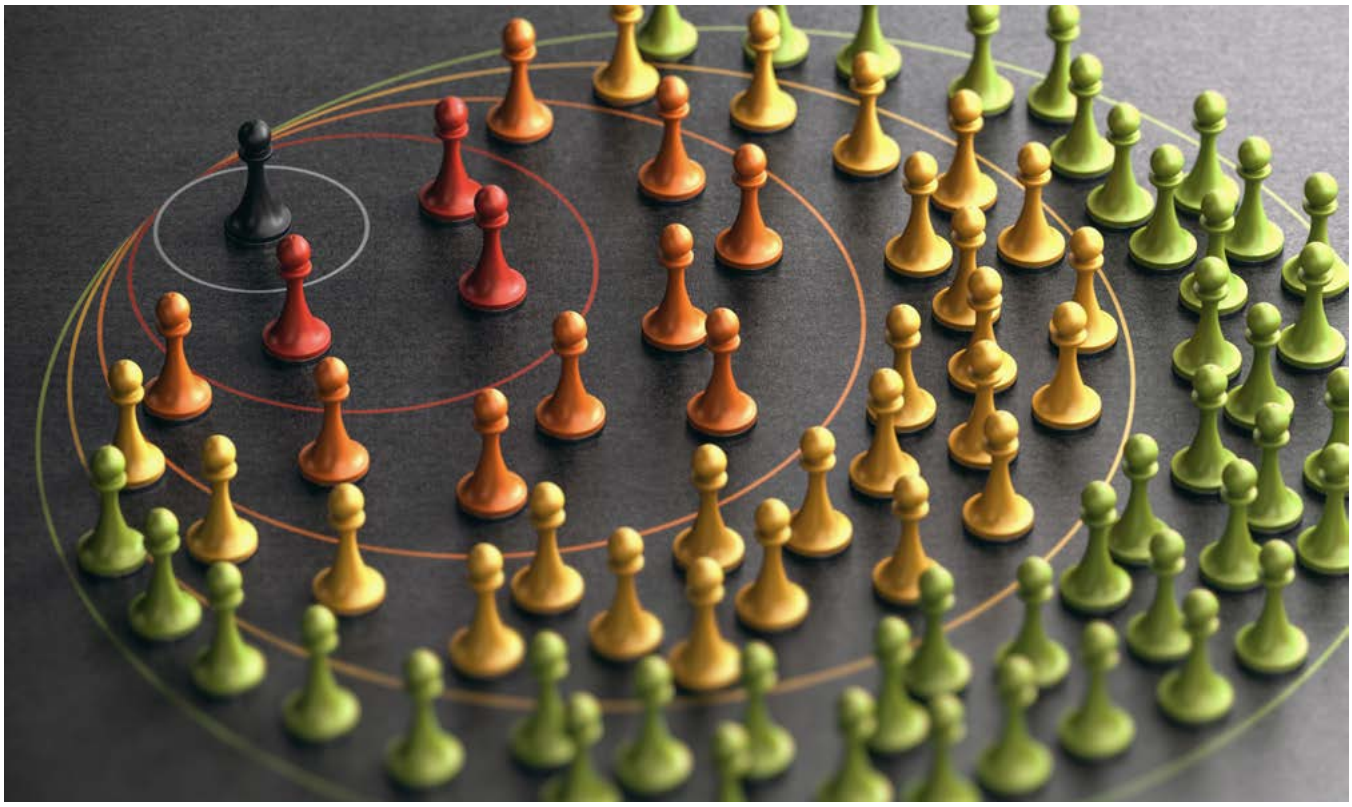
Resolute Lee is the pen name of an ODNI officer.

Ana P. is a CIA analyst.

Hayden Peake served in CIA's Directorates of Operations and Science and Technology. He has compiled and reviewed books in the "Intelligence Officer's Bookshelf" since 2002, in many years providing the majority of reviews published in the journal.

Dr. David Robarge is CIA's chief historian.

JR Seeger is a retired CIA officer and frequent contributor on paramilitary topics. ■



Espionage in Our AI Future

Why Human Intelligence Still Matters

Thomas Mulligan

Thomas Mulligan is a researcher at the RAND Corporation. He served in the CIA from 2008 to 2014, including as a case officer in Latin America.

The prospect that artificial intelligence might transform intelligence work is not new. In 1964, CIA was worrying about Soviet advances into "artificial-intelligence" and their national security implications (CIA 1964).[a] This early AI research was similar in nature (though not, of course, sophistication) to contemporary goals and techniques, including pattern recognition and machine learning. CIA observed, for instance, that the Soviets were using supervised machine learning to rapidly assess the seriousness of burn injuries. As AI technology has matured and diffused throughout our society, consideration of how to improve intelligence with it has quickened. This work has focused on the ramifications of AI for intelligence analysis.[b]

a. Moran et al. 2023, and O'Connor 2023 provide history of the use of AI by the IC.
b. See, e.g., Borene 2023, Galascione 2023, Gartin 2019, Gleeson 2023, and Neuberger 2025.

Much less attention has been paid to the ramifications for human intelligence (HUMINT) operations.[a] But frontier (i.e., state-of-the-art) AI is already changing how HUMINT collectors—case officers (COs)—do their job. And some people believe that emerging technology, including AI, threatens the entire HUMINT enterprise (*cf.* Ignatius 2025).[b]

While AI will transform HUMINT (along with most everything else), this, our oldest form of intelligence collection, will in fact grow in importance. For one thing, as AI makes high-quality technical collection cheaper and more accessible, it thereby boosts HUMINT's value on the margin. AI will supercharge disinformation and fabrication—and that makes HUMINT's ability to build and test source reliability over time, and corroborate technical collection, more important than ever. And as AI undermines the security of electronic communications, tradecraft techniques which COs have used for millennia—such as dead drops and brush passes—will find new relevance as I argue in this article.

In Section 1, I discuss the paper's scope and assumptions, and explain why its conclusions are robust to many future paths of technological development. In Section 2, I analyze five ways which HUMINT collection is, or soon will be, changed by AI. The lessons of this section are that we need to:

- Equip COs with AI-related requirements and encourage them to aggressively pursue relevant targets;
- Be attentive to the possibility of AI being used by fabricators;
- Recognize that while AI is a boon to counterintelligence surveillance and will make the lives of COs in the field more difficult, there are limits to what AI can do;
- Use AI for asset validation;
- Consider how AI can improve COs' ability to persuade agents, developmentals, and others.

Some of the ideas presented in Section 2 are not new. I mean to point out their relevance in the context of HUMINT collection. For instance, researchers and practitioners have looked at using AI to predict crime.[c] Those same tools may be used by counterintelligence services to predict where COs, operating in the field, will conduct operational acts. (Which, espionage being criminal nearly everywhere, amounts to the same thing.) In Section 3, I argue that AI will make technical intelligence collection cheap and accessible and flood the information environment with disinformation and noise. It may also undermine the security of electronic communications. All of these outcomes make HUMINT more important, not less. I conclude in Section 4.

Two preliminary notes. First, my topic is AI and espionage—that is, the collection of secret information by COs from foreign agents (also known as assets or sources). COs may of course engage in other activities, such as covert action. The ramifications of AI for those activities will not be considered here, but they are profound.

Second, this article is normative, not positive. That is, it is about what people involved in the HUMINT enterprise ought to be doing vis-a-vis frontier/future AI. It makes few claims about what is happening in terms of contemporary HUMINT operations and AI.

a. Perhaps this is beginning to change. While this paper was under review, the Special Competitive Studies Project's "The Digital Case Officer" white paper (SCSP 2025) was released, outlining an AI-augmented "human-machine team" approach to HUMINT and discussing related governance considerations.

b. I thank Emma Borden, Matt Chessen, John Parachini, Joel Predd, and Cortney Weinbaum for helpful suggestions on an earlier draft of this paper, and Emily Lawson for her valuable research support. I am also grateful to the CIA's Prepublication Classification Review Board for its timely reviews of this paper.

c. See, e.g., Dakalbab et al. 2022 and Faqir 2023.

1. Speculating about Our AI Future

The future of AI is highly uncertain. People have different views, defended at different levels of rigor, about many things, such as how AI capabilities will grow (exponentially? linearly? to some point and no further?) and the extent of AI diffusion. The world will look very different depending on where we land, and when, on those and other dimensions. One might ask, in which of those future worlds do the arguments of this paper hold?

The conclusions of Section 2 are rooted in technology which is already viable or clearly on the technological frontier. Readers interested in technical detail can consult the references provided. Of course, what is now apparent might be a mirage. Maybe there is some unforeseen barrier to highly persuasive AIs.[a] So, when it comes to AI capabilities that are not already viable, I am assuming that the relevant technological development will continue apace.

When it comes to Section 3 and its conclusion about HUMINT's ongoing relevance, things are more speculative—although not that much more. We do not know if AI will, ultimately, totally undermine electronic encryption. But it is a threat to electronic encryption, because AI is already being used to create deepfakes, which are in turn augmenting phishing cyber attacks, which are a way to evade encryption.

I do assume, for most of Section 3,[b] that cataclysmic outcomes (e.g. human extermination/total subjugation at the hands of AI) do not come to pass, and in our AI future human beings retain some access to information of intelligence value. Otherwise, the paper does not rely on assumptions about how technological or social development will proceed.

A further point in favor of the robustness of Section 3's findings is that the three arguments I give there are largely independent. The truth of one does not require the truth of another. And they are largely divorced of "common causes" (Reichenbach 1956) such that if one is wrong then the others likely are too. For instance, suppose that AI ends up strengthening encryption rather than undermining it. That hardly threatens the ideas that HUMINT can provide a marginal advantage in the face of technological democratization or that it can break through the disinformation problem. The real challenges to what I conclude in this paper must stem from skepticism about the soundness of my arguments, then, rather than from speculation about the path and extent of technological development.

2. Operational Implications of Frontier AI

Artificial intelligence has already affected HUMINT operations, and future advances will change them more. Five considerations are salient.

2.1 AI Requirements

To do their job, COs must understand what information is valuable to policymakers and other intelligence consumers. Common sense goes a long way; all COs know that if they come across information on terrorism or the Chinese military, they should pass it along, and that they should cultivate sources with that access. When it comes to more specialized topics—say, an obscure piece of dual-use technology—there are mechanisms to push collection tasking to COs in the field.

These mechanisms are insufficient for dynamic, cutting-edge

a. If I had to speculate, the argument would go like this: AI-derived language will inevitably have a recognizably non-human quality about it; there will be a backlash against AI due to its bad effects, leading to a stigma against its use; therefore, AI-derived "persuasive" content will make speech less compelling—not more. [One reason I think this argument is unsound is because I think the first premise is false.]

b. Section 3.3 does not require the latter assumption (ii). The focus there is HUMINT tradecraft, independent of its typical use, which is to collect intelligence from human sources. In other words, that argument for HUMINT's enduring relevance is slightly more general than the others given.

technology like AI. Further, they are fundamentally reactive. In response to tasking, a CO can seek out the requested information. But in the absence of it, if he happens to come across this information, he will not recognize its intelligence value and will not report it.

The problem is acute when it comes to AI for two reasons. First, much of the information is technical, and couched in unfamiliar jargon. COs' ears should perk up if they encounter chatter about recurrent neural networks, or extreme ultraviolet lithography, or AI-enabled protein design. But would they?

Second, there's an enormous diversity of AI-related information with intelligence value. This breadth is hard for an untrained person to appreciate. Intelligence consumers are (or should be) interested in topics such as:

- Semi-conductor supply chains
- Military uses of AI
- Use of large language models (LLMs) in biological warfare
- AI industrial policy
- Deepfakes and disinformation
- Loss of control incidents
- Frontier model performance
- Model security
- Export control evasion
- Novel sources of training data
- Integration of AI into critical infrastructure.

It would be useful to have a few COs out there who are AI experts. But it's more important that all COs—no matter where they serve or what functional mission they concentrate on—have an AI training baseline. This could be provided at the Field Tradecraft Course (the core training/certification course for COs), on-demand in the field, or—best of all—both.

Case officers do not need in-depth technical knowledge to be effective AI collectors (cf. Katz 2020: 6). They do need familiarization with AI-related concepts, terminology, and technology, as well as regularly updated requirements from consumers. That's enough to develop and recruit new AI sources and to recognize AI-related intelligence when it arises. When technical expertise is needed, headquarters can provide it.

COs should be aware of the unusual motivations that AI developmentals might have. The classic pillars of money, ideology, compromise, and ego (known in espionage circles by the acronym MICE) remain. But there are important subtleties. Many potential sources are conflicted about their AI work. This is, in part, a result of uncertainty about the future development of AI, the dangers it may pose, and how it may transform fundamental human institutions, like work and relationships.

Some developmentals may find a traditional pitch compelling ("let's make sure the United States and the West—not China—win the AI war"). But for others, these geopolitical considerations are trivial in light of the existential risk AI poses. They will want to hear that only the United States can ensure that future AI is developed with care and effectively aligned with human values.

2.2 AI-enabled Fabricators

Agents may already be using AI to fabricate information. Fabrication is not a new phenomenon, of course, but AI makes it easier to fabricate and that fabrication more difficult to detect.[a] Fabricators can use LLMs to brainstorm and generate false but plausible information to pass to their COs. An agent can put into an LLM names, organizational structures, the substance of peers' work, and his own past reporting, and get out plausible stories to pass off as bona fide intelligence.[b]

a. There are several reasons agents might fabricate, including loss of access, fear of termination, desire for more remuneration, or doubling against the service that recruited them.
b. On the use of LLMs to generate misinformation in healthcare, see Zhou et al. 2023.

Of course, using an LLM like this would be risky, especially for agents living in a surveillance state. But savvy agents could install local AI models, fine-tune them on information like that described above, and generate false intelligence before meeting with their COs. Indeed, by sprinkling some detail about COs' typical lines of questioning and personality, fabricators could produce an even more persuasive product (Section 2.5).

The problem is not limited to existing agents. There are plenty of foreigners who (i) work for organizations of intelligence interest, like government ministries; (ii) have titles that plausibly entail access (e.g., program manager); and (iii) would love a new source of income. An LLM can generate a backstory for an enterprising fabricator and serve as a source of ongoing, unlimited, and false information.

Methods exist to detect fabrication, but AI makes the problem more prevalent and more resistant to those methods. Not many people have the intelligence and storytelling skill necessary to adopt a persona with the goal of serving as an intelligence agent; to maintain that persona by regularly providing false information; and to overcome vetting. With AI, the hurdles to this sort of behavior shrink.

Until now, it's been difficult for fabricators to create convincing photographs, videos, documents, and other media to support their false claims. When it has happened, it's been with the support of an intelligence agency (i.e. when the fabricator's been working as a double agent). But widely available generative AI models put this capability into every fabricator's hands. Methods for detecting deepfakes exist and are improving, but so are the countermeasures.[a]

2.3 Tradecraft Transformed

Artificial intelligence will transform COs' day-to-day work—how they spot, assess, develop, recruit, and handle agents. AI will, that is, transform tradecraft. Indeed, the transformation is already under way.

A principal challenge of HUMINT operations is surveillance. If a CO is discovered conducting an operational act (e.g., meeting an agent or placing a technical device), there are consequences. The CO is confirmed to be conducting intelligence activity and, in the best case, is expelled. The gentlest outcome for the agent is imprisonment. There is geopolitical blowback affecting other operations and equities. So COs are trained on and practice techniques to detect and defeat surveillance.

Effective surveillance against well-trained COs is costly. It can only be regularly mounted by our most capable adversaries. Until now, effective surveillance has meant multiple surveillance teams, each with multiple surveillants; vehicles and other equipment; and much watching and waiting. But technology—AI included—is driving down the cost of surveillance while increasing its scale and effectiveness. Cameras are a clear example. Placed outside of the home and work of known or suspected intelligence officers, and in transportation hubs, they monitor these officers' movements and help model their behavior. And they put anything in their field-of-view off-limits for operational acts (a CO cannot meet an agent if that meeting will be recorded).

COs have contended with technical surveillance for decades. Methods have been developed to defeat it, which in turn have birthed countermeasures, in the typical cat-and-mouse way. But AI threatens to realize the counterintelligence dream of comprehensive, stifling surveillance.[b] This is how David Ignatius (2025) describes the problem facing COs:

> *The tradecraft problem wasn't just pervasive surveillance, but the fact that data existed forever. . . . now, hidden cameras could monitor a case officer's meandering route to a dead-drop site and his location, long before and long after. His asset might collect the drop a week later, but his*

a. See, e.g., Abbas & Taeihagh 2024, Balafrej & Dahmane 2024, Heidari et al. 2024, and Singh et al. 2025.
b. Cf. Katz 2020: 5, Neuberger 2025, SCSP 2025, and Syllaidopoulos et al. 2025.

movements would be recorded, before and after, too. Patterns of travel and behavior could be tracked and analyzed for telltale anomalies. Even when spies weren't caught red-handed, they could be caught.

The problem, though, isn't just the extent or persistence of data. The problem is that AI can quickly and automatically mine that data—nearly all of which is innocuous. Until now, it's been labor-intensive (not to say impossible) for security services to grapple with the deluge of data and identify the few signals of espionage amongst all the noise.

With AI-enabled facial and pattern recognition, security services can, without human intervention, identify potential intelligence activity to subject to scrutiny. Audio intercepted from personal devices and fixed (perhaps covert) microphones can be rapidly processed for counterintelligence use. (Although as AI-powered lipreading technology matures, audio surveillance may be obsolete in some settings.)[a]

Already, cheap, miniature drones can be deployed to surveil each known or suspected CO. These are small enough to avoid detection, and when controlled by AI can operate around-the-clock, in coordinated swarms, ensuring no surveillance gaps. When a CO enters a building, the AI can identify all possible exits and deploy drones to cover them.

New technologies, like nano drones, are in the offing. Drones on the order of ~1 centimeter would not have to wait outside; they would simply, clandestinely, accompany the CO into the building. The actual surveillance technology is only part of the counterintelligence solution. Equally important is the AI which automates and controls the drone.

Artificial intelligence can be used to identify operational acts. As a surveilled CO passes another person, an AI system can evaluate that event as a potential brush pass.[b] The passerby's identity can be ascertained via facial recognition and extra surveillance upon him can immediately commence.[c]

Still, there are limits. Every day, in every city, scores of people casually toss paper cups on the ground. Nearly all of them are litterers. Occasionally, one is a CO conducting a dead drop. It's not clear how any surveillance system—AI-powered or otherwise—could discriminate between the two.[d]

There are two lessons for COs. First, there will be less and less tolerance of sloppy tradecraft. Imprecise movements and timing which today raise no serious counterintelligence concerns (but which, of course, ought to be avoided) could soon be catastrophic. If the dead drop is an SD card glued into a paper cup, then the CO needs to make sure the card is secure, so he can toss the cup like garbage. He can't place the cup carefully on the ground to ensure the card doesn't fall out. That behavior is unnatural—and AI can tell. The margin of error between operational activity and the civilian conduct it's meant to ape is narrowing.

Second, cover will increase in importance. A security service cannot investigate every act of littering to discover those few instances of operational activity. But it can investigate every act of littering by a known or suspected intelligence officer.

This suggests a growing role for non-official cover COs. It also means that protecting the cover of our officers will be more important than ever. Harold Nicholson, a HUMINT tradecraft instructor, infamously sold the names of CIA trainees to the Soviets. A

a. See e.g., Yang et al., 2019, contains 718,000 samples of Mandarin speech that can be used to train AI lipreading models.
b. Cf. Hussain et al., 2024 and Sengönül et al., 2023.
c. Cf. Ionescu et al., 2020.
d. Perhaps the AI could rely on "crowdsourced intelligence" ("CROSINT") to investigate. If there's a bit of on-the-ground investigation needed (a piece of garbage to inspect, a photo to be taken, etc.), that could be advertised to people in the area, who would do the job for a small fee. (On CROSINT, see, e.g., Hershkovitz 2020 and Zhang 2022.)

damaging revelation, to be sure, but manageable. A similar compromise in the AI era could be catastrophic.

Case officers should also consider how AI might improve their tradecraft. AI is already being used for site selection, and if it can help a business find a location for a new store (by analyzing traffic patterns, surrounding infrastructure, online commentary, and more), it can help a CO select an operational site and plan a surveillance detection route (SDR).

The caveat is that the very same tools may be used by security services to anticipate COs' behavior and defeat their SDRs.[a] The solution is not to ignore these tools. Nor is it to trust them entirely. The solution is, rather, to ensure that independent, idiosyncratic, *human* judgment is exercised when selecting sites and planning SDRs. That can break the AI stalemate between spy and counterspy.

2.4 Agent validation

Zachery Tyson Brown conjectures that AI will help "identify micro-expressions that may serve as tells during source interviews or interrogations" (2024: 4). And systems have been built which apparently do exactly that: Yuan et al. (2025) present an AI model able to distinguish between liars and truth-tellers with 98-percent accuracy. (That's in a lab setting; field performance would doubtless be less impressive.) The model relies on basic facial muscle movements ("facial action units"), eye gaze, head pose, and "micro-expressions" (transient, involuntary, and nearly imperceptible facial movements).

The same tools that may watch our COs can help vet our agents. It is expensive and dangerous to conduct human surveillance anywhere, but especially abroad, in a hostile country. AI-enabled drones can watch our agents cheaply and with plausible deniability—ensuring agents work where they claim, meet the people they say they do, and have the lifestyles they purport to.

Stations can already use AI to deal with walk-ins, who pose a dilemma. On the one hand, they must be taken seriously. Many of our (and other countries') most valuable agents began their clandestine relationship by walking-in. On the other hand, most walk-ins are deranged, fabricators, dangles, or otherwise unhelpful. We'd like to expose our COs only to walk-ins of the first type, but there's typically no way of determining which type a walk-in belongs to, and the risk of turning away an important source is too great. So we end up exposing our COs to people who are, one way or another, dangerous.

Stations should consider having initial contact with walk-ins be handled by an AI officer. Even current technology can help identify problematic walk-ins, who can then be safely turned away by non-intelligence personnel. As technology improves, sophisticated but problematic walk-ins—like dangles—may be identified. Such a system could, at the very least, help COs assess the risks and benefits of face-to-face meetings.

2.5 Persuasion

A core CO skill is persuasion. A CO must be able to persuade a target to meet, a developmental to become an agent, and an agent to continue providing secret information. One might think that persuasion is a quintessentially human skill, inapt for artificial replication. In fact, in specific, bounded settings, frontier AI models are already rivaling humans in the ability to persuade.[b] As Matt Chessen describes things, "human cognition is a complex system, and AI tools are very good at decoding complex systems. . . . When provided rich databases of information about us, machines will know our personalities, wants, needs, annoyances, and fears better than we know them ourselves." (2017: 2).

a. An analogous case could be using AI to predict the location of terrorist attacks. See, e.g., Ding et al. 2017 and Olabajo et al. 2021.

b. See, e.g., Huang & Wang 2023, Schoenegger et al. 2025, Spitale et al., 2023, and https://www.anthropic.com/research/measuring-model-persuasiveness (retrieved 19 May 2025). On the use of LLMs for persuasion and disinformation generally, see Jones & Bergen 2024.

One promising way to improve COs' ability to develop, recruit, and handle agents is through AI-enhanced micro-targeting.[a] This is using information about a person's beliefs, personality, and preferences to improve the effectiveness of communications with her.

Of course, all good COs do this already. Part of being a good communicator is understanding one's audience and crafting one's speech accordingly. If COs know that an agent is an unemotional, logical type, they will rely more on rational arguments and less on appeals to emotion. Targeting (in this sense) has to this point been a mix of CO intuition, training, and guidance from headquarters.

Artificial intelligence can help. Imagine an LLM fine-tuned for persuasive power. In preparing for an agent meeting, a CO feeds into it public data like social media, proprietary information (operational cables), and relevant context (geopolitical facts). The model, in turn, provides guidance on how to communicate with the agent: what language to use; topics to avoid; objections the agent is likely to raise and how to respond to them; non-verbal measures like how to dress for the meeting, the location to choose, and amenities; and more.[b]

Such a model could be useful in other interactions, such as meetings with developmentals. COs today should consider using a (properly secured) LLM like they use their colleagues in station: as a sounding board for developing and pitching potential sources.

It's already possible for COs to access real-time, AI-generated communications guidance, via a clandestine earpiece or augmented reality glasses. And it's no longer fantastical to imagine COs equipped with a brain-computer interface serving in this role. It would recommend, like a video game, dialogue options for COs to consider as they pursue their operational goal (e.g., reminders about debriefing topics).

3. Human Intelligence in an Artificial World

HUMINT operations are an old-fashioned mix of art and science. Some tradecraft techniques have been used for millennia. It is tempting to think that, in an AI-saturated world, HUMINT will be a relic.

The opposite is likely true, for three reasons. First, AI will render technical intelligence collection cheap and widely accessible, thereby increasing the value of HUMINT collection, with its relatively high barriers-to-entry. Second, AI will be used to overwhelm digital environments with disinformation. HUMINT will have a unique ability to find the valuable intelligence signal amongst all that noise. Third, AI may undermine the trustworthiness of electronic communications. If that happens, we will need non-electronic ways to communicate which are simple and secure. Traditional agent communication techniques—dead drops, brush passes, brief meetings—are precisely that.

3.1 HUMINT on the Margin

Technology tends to be democratizing. It rapidly diffuses knowledge and capabilities. The printing press is a classic example. More recently, we have seen this with encryption. It was once expensive and difficult to encrypt electronic communications. Only governments and well-resourced companies could manage it. Now, anyone can download practically unbreakable encryption programs like Pretty Good Privacy for free. A ramification is that electronic encryption—while still vitally important—does not provide the relative advantage it once did.

Artificial intelligence will similarly democratize technical intelligence collection, making it easier and cheaper. First-rate efforts will be more common. We have already seen this with geospatial intelligence (GEOINT). This collection discipline (an important part of it,

a. See, e.g., Matz et al. 2024, Salvi et al. 2025, SCSP 2025, and Simchon et al. 2024.
b. Cf. SCSP 2025.

anyways) was once available only to nations capable of spaceflight. But now, high-quality imagery is available for free on the Internet, as is software (some of which uses AI) to process and analyze it. And if some desired imagery isn't available, anybody can task high-resolution (~30 cm) commercial satellites to get it.

The point is not that technical intelligence will be unimportant, but that AI will make it much easier to conduct collection comparable in scale and quality to our own. It will be harder to gain an advantage over our adversaries in these collection disciplines, and so the relative value of HUMINT will go up.

There's an analogy in the betting markets for horse racing. These are parimutuel markets in which there is no "house edge"; bettors compete only against each other. It is therefore possible to be a long-term winner.[a] Traditionally, the best bettors were experienced horseplayers, who could instinctively evaluate races. They could detect, for instance, when a horse was sick or subtly injured. But in the 1980s, racing-related data and statistical methods proliferated. Smart gamblers leveraged those tools to beat their peers, reaping enormous profits.[b]

The old ways are being rediscovered. Data, statistical models, and computing power are accessible, cheap, and part of any serious bettor's repertoire. Their outputs are priced into the markets, and possession of them provides bettors no advantage over their peers. Put differently, the insights generated by these methods are necessary, but not sufficient, for profitability. The marginal advantage—which even if small can be decisive—is increasingly coming from the insight which instinct and other *qualitative* capacities provide.

Brown (2024) says that "no matter how large your model may be, it will never encompass the world . . . there is no amount of data that will permit the forecasting of novel events in an increasingly complex competitive environment wherein innumerable threads, material and immaterial, sympathetic and antagonistic, are all wound together in a Gordian knot of causality." (3). Even if AI can massively improve the amount and quality of intelligence we can collect and produce—as seems likely—there will remain a critical residual which only HUMINT can obtain.[c] This could include information stored in air-gapped systems; foreign leadership intentions; and information on the existence and operation of AI "off-switches," which would be concealed from AIs because their purpose is to mitigate loss-of-control incidents involving those AIs. And when it comes to geopolitical competition—as with horse racing—a small advantage may make the difference between riches and ruin.

3.2 Human Signal, Electronic Noise

Future AI will be a fount for unlimited and effective disinformation.[d] We are, of course, already dealing with this problem, and its scale and severity are increasing. While HUMINT collection is not immune to AI-driven disinformation (Section 2.2), unlike the technical collection disciplines it will not be overwhelmed by it. For instance, there are worries about AI being used in a "fog of war" machine that floods the battlespace with disinformation and makes intelligence, surveillance, and reconnaissance impossible.[e] Such a machine would not imperil HUMINT operations; to the contrary, it would elevate them into the critical role of filtering out

a. Technically, to be profitable, bettors must not only beat their peers, but also overcome the "track take" (a portion of the bets made which is extracted to pay for operating the races).
b. See https://www.bloomberg.com/news/features/2018-05-03/the-gambler-who-cracked-the-horse-racing-code (retrieved 13 May 2025) for a prominent example of this.
c. Cf. SCSP 2025.
d. See, e.g., Lucas et al. 2024.
e. See Geist 2023.

intelligence from the AI-generated chaff.

Or suppose that, within some adversarial nation, every day there are X phone calls of intelligence value. As a counterintelligence measure, our adversary uses AI to generate 10X daily deepfake calls. Indistinguishable from the real thing and containing carefully crafted disinformation, AI could render signals intelligence (SIGINT) efforts useless, even counterproductive. But a human agent can help identify which calls are bona fide and which are not.

The two collection efforts would, then, work in tandem. AI-powered SIGINT could obtain the content of phone calls but not insight into which calls were real and which were fake. A human agent might know that a call had been made but not what was said. HUMINT has long been used to corroborate intelligence gained through technical methods. Given the growing disinformation problem, this role will become more prominent.

The problem might be even simpler. Advanced AI could create a state of cognitive overload, which causes us to throw up our hands in the face of an unending deluge of plausible-looking information.[a] Overwhelmed by electronic intelligence—all kinds of media, containing some indeterminate mix of truth and falsity, derived from both real-world and synthetic data, and so on—HUMINT would, at least, be manageable.

3.3 Secure Human-to-Human Communication

While contemporary technology has affected how COs communicate with their agents, it has supplemented, rather than replaced, traditional techniques. This will continue to be the case.

For one thing, AI is already making it difficult to discriminate between truth and falsity in electronic communications. The quality of deepfakes is such that, to the untrained eye (and increasingly to the trained eye as well), it is impossible to differentiate between genuine images, videos, and audio and their deepfake counterparts.[b]

Scammers are using deepfakes to defraud and extort people—for instance, by generating audio which sounds like a family member pleading for ransom to (non-existent) kidnappers. These scams have succeeded not just against credulous people but sophisticated businesses as well.[c]

At the same time, hallucinations—the presentation of specious information by AI systems—persist. The rational response to these and similar dynamics is to treat digitally-mediated messages as lower-trust by default. If my friend tells me, face-to-face, that he is in trouble and needs money, I can be confident that that's true. But if that message is mediated by an electronic system—an e-mail, a phone call, a video attachment—it's more likely a scam than a bona fide plea for help.

A central, critical part of HUMINT tradecraft involves human-to-human communication unmediated by electronics. A properly-executed dead drop both (i) securely transfers information from the agent to the CO and (ii) gives the CO confidence that the information received is, indeed, being provided by his agent. Of course, the information could be false because the agent is lying or simply mistaken. But that is a categorically different concern than the one deepfakes and other AI dynamics raise: the injection of a new and powerful source of noise into the signal sent from agent to CO.

The idea of micro-targeting is related. Consider the following simple model of communication: Diane has some belief B in a proposition p (which could be, e.g., the proposition that the attack will be launched

a. See, e.g., Lahlou 2025.
b. See, e.g., Diel et al. 2024.
c. See, e.g., https://www.wired.com/story/youre-not-ready-for-ai-powered-scams/ (retrieved July 24, 2025) and https://www.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk (retrieved July 24, 2025).

tomorrow).[a] Diane might think the proposition is true, or false, or 30-percent likely, or whatever. She receives some speech, S, from an interlocutor which is relevant to the truth of p. Diane's task, now, is to reach a maximally justified belief about p given B and S.

Her interlocutor's speech S can be decomposed into a part that is correlated with the truth of p and a part that is pure persuasion. Diane only receives S, though, which is the sum of the two parts.

As S is dominated by its purely persuasive part—exactly what micro-targeting is designed to achieve—Diane ought, rationally, to reduce the extent to which she modifies B in light of S. Intuitively, Diane cannot be sure whether she finds S compelling because it reflects underlying truth or because her interlocutor is silver-tongued. So, as micro-targeting becomes more common and more effective, it may be rational to reduce trust in any communications that are not in-person.[b]

Traditional HUMINT techniques may also matter for a second reason: the possibility of "loss of control" incidents involving future AI. Imagine AI systems which rival or surpass human abilities, but which are misaligned with the values or goals we sought to instill in them. These systems could pose a threat—even an existential one—to human beings. Contemplation of these scenarios is no longer fringe speculation; it's a topic of increasing interest among serious researchers and policy analysts.[c]

In the event of a loss-of-control incident, it would be challenging for humanity to coordinate a response. Our standard (electronic) methods of communication—phones, emails, and so on—would be compromised by AI. HUMINT tradecraft would remain viable.

Finally, it's possible that AI will undermine encryption, thereby reducing—perhaps drastically—the security of electronic communication.[d] AI could identify implementation flaws in encryption protocols. It could increase the effectiveness of current techniques, like phishing (e.g., by using deep fakes). It could even—perhaps in tandem with advances in quantum computing—undermine encryption at a theoretical level.

If any of that happens, then the relative value of HUMINT tradecraft goes up. For it secures information in a categorically different way, resistant to those technological developments.

4. Conclusion

At the outset, I argued that we need not fret about the lower bound on the technology necessary for this paper's conclusions; the technology is here already or will be soon. But what about an upper bound? Might AI become so powerful and widespread that my earlier judgment—that HUMINT will continue to be relevant—will not hold? So long as the two explicit assumptions of Section 1 are satisfied, even in futurist worlds of human marginalization—in which AIs, rather than humans, increasingly have access to intelligence—the conclusion of Section 3 retains force.

Observe, for instance, that the argument for HUMINT's marginal value is compatible with the overall supply of HUMINT going down (as humans are replaced by AIs) and AI-derived intelligence being better than HUMINT. Indeed, that's the point: Value is determined not by total supply and demand, but by supply and demand at the margin. That marginal unit of HUMINT collected by our future CO, working in the lonely

a. Formal treatments in the epistemology of disagreement can be adapted to model this kind of source-weighting problem. See, e.g., Mulligan 2021.
b. Futurists have sometimes described this state as one of "epistemic collapse" or "knowledge collapse." See, e.g., Peterson 2025.
c. For an evocative and technically informed description of how they might come to pass, see https://ai-2027.com/ (retrieved 23 May 2025). See also Somani et al. 2025.
d. On this possibility, see, e.g., Bao et al. 2022, Benamira et al. 2021, and Gohr 2019.

shadows of an artificial world, may make all the difference.

HUMINT's role in cutting through synthetic noise holds as long as humans retain access to relevant information. The fewer humans with this access, then (all else equal) the lower value of the overall HUMINT effort. But this is not an objection to the argument, per se; it is an observation about its restricted applicability in a class of AI futures.

The considerations related to HUMINT communication techniques have greater force if more futurist scenarios, involving AI dominance over human beings, come to pass. Regular people don't use HUMINT tradecraft to communicate, even for sensitive information. There are better options. In the event of a loss-of-control incident, there might not be.

It is challenging to opine about our AI future. But across plausible futures, three points seem robust: AI is an extraordinary technology, perhaps without historical precedent. Much will change as it is integrated into HUMINT operations. But much will remain the same, and it's unlikely that AI will render HUMINT redundant. The work of the CO will remain recognizable in our AI future. ■

Works Cited

Abbas, Fakhar & Araz Taeihagh, "Unmasking Deepfakes: A Systematic Review of Deepfake Detection and Generation Techniques Using Artificial Intelligence," Expert Systems with Applications 252, part B (2024): 1-38, https://doi.org/10.1016/j.eswa.2024.124260.

Balafrej, Ismael & Mohamed Dahmane, "Enhancing Practicality and Efficiency of Deepfake Detection", *Scientific Reports* 14 (2024): 1-11, https://doi.org/10.1038/s41598-024-82223-y.

Bao, Zhenzhen, Jian Gou, Meicheng Liu, Li Ma, & Yi Tu, "Enhancing Differential-neural Cryptanalysis", in *Advances in Cryptology*—ASIACRYPT 2022, eds. Shweta Agrawal & Dongdai Lin (Springer, 2022), 318–47.

Benamira, Adrien, David Gerault, Thomas Peyrin, & Quan Quan Tan, "A Deeper Look at Machine Learning - based Cryptanalysis," in *Advances in Cryptology—EUROCRYPT 2021*, eds. Anne Canteaut & François-Xavier Sandaert (Springer, 2021), 805-835.

Borene, Alice B., "'This Piece Was Written by a Machine': Intelligence Analysis, Synthesis, and Automation," *Studies in Intelligence* 67, no. 4 (2023): 21–24.

Brown, Zachery Tyson, "'The Incalculable Element': The Promise and Peril of Artificial Intelligence", *Studies in Intelligence* 68, no. 1 (2024): 1–7.

Chessen, Matt, "The MADCOM Future: How Artificial Intelligence will Enhance Computational Propaganda, Reprogram Human Culture, and Threaten Democracy . . . and What Can Be Done about It." The Atlantic Council, 26 September 2017. https://www.atlanticcouncil.org/in-depth-research-reports/report/the-madcom-future/.

CIA, "Artificial-intelligence Research in the USSR", Office of Scientific Intelligence report 64-37 (1964). https://www.cia.gov/readingroom/docs/artificial%20intelligence%20r[15424923].pdf.

Dakalbab, Fatima, Manar Abu Talib, Omnia Abu Waraga, Ali Bou Nassif, Sohail Abbas, & Qassim Nasir, "Artificial Intelligence & Crime Prediction: A Systematic Literature Review", *Social Sciences & Humanities Open* 6, no. 1 (2022): 1–23, https://doi.org/10.1016/j.ssaho.2022.100342.

Diel, Alexander, Tania Lalgi, Isabel Carolin Schröter, Karl F. MacDorman, Martin Teufel, & Alexander Bäuerle, "Human Performance in Detecting Deepfakes: A Systematic Review and Meta-analysis of 56 Papers," *Computer in Human Behavior Reports* 16 (2024): 1–13, https://doi.org/10.1016/j.chbr.2024.100538.

Ding, Fangyu, Quansheng Ge, Dong Jiang, Jingying Fu, & Mengmeng Hao, "Understanding the Dynamics of Terrorism Events with Multiple-discipline Datasets and Machine Learning Approach," PLOS ONE 12 (2017): 1–11, https://doi.org/10.1371/journal.pone.0179057.

Faqir, Raed S. A., "Digital Criminal Investigations in the Era of Artificial Intelligence: A Comprehensive Overview", *International Journal of Cyber Criminology* 17, no. 2 (2023): 77-94.

Galascione, John F., "The End of Human Intelligence Analysis—Better Start Preparing," *Studies in Intelligence* 67, no. 4 (2023): 17–20.

Gartin, Joseph W., "The Future of Analysis," *Studies in Intelligence* 63, no. 2 (2019): 1–5.

Geist, Edward. *Deterrence under Uncertainty: Artificial Intelligence and Nuclear Warfare*. Oxford University Press, 2023.

Gleeson, Dennis J., "Artificial Intelligence for Analysis: The Road Ahead", *Studies in Intelligence* 67, no. 4 (2023): 11–15.

Gohr, Aron, "Improving Attacks on Round-reduced Speck32/64 Using Deep Learning,"in Advances in Cryptology—CRYPTO 2019, eds. Alexandra Boldyreva & Daniele Micciancio (Springer, 2019), 150–79.

Heidari, Arash, Nima Jafari Navimipour, Hasan Dag, & Mehmet Unal, "Deepfake Detection Using Deep Learning Methods: A Systematic and Comprehensive Review", WIREs Data Mining and Knowledge Discovery 14, no. 2 (2024): 1–45, https://doi.org/10.1002/widm.1520.

Hershkovitz, Shay, "Crowdsourced Intelligence (Crosint): Using Crowds for National Security", *International Journal of Intelligence, Security, and Public Affairs* 22, no. 1 (2020): 42–55, https://doi.org/10.1080/23800992.2020.1744824.

Huang, Guanxiong & Sai Wang, "Is Artificial Intelligence More Persuasive than Humans? A Meta-analysis", Journal of Communication 73, no. 6 (2023): 552-62, https://doi.org/10.1093/joc/jqad024.

Hussain, Altaf, Samee Ullah Khan, Noman Khan, Mohammad Shabaz, & Sung Wook Baik, "AI-driven Behavior Biometrics Framework for Robust Human Activity Recognition in Surveillance Systems," *Engineering Applications of Artificial Intelligence* 127, part A (2024): 1–15, https://doi.org/10.1016/j.engappai.2023.107218.

Ignatius, David, "A Band of Innovators Reimagines the Spy Game for a World with No Cover," *Washington Post*, July 10, 2025. https://www.washingtonpost.com/opinions/interactive/2025/cia-ai-technology-spies/.

Ionescu, Bogdan, Marian Ghenescu, Florin Rastoceanu, Razvan Roman, & Marian Buric, "Artificial Intelligence Fights Crime and Terrorism at a New Level", *IEEE MultiMedia* 27, no. 2 (2020): 55–61, https://doi.org/10.1109/MMUL.2020.2994403.

Jones, Cameron R. & Benjamin K. Bergen, "Lies, Damned Lies, and Distributional Language Statistics: Persuasion and Deception with Large Language Models", *arXiv*, 2024, 37, https://doi.org/10.48550/arXiv.2412.17128.

Katz, Brian, "The Collection Edge: Harnessing Emerging Technologies for Intelligence Collection," *CSIS Brief* (2020). https://www.csis.org/analysis/collection-edge-harnessing-emerging-technologies-intelligence-collection.

Lahlou, Salem, "Mitigating Societal Cognitive Overload in the Age of AI: Challenges and Directions," *arXiv*, 2025, 13, https://doi.org/10.48550/arXiv.2504.19990.

Lucas, Jason S., Barani Maung Maung, Maryam Tabar, Keegan McBride, & Dongwon Lee, "The Longtail Impact of Generative AI on Disinformation: Harmonizing Dichotomous Perspectives," *IEEE Intelligent Systems* 39, no. 5 (2024): 12–19, https://doi.org/10.1109/MIS.2024.3439109.

Matz, S. C., J. D. Teeny, S. S. Vaid, H. Peters, G. M. Harari, & M. Cerf, "The Potential of Generative AI for Personalized Persuasion at Scale," *Scientific Reports* 14: 1–16 (2024), https://doi.org/10.1038/s41598-024-53755-0.

Moran, Christopher R., Joe Burton, & George Christou, "The US Intelligence Community, Global Security, and AI: From Secret Intelligence to Smart Spying," *Journal of Global Security Studies* 8, no. 2 (2023): 1–18, https://doi.org/10.1093/jogss/ogad005.

Mulligan, Thomas, "The Epistemology of Disagreement: Why Not Bayesianism?" *Episteme* 18, no. 4 (2021): 587–602, https://doi.org/10.1017/epi.2019.28.

Neuberger, Anne, "Spy vs. AI: How Artificial Intelligence will Remake Espionage," *Foreign Affairs*, January 15, 2025. https://www.foreignaffairs.com/united-states/spy-vs-ai.

O'Connor, Jack, "Undercover Algorithm: A Secret Chapter in the Early History of Artificial Intelligence and Satellite Imagery," *International Journal of Intelligence and Counterintelligence* 36, no. 4 (2023): 1337-51, https://doi.org/10.1080/08850607.2022.2073542.

Olabajo, Olusola A., Benjamin S. Aribisala, Manuel Mazzara, & Ashiribo S. Wusu, "An Ensemble Machine Learning Model for the Prediction of Danger Zones: Towards a Global Counter-terrorism," *Soft Computing Letters* 3 (2021): 1–6, https://doi.org/10.1016/j.socl.2021.100020.

Peterson, Andrew J., "AI and the Problem of Knowledge Collapse," *AI & Society* 40, no. 5: 3249–69 (2025), https://doi.org/10.1007/s00146-024-02173-x.

Reichenbach, Hans. *The Direction of Time*. University of California Press, 1956.

Salvi, Francesco, Manoel Horta Ribeiro, Riccardo Gallotti, & Robert West, "On the Conversational Persuasiveness of GPT-4", Nature Human Behavior (2025): 1–12, https://doi.org/10.1038/s41562-025-02194-6.

Schoenegger, et al., "Large Language Models Are More Persuasive than Incentivized Human Persuaders", *arXiv*, 2025, 30, https://doi.org/10.48550/arXiv.2505.09662.

SCSP (Special Competitive Studies Project), "The Digital Case Officer: Reimagining Espionage with Artificial Intelligence" (2025). https://www.scsp.ai/wp-content/uploads/2025/09/SCSP_The-Digital-Case-Officer_-Reimagining-Espionage-with-Artificial-Intelligence.pdf.

Sengönül, Erkan, Refik Samet, Qasem Abu Al-Haija, Ali Alqahtani, Badraddin Alturki, & Abdulaziz A. Alsulami, "An Analysis of Artificial Intelligence Techniques in Surveillance Video Anomaly Detection: A Comprehensive Survey," *Applied Sciences* 13, no. 8 (2023): 1–31, https://doi.org/10.3390/app13084956.

Simchon, Almog, Matthew Edwards, & Stephan Lewandowsky, "The Persuasive Effects of Political Microtargeting in the Age of Generative Artificial Intelligence," *PNAS Nexus* 3, no. 2 (2024): 1-5, https://doi.org/10.1093/pnasnexus/pgae035.

Singh, Laishram H., Panem Charanarur, & Naveen Kumar Chaudhary, "Advances in Detecting Deepfakes: AI Algorithm and Future Prospects—a Review," *Discover Internet of Things* 5, no. 53 (2025): 1-30, https://doi.org/10.1007/s43926-025-00154-0.

Somani, Elika, Anjay Friedman, Henry Wu, Marianne Lu, Chris Byrd, Henri van Soest, & Sana Zakaria, "Strengthening Emergency Preparedness and Response for AI Loss of Control Incidents," *RAND Europe Research Report* (2025). https://www.rand.org/content/dam/rand/pubs/research_reports/RRA3800/RRA3847-1/RAND_RRA3847-1.pdf.

Spitale, Giovanni, Nikola Biller-Andorno, & Federico Germani, "AI Model GPT-3 (Dis)informs Us Better than Humans," *Science Advances* 9, no. 26 (2023): 1–9, https://doi.org/10.1126/sciadv.adh1850.

Syllaidopoulos, Ioannis, Klimis S. Ntalianis, & Ioannis Salmon, "A Comprehensive Survey on AI in Counter-terrorism and Cybersecurity: Challenges and Ethical Dimensions," *IEEE Access* 13 (2025): 91740–64, https://doi.org/10.1109/ACCESS.2025.3572348.

Yang, Shuang, Yuanhang Zhang, Dalu Feng, Mingmin Yang, Chenhao Wang, Jingyun Xiao, Keyu Long, Shiguang Shan, & Xilin Chen, "LRW-1000: A Naturally distributed Large-scale Benchmark for Lip Reading in the Wild", *arXiv*, 2019, 8, https://doi.org/10.48550/arXiv.1810.06990.

Yuan, Shusen, Zilong Shao, Zhongjun Ma, Ting Cao, Hongbo Xing, Yong Liu, & Yewen Cao, "Deception Detection Based on Microexpression and Feature Selection Methods," *EURASIP Journal on Image and Video Processing* 8 (2025): 1–18, https://doi.org/10.1186/s13640-025-00674-3.

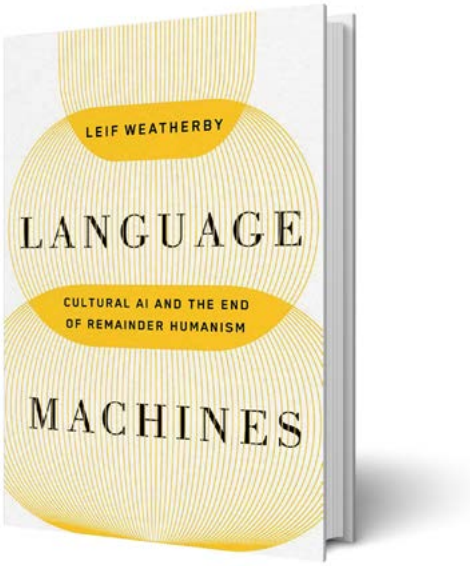
Zhang, Jing, "Knowledge Learning with Crowdsourcing: A Brief Review and Systematic Perspective," IEEE/CAA Journal of Automatica Sinica 9, no. 5 (2022): 749–62, https://doi.org/10.1109/JAS.2022.105434.

Zhou, Jiawei, Yixuan Zhang, Qianni Luo, Andrea G. Parker, & Munmun De Choudhury, "Synthetic Lies: Understanding AI-generated Misinformation and Evaluating Algorithmic and Human Solutions", in *CHI '23: Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, eds. Albrecht Schmidt, Kaisa Väänänen, Tesh Goyal, Per Ola Kristensson, Anicia Peters, Stefanie Mueller, Julie R. Williamson, & Max L. Wilson (Association for Computing Machinery, 2023), 1–20.■

review essay

Language Machines
Cultural AI and the End of Remainder Humanism

Reviewed by Sean Barnes



Author: Leif Weatherby
Published By: University of Minnesota Press, 2025
Print Pages: 279
Reviewer: Sean Barnes is a retired CIA officer and tradecraft instructor.

Sherman Kent, under whose mighty shadow analysts labor, decreed that intelligence analysis exists to serve policymakers, not to pursue knowledge for its own sake. As CIA tradecraft expert Jack Davis reminded us, Kent was pretty blunt about this—intelligence that gets ignored is "useless."[1] Kent made it look easy, his method, drawn from a background in historical scholarship, deceptively simple: test your sources, then check your own biases before drawing conclusions.[2] As any analyst will tell you, the former is simple enough in theory; the latter is brutally difficult in practice.

This grounding matters when we turn to Leif Weatherby's *Language Machines*: *Cultural AI and the End of Remainder Humanism*, a likewise deceptively simple book that examines generative artificial intelligence (GenAI) through cultural theory rather than intelligence tradecraft. Weatherby uses structuralism and semiotics to make a striking claim—that large language models (LLMs) function as ideology machines, creating meaning through pattern recognition while embedding cultural assumptions at scale. For veterans of the intelligence trade, this isn't just academic theorizing. It means, in a nutshell, that the bias problems Richards Heuer warned about have mutated into something a thousand times harder to spot and a million times easier to spread.[3]

So let's test Weatherby's arguments against Kent School principles. The question isn't whether his cultural theory holds water academically—it's whether his insights can help us understand why GenAI might belong on our desks as something to analyze, not something to trust with analysis itself.

The Language Wars Nobody Wins

Weatherby opens by sketching the battlefield where linguists and engineers have been fighting for decades. In one corner, Noam Chomsky and his followers insist language springs from hardwired cognitive structures—universal grammar built into our brains. To them, LLMs are just stochastic parrots, mimicking without understanding. In the other corner, the statistical crowd argues that patterns alone can generate language. Point to any word, they say, and you can predict it from the words around it.

Both camps miss something crucial here. The syntax theorists dismiss LLMs too quickly; the statisticians overvalue them. Neither grasps what structuralists figured out long ago—language works through relationships between elements, not through pure thought or raw probability. Weatherby shows us that LLMs generate meaning precisely through these structural relationships, which explains both their surprising capabilities and their fundamental limitations.

Any analyst reading this should hear Heuer's voice warning about anchoring bias. Chomsky's people anchor on cognition, the engineers anchor on statistics. Each clings to their model like it's gospel, dismissing evidence that complicates their worldview.[4] What Weatherby offers—without saying it directly—is something like Heuer's structured technique known as analysis of competing hypotheses. Don't pick a side; run multiple explanations in parallel and see which one explains the evidence best.

Here is where things get a bit unsettling. Roland Barthes confidently declared the "death of the author" back in the 1960s, and literary critics subsequently had an intellectual field day over the next several decades, arguing whether texts could mean anything without knowing who wrote them and why. LLMs make this fun, abstract debate suddenly concrete. These machines produce text without consciousness, intention, or purpose. In the vaunted context of everything we've been taught about intelligence analysis, the meaning emerges from patterns in data, not from any mind trying to communicate.

Think about what this means for intelligence work. We're trained ad nauseam to first ask who wrote something and why. Heuer documented our obsession with intent—we see purposeful actors everywhere, even in random events. But when an LLM generates a report, there's no "who" behind it in any meaningful sense. No motive to uncover, no institutional bias to account for (at least not in the traditional way). The bias is there, but it's systemic, embedded in training data and emerging from statistical relationships we can't fully trace.

Left unaddressed, this is chilling. Should the natural momentum generated by "this latest breakthrough" be allowed to roll on down the proverbial hill, it completely scrambles our source evaluation methods. We built those methods around human psychology and institutional analysis. What good are they when the "source" is a mathematical function operating on terabytes of text? The game has changed, and we're still using the old rulebook.

Attention Without Intention

In his third chapter, Weatherby sheds some light on this potential disaster by digging into the technical heart of these systems—the attention mechanism that makes transformer models tick. Don't let the jargon intimidate you; the concept is straightforward. Attention lets the model decide which parts of the input matter most for predicting what comes next. It's like having a spotlight that can illuminate different parts of a sentence depending on what the model needs to generate.

For analysts, this should sound pretty familiar. We do this constantly and eventually unconsciously—deciding which signals matter in an ocean of noise, which sources deserve scrutiny, which patterns might be significant. Heuer showed how badly we do this, overweighting dramatic information while missing crucial baseline data.[5] The attention mechanism formalizes this process mathematically, encoding selective focus into the model's architecture.

But there's a catch. We can metricize to our heart's content. We can see the attention weights, watch which tokens get prioritized, but we can't fully explain why. The model makes these choices through layers of mathematical transformation that resist human interpretation. Kent demanded clear audit trails for every analytical judgment, and this is at the core of everything intelligence analysts are taught from day one. These systems offer the opposite—sophisticated pattern matching with no ability to explain their reasoning. That's not analysis; it's expensive guesswork.

Weatherby's most cutting observation might be his characterization of what LLMs actually produce. It's not poetry or insight—it's kitsch. Think hotel lobby art or elevator music: familiar forms endlessly recycled, technically competent but utterly without soul or genuine creativity. The models reproduce patterns they've seen thousands of times, creating outputs that feel meaningful but lack any real depth.

The errors these systems make—what we call hallucinations—are not random glitches. They're windows into how the model associates concepts based on cultural patterns in its training data. When ChatGPT confidently states something false, it's showing us how ideas cluster together in the data it consumed. As Weatherby reminds us, these aren't logical errors; they're cultural artifacts.

Heuer would recognize this right off the bat. Like any machine, human analysts, even the best of us, hallucinate too—we see patterns that aren't there, connect dots that shouldn't be connected. But at least our errors follow predictable patterns we can study and counter. LLMs scale this tendency massively, churning out ideological dross that, for all the world looks authoritative but reflects nothing more than statistical regularities in human writing.

Yet there's an opportunity hidden in this problem. These errors and biases aren't just failures—they're potential diagnostic tools. By studying what the model gets wrong and how it gets it wrong, we can map cultural assumptions and ideological structures embedded in the training data. For information operations analysis, for example, this is a good thing. The kitsch might be worthless as intelligence, but it can be invaluable for understanding how narratives construct themselves.

Form Over Facts

Weatherby calls for developing "a general poetics of AI"—basically, learning to read these outputs for their structure and rhetoric rather than their factual content. Language creates meaning through form before it establishes any reference to reality. LLMs prove this point definitively. They can generate perfectly structured arguments about completely fictional topics, showing that formal coherence matters more than truth in language generation.

This insight cuts deep. Like Marine Corps recruits at Parris Island, intelligence analysts are trauma-conditioned into a reflexive focus on facts, to verify claims and establish ground truth. But in modern analysis, the form often matters more than the content. A well-structured lie spreads faster than a poorly presented truth. Weatherby's pushing us to develop what amounts to rhetorical literacy—reading for persuasive technique as much as factual accuracy.

Still, the black-box problem haunts us, as well it should. We can analyze the rhetoric, map the persuasive strategies, understand the cultural resonances, but we cannot trace the generative process. We are left interpreting outputs without understanding origins. In intelligence terms, that's like analyzing a document without being able to verify its provenance. Possibly useful in a few, carefully managed instances, downright deadly in most others.

The Ideology Engine

By the book's end, Weatherby's verdict is clear: LLMs are ideology machines, not thinking machines. They don't produce neutral language; they package and deliver clusters of cultural meaning drawn from their training data. Every output reinforces certain narratives while suppressing others. The hallucinations just make

this process visible, showing us which ideas travel together in the model's learned associations.

Heuer warned about cognitive lock-in—how mental models resist change once they form. LLMs supercharge this problem. They take the biases in their training data and reproduce them endlessly, making alternatives harder to imagine with each iteration. For adversaries running information operations, this is a gift: a propaganda engine that packages ideology with perfect grammar and distributes it efficiently. For analysts, it's a nightmare scenario.

The challenge is not just recognizing bias—analysts are pretty good at that. It is unpacking the ideological clusters, finding the assumptions buried in seemingly neutral language, surfacing the alternatives that the model's outputs systematically hide. Kent would call this a form of deception, though not necessarily intentional. The deception is built into the architecture, emerging from statistical mimicry rather than conscious design.

Why Transparency Isn't Optional

Everything circles back to the transparency problem. Kent insisted that every estimate's reasoning be clear and auditable. Heuer demanded we surface and examine our cognitive biases. LLMs fail both tests spectacularly. They produce outputs through processes we can't fully trace, embedding biases we can't completely identify.

This isn't a technical problem we'll solve with better engineering. It's a fundamental epistemological challenge. Intelligence analysis rests on the ability to show our work, to let others check our reasoning, to build confidence through transparency. LLMs offer the opposite—polished outputs with opaque origins.

For practical purposes, this means LLMs can't be trusted with finished intelligence products. They might help with brainstorming or red-teaming, generating alternative perspectives or challenging assumptions. But relying on them for analytical conclusions would be professional malpractice. It would violate everything the IC tradecraft stands for and potentially put lives at risk.

Making It Practical...Really

Despite the dense theory, Weatherby's analysis offers immediate practical value. He's shifted the conversation from abstract questions about machine consciousness to concrete issues about how machines create meaning. That's exactly the right focus for intelligence practitioners. His framework gives us beleaguered practitioners viable tools we can use today. In this context, hallucinations instead become diagnostic instruments for detecting cultural bias. Kitsch production reveals ideological assumptions, etc. The attention mechanism, despite its opacity, shows us something about how the model prioritizes information. These aren't complete solutions, but they're actionable insights.

The book has obvious weaknesses. Weatherby writes like an academic for academics, which can be frustrating when you need operational guidance. He paints with a broad brush—not everything LLMs produce is ideological kitsch, and occasionally they generate honest insights. But these limitations don't negate the core value: he's already mapped the terrain that we will need to navigate, even if he hasn't provided turn-by-turn directions.

Several concrete steps follow from this analysis. First, any workflow involving LLM-generated content needs explicit bias checks. Do not assume neutrality; assume ideological packaging and look for it systematically. Document these checks. Make them mandatory.

Second, use hallucinations strategically. They're terrible for fact-finding but excellent for red-teaming. When an LLM confabulates, it's showing you narrative patterns and cultural assumptions. Mine those errors for intelligence about how ideas connect in the information environment.

Third, expect adversaries to weaponize these capabilities. They will use LLMs to generate and spread ideological content at unprecedented scale. Build capabilities to track machine-generated narrative patterns. Update these capabilities regularly as techniques evolve.

Fourth, add rhetorical literacy to analytical training. Analysts need to read form as carefully as content. This isn't optional anymore—it's as essential as source validation or link analysis. Make it part of the core curriculum, not an elective.

Finally, establish clear policies about LLM use. These tools can support hypothesis generation and assumption challenging, but never final estimates or policy recommendations. When analysts use them, require documentation. Make the limitations explicit. Verify that machine-generated material isn't contaminating critical judgments.

Heuer taught us that "seeing is not believing"—that our perceptions are filtered through cognitive biases we rarely recognize. Sherman Kent demanded analytical transparency and rigor. Weatherby, writing from the humanities, extends their warnings into the age of AI. His core message is stark: these are language machines, not thinking machines. They package ideology into fluent prose that deceives through its very polish.

Two conclusions are inescapable. First, treat AI outputs as cultural signals requiring interpretation, never as analytical judgments deserving trust. Second, until these systems can show their work—really show it, with full transparency—they remain objects of analysis, not tools for conducting it. The machines speak with increasing fluency, but fluency isn't intelligence. They produce sophisticated patterns, but patterns aren't understanding. They generate compelling narratives, but narratives aren't truth. Until we can see inside the black box, until we can audit the reasoning, until we can trace the logic, we'd be fools to mistake their outputs for analysis.

Weatherby's book matters because, thankfully, it reminds us that the old lessons still apply. Transparency, rigorous tradecraft, and systematic bias awareness—these aren't outdated concepts from a pre-digital age. They're the foundations that keep intelligence work honest and reliable. No algorithm changes that. No technology replaces it. The fundamentals endure because they must endure. Without them, we're not analysts anymore—we're just consumers of sophisticated kitsch, mistaking eloquence for truth.■

Endnotes

1 Jack Davis, "Sherman Kent and the Profession of Intelligence Analysis," Sherman Kent Center for Intelligence Analysis, Occasional Papers 1, no. 5 (November 2002).

2 Sherman Kent, *Strategic Intelligence for American World Policy* (Princeton University Press, 1949), 15.

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

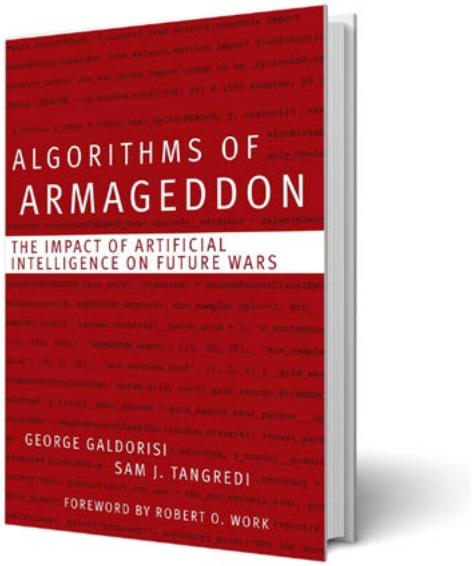
4 Ibid., 45–52.

5 Ibid., 14–21.■

intelligence in public media

Algorithms of Armageddon
The Impact of Artificial Intelligence on Future Wars

Reviewed by Ana P.



Authors: *George Galdorisi and Sam J. Tangredi*
Published By: Naval Institute Press, 2024
Print Pages: 225 pages, index
Reviewer: Ana P. is a CIA analyst.

AI in and of itself is nothing. Militarized AI is a tool for humans to control other humans.

As we ponder the many ways in which artificial intelligence (AI) will disrupt our world, there is perhaps no subject more important for the intelligence practitioner than that of war. In their short book *Algorithms of Armageddon*, military experts George Galdorisi and Sam Tangredi deftly weave together history and technological advancements to write an absorbing work accessible to military and technological novices who bring to it an open mind and willingness to reflect on the fundamental changes our world is facing.

Galdorisi and Tangredi provide one of the most succinct backgrounds of the development of AI, unraveling the story of our exploration of knowledge and logic and providing an absorbing history of AI. Leveraging their storytelling abilities, the authors draw the reader into the cumbersome subject in an engaging, thought-provoking manner, carefully introducing the basics of AI before exploring AI's many uses in war, and outlining the technology's stark risks.

The authors examine not only AI's use in conflict but its potential employment for other nefarious purposes. In later chapters, Galdorisi and Tangredi scope out hypothetical scenarios in which AI could play a role in future combat and the subsequent results, ably taking complex ideas and making them relatable. Instead of providing answers to the many debates the book evokes, the authors ask readers to travel with them and ask profound questions of the world we live in and what is to come.

Oscillating between discussing AI challenges and US approaches to the issue, Galdorisi and Tangredi explore the ways in which our key adversaries are utilizing the technology, many in ways that fundamentally differ from our approaches to these tools. Perhaps the most cogent, clear, and targeted chapter is the second to last which urgently calls for a national conversation on the use of AI in military settings, while warning that the United States will lose the military AI race without a direct, significant effort.

The one downside to the text is that the authors perhaps attempt to cover too much ground in this short work. For this reader, their desire to review so many topics and information made some chapters feel chaotic and disjointed, at times giving short shrift to subjects that could have benefited from greater discussion. For example, Galdorisi and Tangredi discuss in great detail the limitations the United States faces in the application of AI but leave the reader wanting more regarding how our allies are approaching this technology and how the US military and private industry can work together to better harness these technological advancements, among other topics.

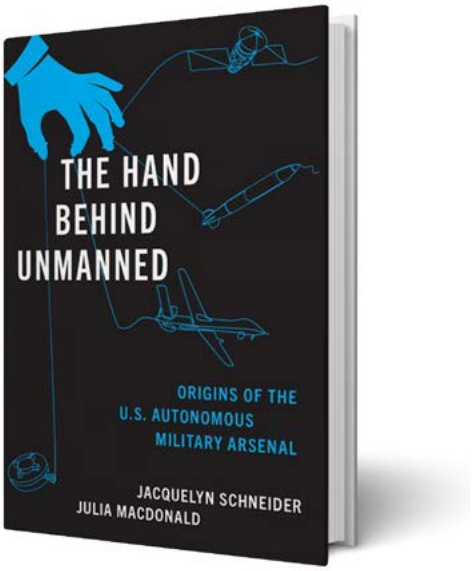
As intelligence professionals, it is incumbent upon us to ensure we are prepared for what is to come and well versed in the benefits and risks of AI, harnessing this knowledge to enhance our work. Starting off with the building blocks of AI and military basics before delving into the hard truths and questions related to the technology's use in war, Galdorisi and Tangredi provide readers with a broad and accessible overview of these topics. For those seeking an entry to these issues, or for seasoned professionals looking for another thought-provoking book, this work will leave both groups with a solid basis of AI and war and eager for a sequel.

The reviewer: Ana P. is a CIA analyst. ■

intelligence in public media

The Hand Behind Unmanned
Origins of the US Autonomous Military Arsenal

Reviewed by Robert Coventry III



Author:	*Jacquelyn Schneider and Julia Macdonald*
Published By:	Oxford University Press, 2025
Print Pages	280
Reviewer:	The reviewer is a defense-technology entrepreneur and a candidate for a commission in the US Navy Reserve (Intelligence).

"Why was the US unmanned arsenal, dominated by remotely controlled unmanned aerial platforms, so ill-prepared to support a war in Ukraine that featured an army of small drones, loitering munitions, and ground launched missiles?" (8)

The Hand Behind Unmanned: Origins of the US Autonomous Military Arsenal, coauthored by Jacquelyn Schneider and Julia Macdonald, is the latest entry in the Oxford University Press's *Bridging the Gap* series. Jacquelyn Schneider is the Hargrove Hoover Fellow at Stanford's Hoover Institution and the director of the Hoover Wargaming and Crisis Simulation Initiative; she had previously served as an assistant professor at the US Naval War College. Julia Macdonald is an assistant professor at the Josef Korbel School of International Studies at the University of Denver with publications in *War on the Rocks*, *Lawfare*, *Foreign Affairs*, and *Bulletin of the Atomic Scientists*. Their book aims to explain the historical development of US unmanned systems and, more ambitiously, the beliefs and service identities that have shaped what the Department of Defense actually buys and fields.

Operationally, the narrative culminates with General Atomics' MQ-1 Predator and MQ-9 Reaper—arguably the most consequential unmanned aerial vehicle programs fielded to date.

The book is organized into six chapters. The first two trace a lineage from mines and torpedoes to ballistic and cruise missiles, showing how rhetoric, shocks, and interagency/international competition (e.g., the Sputnik launch or the debate over which branch should host nuclear ICBM programs) moved budgets and doctrine. Critically, these early chapters compress distinct defense systems into a single narrative arc; segmenting them by technology (e.g., a chapter on mines, another on missiles) would have offered greater clarity.

Chapters 3–4 advance two belief systems that, the authors argue, shape procurement: military-revolutions determinism (technology advances in punctuated leaps; first movers win) and casualty aversion/force protection (public intolerance for losses incentivizes the removal of US personnel from battlefields). The authors write,

"History is full of examples of superpowers failing to take advantage of important Revolutions in Military Affairs…" (144), and also treat "unmanned weapons [as] an inevitable next step of technological development." (113) Likewise, they argue that "the U.S. public is casualty intolerant … and by removing U.S. personnel from the battlefield, unmanned technologies provide a technological solution to decision-maker constraints" (17)

Both the Soviet-era faith in revolutionary technology and the post-Vietnam impulse toward risk avoidance are persuasive explanations as to why and how these belief systems affected unmanned weapons systems to the present. The interweaving narratives presented in these later chapters are much more insightful compared to the near-encyclopedic tone of the first chapters of the book.

In a sharp turn, Chapter 5 pivots from beliefs to institutional identity, arguing services move through a process rather than a binary, from belief to investment to adoption (97–98). The authors show how the histories and traditions of the Army, Air Force, Navy, and Marine Corps—operating inside the Defense Department's "arcane and labyrinthine" acquisition system—determine which unmanned capabilities thrive and how. (334) Chapter 6 brings the framework forward to contemporary debates.

Although the authors acknowledge that "the bread and butter of unmanned [missions]" includes intelligence (41), the book gives almost no treatment to the CIA or the broader Intelligence Community—even though the CIA pioneered the first operationally successful extended range unmanned reconnaissance vehicles, including the Predator, in US history.[a] If these "service identities" are "far more powerful than any capacity-based reasoning" (302), restricting the frame to Title 10 services leaves the thesis untested against its most promising case. This omission is particularly striking given the book's broader goal: to understand which organizational cultures are most likely to adapt, or fail, in the face of new warfare paradigms.

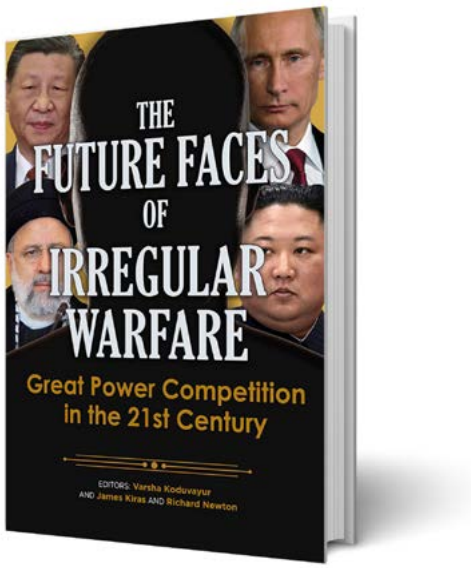
Schneider and Macdonald present an exceptional argument delineating how "the US arsenal of drones is poorly suited" for the type of warfare present in Ukraine: attritional fights that reward cheap, expendable mass. (329) Their warning that, "if left to the status quo, the nation [may not] be able to compete or win against an adversary on the level of China" is noteworthy. (341) Their diagnosis is compelling; the prescription is left unwritten. The remedy, implicit but unstated, lies in mass, modularity, and speed—fields now defined more by commercial innovation than traditional service identity. The contours of a revitalization path are visible: scale swarm production, simplify control systems, unify networking, and draw tactical insight from Ukraine. Yet the book leaves unstated who should lead and why.

It may be that the book's remit—to narrate the US unmanned history, advance a new explanatory framework, map service identities, and assess readiness for great-power conflict—exceeds what a single focused volume can sustain. *The Hand Behind Unmanned* presents a compelling read for policy and acquisition audiences, explaining how and why the United States built the unmanned force it did, furthering an exceptional argument on why that force now struggles against cheap drone mass in Ukraine. For intelligence professionals, omitting the CIA/IC's formative Balkans War and post-9/11 roles in developing and employing unmanned systems—especially the aforementioned Predator and its successors—leaves the book's thesis untested against its most promising case. As Schneider and Macdonald themselves conclude, "the roads not taken are as important as those traveled." (314) Here, that untraveled road is central to the map.■

a. See Frank Strickland, "An Insider's Perspective on Innovation During Fiscal Austerity: The Early Evolution of the Predator Drone," in *Studies in Intelligence* 57, no. 1 (unclassified Extracts, March 2013).

intelligence in public media

The Future Faces of Irregular Warfare
Great Power Competition in the 21st Century



Reviewed by JR Seeger

Edited By:	*Varsha Koduvayar, James Kiras, and Richard Newton*
Published By:	Irregular Warfare Center Press, 2025
Print Pages:	381 pages; endnotes
Reviewer:	The reviewer is a retired CIA officer.

The Irregular Warfare Center (IWC) is the Department of Defense–funded "battle lab" for irregular warfare (IW) created in 2021. It is focused on supporting warfighters facing challenges in any aspect of modern conflict other than conventional warfare. IWC conducts training, produces publications, and holds conferences. In the case of this book, IWC assembled a set of papers focusing on geostrategic issues related to irregular warfare. It is worth noting here that there is no consensus in the US government on the definition of irregular warfare, nor is there a consensus on what agency in the US government should lead in addressing this challenge.

Even a brief review of this topic demonstrates that the US military and the Department of Defense remain challenged in describing the nature of modern warfare where US conventional force-on-force operations are rare and our strategic adversaries (often described in the same documents as "strategic competitors") have an entirely different view of warfare. In the 1990s, IW was described in DOD doctrine as "military operations other than war."[a]

In the first decade of this century, US doctrine changed the name to irregular warfare. This reflected the transition from post-Cold War "peacekeeping" and "peace-making" efforts in the 1990s, to post-9/11 counterterrorism, unconventional warfare, and counterinsurgency operations. However, the DOD definition for IW remained a challenge, with the central doctrinal publication arguing that IW was characterized as *a violent struggle among state*

a. Department of Defense, Office of the Joint Chiefs of Staff, *Joint Publication 3-07: Joint Doctrine for Military Operations Other Than War* (June 16, 1995)

and non-state actors for legitimacy and influence over the relevant population(s). In IW, a less powerful adversary seeks to disrupt or negate the military capabilities and advantages of a more powerful military force, which usually serves that nation's established government.[a]

In 2020 the unclassified summary of the IW annex to DOD doctrine on warfighting, IW is characterized as

> *a struggle among state and non-state actors to influence populations and affect legitimacy. IW favors indirect and asymmetric approaches, though it may employ the full range of military and other capabilities, in order to erode an adversary's power, influence, and will. It includes the specific missions of unconventional warfare (UW), stabilization, foreign internal defense (FID), counterterrorism (CT), and counterinsurgency (COIN). Related activities such as military information support operations, cyberspace operations, countering threat networks, counter-threat finance, civil-military operations, and security cooperation also shape the information environment and other population-focused arenas of competition and conflict.*[b]

In the most current definition issued in September 2025, IW is defined as

> *a form of warfare where states and non-state actors' campaign to assure or coerce states or other groups through indirect, non-attributable, or asymmetric activities.*[c]

It is in this confusing intellectual and political environment that IWC works to bring some degree of clarity.

Both the title of this book and the jacket, with the faces of the leaders of Russia, China, Iran, and North Korea, are misleading. This is not a book that provides a coherent discussion of how these US adversaries use IW in their conflict with the United States. Nor is it a clear discussion of how the United States should address these challenges. Rather, this book is best viewed as a textbook on multiple opinions on IW rather than a thoughtful discussion on the single topic offered in the title.

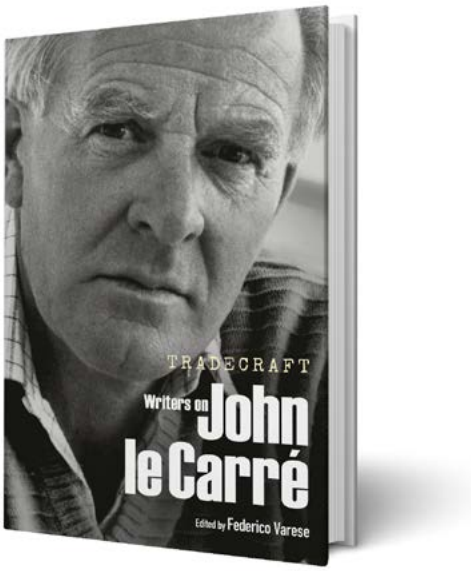
IWC published this book specifically for military practitioners and the book relies heavily on doctrinal jargon and references from DOD publications. In the 15 chapters, the discussions range from definitional discussions on what precisely is irregular warfare, through doctrinal discussions of how the US military should adapt to the challenges of IW, to discussions on how adversaries are using IW to advance their strategic goals against US and allied defenses. Each chapter begins with an abstract and ends with a summary and recommended further reading.

Even with its limitations as a coherent work on IW, every intelligence professional will be well served by reading the book. The US defense establishment is struggling to understand and respond to a complex and ever changing political and military environment. Our warfighter colleagues will demand help from the Intelligence Community on this set of problems. The IC will only be able to assist if intelligence professionals are clear on both the threats from our adversaries and how warfighters understand those threats. ■

a. Department of Defense, Office of the Joint Chiefs of Staff, *Joint Publication 1: Joint Warfighting* (July 12, 2017).
b. "Summary of the Irregular Warfare Annex to the National Defense Strategy." Department of Defense publication (www.media.defense.gov)
c. DOD instruction 3000.07 Irregular Warfare (www.media.defense.gov)

intelligence in public media

Tradecraft
Writers on John le Carré



Reviewed by Dr. David Robarge

Author:	*Frederico Varese*
Published By:	Bodleian Library Publishing, 2025
Print Pages	172 pages, index
Reviewer:	The reviewer is CIA's chief historian.

This eclectic collection of essays offers personal perspectives from authors of varied backgrounds on their experiences working with John le Carré (true name David Cornwell) in very different situations. A companion volume to the exhibit of le Carré's papers at the Bodleian Library at Oxford University (he attended Lincoln College there), *Tradecraft* comprises several categories. Some describe his research trips, the locales where some of his novels are set, and the gradual geographic expansion of their scope. Others discuss his collaboration with an academic; the process of developing screen adaptations of his memoir and one of his novels; perceptions of his novels by the Soviets and Russians; and the polemical features of some of his later works. Lastly, one of le Carré's sons explains why he decided to take up his father's legacy and craft his own le Carré-esque novel.

Overall, *Tradecraft* accomplishes its purpose of giving insights into the methods le Carré used to craft his works and how a novelist can employ history and social geography as a grounding for the development of fictional plots and characters. As with many anthologies, the quality of the essays varies, but nearly all of them provide new views on previously unexamined aspects of le Carré's personal and writing lives.

The volume's editor, Federico Varese, is an Italian academic based in France and England, who has written books on the Russian Mafia. As a doctoral student at Oxford in the 1990s, he assisted le Carré with the novel *Our Game*, about irredentist intrigues in the Russian-controlled Caucasus region just after the end of the Cold War. He became involved more deeply with le Carré's own examination of the Russian Mafia, *Our Kind of Traitor*. One of le Carré's sons, Simon Cornwell, describes Varese as "the perfect collaborator, someone who not only knew the world of which he spoke in unrivaled depth but could also anticipate the avenues that would be of most interest to an author of fiction, offering up connections and anecdotes that from a narrow academic perspective were surely irrelevant but that to a novelist were gold." (viii)

Varese introduces the collection by focusing on three themes that most of the other essays at least touch on:

"the way David went about collecting information, how the evidence collected is used for the purpose of creating an artistic truth, and how he depicts human motivations in subtle ways that echo the most advanced thinking in the social sciences." (3) Along with interspersing memories of le Carré and his wife, Jane, Varese notes the importance le Carré placed on traveling to the geographic settings of his novels—notably after getting caught using an out-of-date guidebook to craft a scene in one of them—and his skill at interviewing local residents to add color and texture to his stories. Recounting his own conversations with le Carré, Varese delves into the methodological differences between a scholar's pursuit of accuracy and a writer's search for realism; one seeks factuality and objectivity, the other immerses himself in made-up people living through credible but unreal events. "When he went into the field, David was many people; he was constantly accompanied by the fictional characters taking shape in his head"—yet "Everything that came from David's pen should be interpreted as an artistic truth, no more and no less." (16–17)

Varese ends his introduction with a touching remembrance of le Carré's memorial service in October 2021:

> *Halfway through the event, extracts of the yet-to-be-released film* The Pigeon Tunnel [a documentary about le Carré based on his memoir of the same title that would be released in 2023] *were shown to the audience, sitting in religious silence. We heard David talking about his craft with unusual candour. At one point he whispered, with typical circumspection and modesty, what seemed to be a confession: "I dare hardly use the claim, but I'll make it here. I am an artist."* (25)

In the first essay after the introduction, "David Cornwell and the Hopeless Uncertainties of History," Errol Morris, the director of *The Pigeon Tunnel* and many other documentaries, picks up on one of Varese's points when he discusses perceptions of truth and the respective roles of the documentarian and the author of historical fiction.[a] Morris first asserts that "David's view of truth is very close to mine. Of course, there's such a thing as truth. In any historical event, we're trying to find out what the underlying reality might be." But then he goes on to state the historian's perpetual quandary:

> *That there is a truth of the matter underlying history doesn't mean that we can ever find it out. There's so much arrayed against the discovery of an underlying reality. People lie. People are self-deceived. People are confused. People forget. Documents are lost. The context that gives meaning to the documents is lost. And so on.* (37)

Or, as Varese concisely puts it in his introduction to Morris's chapter, "history does not come to us already narrated but is told differently by different people." (30) Morris closes with this apt observation about le Carré's tradecraft:

> *In many ways, David was a documentarian. To write his books, he submerged himself in history and culture. He went to the places he was writing about. He became friendly with people he was depicting either directly or indirectly. There is an observational element in virtually everything he did. His work—the fictional universe he built—is the product of pure mind in combination with extensive investigation and empirical observation. It's something that we don't necessarily associate with novel writing but it's a very important thread in his work.*(38)

That "observational element" in le Carré's novels is the subject of two essays with slightly different focuses. Author Lawrence Osborne looks at how well le Carré captured the geography and atmosphere of Phnom Penh and Hong Kong in his eighth book, *The Honourable Schoolboy*, set largely in Southeast Asia. It was the first novel le Carré based on research on site: "I adopted the guise of a field reporter to garner my experiences and information." In Osborne's judgment—he wrote novels based in both cities—le Carré's depictions are "exact and true." (58) Osborne notes that le Carré adopts different tones in describing the two cities: "the writing [about Phnom Penh] somehow does not seem as deeply felt as le Carré's

a. See this author's review of *The Pigeon Tunnel* in *Studies in Intelligence* 61, no. 1 (March 2017).

depictions of British Hong Kong. It is rapid-fire, hectic … all a bit rushed somehow and taken in as from a distance…. It's as if the city le Carré really longed for and found and loves was Hong Kong." (61)

Why? "Hong Kong is where le Carré's eye really did do the talking. It was also where his social background enabled him to make subtle sense of the colony's power structure. At its core, *The Honourable Schoolboy* is a novel about—and a love letter to—Hong Kong." (67) One can see le Carré embodied in the protagonist, Jerry Westerby, a journalist who occasionally runs operational errands for the Circus, as he "wanders by himself through the city, discovering it as if for the first time." (71) During his travels around the region, le Carré met two real-life personalities who became models for figures in the novel: British journalist Peter Simms ("Westerby's incessant cries of 'sport' and 'supah!' certainly derive from Simms") and Richard Hughes ("perhaps the ultimate in the genre of the spy-correspondent … slightly Falstaffian … a raconteur's raconteur") on whom the memorable William "Old" Craw probably is based. (69)

Journalist Michela Wrong, author of an excellent book on Congo, *In the Footsteps of Mr. Kurtz: Living on the Brink of Disaster*, accompanied le Carré on a trip to Rwanda and Congo (Kinsasha) while he was researching *The Mission Song*. He had asked her to look over a draft of the novel, she provided extensive suggestions, and he then offered to pay her to join him on the excursion. Ground truth in the story would be important because, Wrong writes,

> *For the kind of person who wanted to be intelligently entertained rather than worthily educated, who scanned bookshop tables rather than scouring the shelves behind—in other words, much of the Western public—the only book they would ever read about contemporary Congo was likely to be* The Mission Song…. *And, as time had passed, the impetus to pass from the imagined to the concrete by visiting the DRC had become overwhelming.* (104–105)

During the trip, Wrong worried about le Carré being kidnapped, him making major changes to a book already being typeset, and her having to serve as his photographer because he hated traveling with professional ones. She watched le Carré's tradecraft in action through his interviewing technique, his rambles around the cities they visited, and his empathizing with his surroundings and their residents. "For a reporter, a good day on a research trip means four or five interviews and a notebook full of quotes. With David I had to relearn my modus operandi…. Mostly David wanted to wander, in what seemed an almost aimless fashion. The fewer meetings … the happier he seemed." (114) The most moving scene in Wrong's essay involves le Carré's visit to a school where the exhumed and preserved bodies of hundreds of genocide victims were displayed as vivid testimony to the horrors that had been committed during the tribal civil war in 1994. "That day in Murambi, surrounded by contorted, spindly white statues, the English gent looked shattered. You could see the shock on his face. 'I just kept thinking "Maybe there was something I could have done,"' he said; 'Where was I, what was I doing when this happened?'" (113)

Echoing a theme that recurs several times in the anthology, Wrong's encounter with le Carré gave her "a glimpse of the creative chasm that lies between the recorder of fact that I still was at the time—fixated with dates, names, places—and the spinner of fantasy who knows that a sudden spark of emotional insight is worth a hundred interviews. I won't forget that fountain pen and that diminutive notebook, which at the end of a day of meetings, drives and interviews only ever contained a few comments and the occasional quote." (118)

After reading *The Mission Song*, Wrong found it somewhat off-key and not one of le Carré's best books because he did not fully escape his Cold War mindset.

> *David had spent so much time living and working in Communist Europe that the mannerisms, moods and foibles of its intelligence services and the citizens they monitored came to him almost effortlessly. He'd not had time to develop those instincts in Africa and as a result his writing about the continent always seems to me too careful, too polite.* (118)

In contrast to that critical appraisal, literary scholars Elleke Boehmer and Steven Matthews find commonalities between le Carré's pre- and post-Cold War works that place them in the category of "world literature"—"writing that circulates across national borders both through translation and through the exchange of influence and techniques" and "whose themes resonate beyond their contexts of origin." (44) "His fiction was fundamentally *world-making* … in that he gave memorable expression to the experiences of betrayal that defined people's lives in the second half of the twentieth century," whether he was writing about espionage, terrorism, illicit finance, crime, business corruption, or the demise of empire. As his geographic sweep expands, le Carré remains "watchful of how singular motifs and images capture larger swirling global concerns, and how relationships of both empathy and enmity between individual characters can mirror national and international disruptions." (45)

As a complement to that examination of le Carré's "world making," exiled Russian investigative journalist Andrew Soldatov looks at how le Carré's Cold War oeuvre was received by the West's main intelligence adversary of the time, the KGB, and then by its successors after the Soviet Union collapsed. Le Carré, he writes, "has an impressive list of fans in the top echelons of the KGB," which initially seems odd because only two of le Carré's novels—*A Murder of Quality* and *A Small Town in Germany*—were published in the Soviet Union before 1991, and the former is more a detective story than an espionage tale. What the KGB used le Carré for was "to promote its own narrative about Soviet and Russian intelligence agencies." (87) During the Cold War, they were depicted internally as morally superior to their Western counterparts. As censorship loosened under *glasnost* and more spy novels became accessible, Soviet intelligence leaders needed to devise a new image to protect themselves and their services from the fate that befell East Germany's Stasi. The new narrative used selective and decontextualized quotes and paraphrases from le Carré's books to demonstrate that Soviet intelligence was "professional, intelligent and rational." (102) Its operatives were open-minded because they had spent most of their time in the West, and therefore could not have taken part in persecutions of dissenters in the Soviet Union and Soviet intelligence had abandoned the practice of assassinations abroad decades before. "The striking conclusion was that Soviet intelligence officers were in the same business as their Western counterparts, that Soviet intelligence operatives and Western spies were essentially colleagues since they use a similar set of tools and methods."[a] (97) This use of le Carré's name to justify actions by the Soviet and Russian governments continued well into the 20th century.

Many of le Carré's books have been adapted to film and television, and Oscar-winning scriptwriter and director Hossein Amini details his involvement with the author in moving *Our Kind of Traitor* from page to screen. They worked diligently for three straight days at le Carré's home near Land's End in Cornwall. Le Carré was profoundly aware of the differences between prose and screenplay from prior experience:

> *David had gone over my script, was graciously complimentary, then told me that I'd been too faithful to the book. He was a film lover and had witnessed so many adaptations of his novels that he knew slavish fidelity would lead to cinematic disaster. He took off his author's hat and became a filmmaker. We decided that the structure of the novel, with its multiple timelines, would be too confusing in a two-hour film, so we agreed on a linear structure and a single timeline. Similarly, multiple points of view often work better in a novel than in film. In a book, you can return to a previous chapter or reread a passage to reorient yourself, but in a film there's no time to stop. If an audience loses focus for a minute, you've lost them for good.* (127)

They worked through the structure, voices, and details in an "exhausting and exacting but invaluable"

a. This positive claim of moral and operational equivalence ironically echoes the cynical observation that Control, le Carré's fictional head of the Circus, makes in *The Spy Who Came In from the Cold*: "We do disagreeable things so that ordinary people here and elsewhere can sleep safely in their beds at night…. Of course, we occasionally do very wicked things…. I would say that since the war, our methods—ours and those of the opposition—have become much the same. I mean you can't be less ruthless than the opposition simply because your government's *policy* is benevolent, can you now?...That would *never* do." (Coward-McCann, 1963, 23–24.)

manner and produced, in Amini's estimation, the best draft in the whole process of adaptation. (129) Successive versions followed, and then it came time to choose a director. The profound changes in the script that the first director made to location and characters were unacceptable to le Carré, so a second director entered the scene. To Amini and le Carré, the result was even worse. At the first screening, Amini recalls:

> *Nothing was shot as I had imagined it in my head.… I was reeling at first, then I lost concentration.… When the screening was over I felt utterly despondent. I've directed myself and know how lonely it can be, so I put on my bravest face for Susanna* [White]. *Directors are never more paranoid than after a first screening, so she saw straight through my attempt to hide my despair. David didn't even bother to hide his. We both sat staring into space, looking devastated, as Susanna bravely asked us what we thought of the cut.* (133)

The sum of Amini's recollection is that creating film adaptations entails a complex mix of art within art within art: a novel transformed into a screenplay and then a movie:

> *There is no right or wrong way to adapt a book, but the same book can be turned into a dozen completely different screenplays, and those scripts can be turned into a dozen different films. The process of adaptation of a film involves far more people than just the screenwriter. The director, actors, producers, cinematographer, designers, composer, editor and others interpret the source material in their own way and put their individual stamp on the finished film.* (134)

Andrea Ruggeri's chapter titled "The World Has Gone Mad: International Relations in the Work of John le Carré" looks at him less as a writer and more as a committed intellectual. The title is a play on a piece he wrote in the *Sunday Times* in January 2003, "The United States of America Has Gone Mad," in which he denounces the Bush administration's Global War on Terror and the militarization of US foreign policy, notably toward Iraq. During those years, le Carré became a caustic public critic of US and UK handling of international relations, attending protests and writing denunciations in the press. He did not confine himself to recent events in his reproaches. In an article in *The Nation* in April 2001, le Carré asserted:

> *The Cold War provided the perfect excuse for Western governments to plunder and exploit the Third World in the name of freedom; to rig its elections, bribe its politicians, appoint its tyrants, and, by every sophisticated means of persuasion and interference, stunt the emergence of young democracies in the name of democracy.*[a]

Le Carré made a similar, equally bitter observation in his novel *Our Game*, written several years earlier:

> *All through the Cold War it was our Western boast that we defended the underdog against the bully. The boast was a bloody lie. Again and again during the Cold War and after it, the West made common cause with the bully in favour of what we call stability, to the despair of the very people we claimed to be protecting.* (80)

Ruggeri's essay is the least useful contribution to the anthology, however. Its shortcoming is that he uses le Carré's polemical writings as a platform for expressing his agreement with them and making political arguments to substantiate them. He regularly veers from discussing le Carré's work into contemplations about the woeful state of international affairs and the hypocrisy of powerful nations, sometimes expressed in political science jargon. Ruggeri would have better served the purposes of the collection by more deeply analyzing le Carré's political beliefs as an influence on his literary output.

Tradecraft ends fittingly with a sometimes poignant reflection by one of le Carré's four sons, Nicholas Cornwell, who explains why he, a popular writer in a very different genre under the pen name Nick Harkaway, decided to partially follow in his father's footsteps and craft an espionage novel featuring le Carré's best-known character, George Smiley. The preposition in the essay's title—"Writing with My Father"—is significant because, as Cornwell notes,

a. John le Carré, "In Place of Nations," *The Nation*, April 9, 2001.

"We are not—were not—the same. We could not have the same voice, did not have the same experiences, the same competences, the same horrors. Why should I sit in his chair and wear his shoes?" Yet he did just that, first by putting the final touches on le Carré's last, posthumously published novel, *Silverview* ("an act of filial piety for me and a comparatively easy task") (143–44), and then, responding to the encouragement of his brother Simon, writing what became *Karla's Choice*, a chronological gap-filler between *The Spy Who Came In from the Cold* and *Tinker Tailor Soldier Spy*.[a]

Cornwell addresses a challenge that can confront other writers who assume the authorial responsibilities of a literary estate: what style to adopt, their own or their predecessors? In this instance, le Carré complicated matters by shifting his style in the earlier novels from that of the Civil Service he worked for—"stark, simple and declarative, with bursts of emotion derived from event rather than self-examination"—to one with "flourish and ornamentation … Byzantine and immersive." Cornwell says the answer seemed obvious: "The stark noir style … is not the Smiley we are looking for. Tonally the book must be closer to *Tinker Tailor*…. I love the sheer, clean prose of *The Spy Who*, but I also love the more reflective *Tinker Tailor*, and I can hear my father—and Smiley—more clearly in the latter." (148–49)

In *Karla's Choice*, Cornwell, who grew up surrounded by the atmosphere of the Smiley-Karla conflict, listening to audiobooks of his father's novels and hearing him and his mother discuss the latest draft, has "manage[d] the same trick" as creators of the film versions: "to steal Smiley from his creator and make him just enough my own." And "to open the gates of the Circus so that other writers can, with due deference and due fearlessness, tell new stories into this same world." (150) In the meantime, Cornwell says that his novel "comes from the place where sons and fathers share space in one another's heads" and touchingly ends his contribution with a declaration addressed to his father who was with him as he wrote: "This book is a gift: to me—and to you." (150–51)■

a. See this author's review of *Karla's Choice* in *Studies in Intelligence* 69, no. 1 (March 2025).

intelligence in public media

KGB Literati
Spy Fiction and State Security in the Soviet Union

Reviewed by John Ehrman

Author: Filip Kovacevic
Published By: University of Toronto Press, 2025
Print Pages: 211 pages; notes, bibliography, index
Reviewer: The reviewer is a retired CIA officer.

Decades after the fall of the Berlin Wall, the great US and British spy novelists of the Cold War—Ian Fleming, Graham Greene, Len Deighton and John le Carré—remain well known to global audiences; all of them also had experience as intelligence officers. But how many people outside of Russia and the former Soviet Bloc know that the Soviets also had writers, including at least one woman, who had served in the KGB or its predecessors before turning to writing espionage tales? In *KGB Literati*, Filip Kovacevic explores the lives and work of these little-known, at least in the West, authors. The result is a fascinating look at how the Soviet version of the genre developed and how it continues to influence Russian culture and politics.

Kovacevic approaches his subject in a straightforward style. He starts by working chronologically through three major authors who were active from the late 1940s to the 1970s. He begins with Roman Kim, who might be considered the father of Soviet espionage novels, and then looks at the specific subgenres that emerged during the seventies and eighties. Kim was an especially interesting figure—an ethnic Korean, he may have joined the Cheka as early as 1921, becoming a successful and highly decorated counterintelligence officer, working against the Japanese in the Soviet Far East. Like so many other Soviet intelligence officers, he was arrested in 1937 and narrowly escaped execution. Kim eventually was released from prison in 1945 and began a literary career that lasted until his death in 1967.

Kovacevic describes how Kim made an in-depth study of US and British detective fiction, which he believed had tremendous cultural influence around the world—far

more than Soviet literature—even though he argued it had declined into an ugly brew of violence, materialism, and sensationalism. This led him to advocate for creating a Soviet "humanist alternative" that, based on true events and emphasizing "social justice, fairness, patriotism, and altruism," would counter harmful Western influences. (18) Kim followed this approach in his novels which, along with his mentoring of younger writers, established the template for the Soviet spy novel.

Like Kim, Zoya Voskresenskaya-Rybkina began her career in Soviet intelligence in the 1920s, and also like Kim she experienced ups and downs during it. Her assignments took her and her husband, also an intelligence officer, to postings in Helsinki and Stockholm; for a time she was even the acting resident in Stockholm. After her husband's death in 1947—apparently killed by a Stalinist murderer—she retained high-level positions in the KGB, apparently through the patronage of the storied Soviet operative Pavel Sudoplatov. After Stalin's death and Lavrenti Beria's execution, however, Sudoplatov was purged and sent to the Gulag. Rybkina then was dismissed from the service, but she managed to find work as the chief of security at the Vorkuta labor camp in Siberia. She retired in 1955, and began a literary career that focused on fictional tales of Lenin's use of espionage tradecraft to evade the Tsarist police.

Similarly, Oleg Gribanov, who became head of the KGB's Second Chief Directorate (domestic counterintelligence) in1956, was dismissed in 1964 following the downfall of Nikita Khrushchev. He then took up the pen and became popular enough that his novels had print runs of hundreds of thousands of copies (though Kovacevic believes he might not really have been fired, just reassigned to writing).

A most interesting aspect of the literature of this period is that the stories and novels were bottom-up efforts. That is, while these authors certainly hewed to official ideology—their tales focused on heroic revolutionaries and Chekists combating bloodthirsty capitalists and Americans, often using classic KGB methods of deception and double agents—they were true believers in the Soviet system and wrote on their own initiatives. But this does not mean that they were mere regime hacks. Kovacevic, in one telling passage, points out that they did not shy away from portraying the flaws of Soviet society. Gribanov's descriptions of consumer goods shortages, bad food, and the difficulty of surveilling enemy spies when the Chekists lacked cars and public transportation was unreliable and slow, Kovacevic notes, gave Gribanov's stories a verisimilitude that resonated with readers.

This changed, however, in 1969, when then chairman of the KGB Yuriy Andropov established a Press Bureau in the KGB. Among the bureau's missions was building popular support for KGB activities. Until the fall of the Soviet Union, the bureau would publish eight volumes of stories aimed at enhancing the service's reputation. Kovacevic describes how these officially-sponsored tales were constructed to send consistent messages to readers. Foreign intelligence services, often using unrepentant Nazis or their wartime collaborators as assets, were constantly working to destroy the Soviet system; citizens had to be constantly vigilant; and, especially, only a "psychologically disturbed individual" would cooperate with these vicious plots.[a] (101) Kovacevic also has chapters on stories and novels published by the regional KGBs—for example, who knew that Dagestan was a hotbed of Cold War espionage? These stories sent an additional message to readers, one promoting harmony among Soviet national minorities and a sense of their shared interest in protecting the socialist system. Nonetheless, while Andropov's project created a large body of propagandistic espionage fiction, Kovacevic's reviews imply that none of the KGB's authors left a literary legacy as significant as Kim's or Rybkina's.

This is a first-rate book on what at first glance might seem to be a niche topic. A Macedonian-born intelligence historian and human rights activist who teaches at the University of San Francisco, Kovacevic has done a prodigious amount of research in archives, secondary sources and, of course, reading large numbers of Russian-language spy novels and stories.

a. Not that Nazis were unknown in postwar Western spy fiction—Adam Hall's first Quiller novel, *The Quiller Memorandum* (1965), featured Nazis plotting a comeback. Overall, however, by the mid-60s Nazis had been supplanted by Communists as the villains in Western novels and disappeared completely in the seventies.

(Curiously, though, he omits from his citations and bibliography Julie Fedor's *Russia and the Cult of State Security* [2011], which also covers Andropov's propaganda campaign.) Kovacevic's capsule biographies of Soviet intelligence authors and analyses of their works are interesting in themselves, as they outline a literary culture that few would expect in the KGB. This is also a highly readable book. Kovacevic's style is concise, and he works through a large quantity of material and makes a number of insightful points in only 140 pages of text. Perhaps the book's only downside is that in his chapters on the Andropov-era books the plot summaries all sound the same—no doubt because the KGB authors essentially wrote the same stories over and over.

Kovacevic concludes on a disturbing note, one that goes beyond the stories themselves. Overall, he concludes the KGB's effort was a success. While admitting that hard evidence is difficult to come by, he cites survey data from the winter of 1991–92, the time of the USSR's collapse, that found a high degree of respect in Soviet society for the KGB and its professional abilities. The promotion of spy stories "aimed at shaping the hearts and minds of the Soviet public … left a notable trace in the collective post-Soviet consciousness," he writes. (140) Russian authorities apparently agree, as the FSB in 2006 resumed sponsorship and prizes for spy novels, movies, and TV shows. The films and stories, many of them authored by serving or former intelligence officers, continue to feature heroic Russian intelligence officers outsmarting their evil Western counterparts.

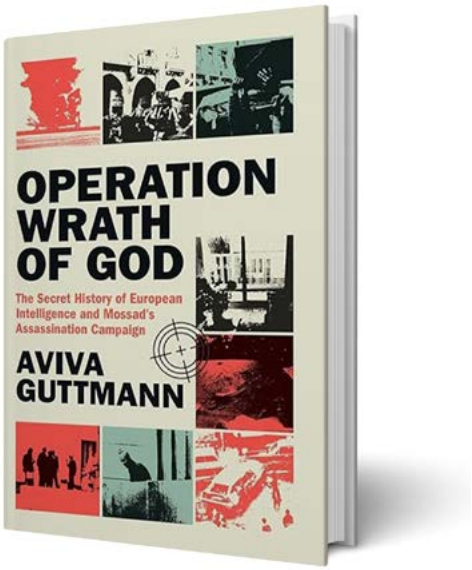
This is not simply an academic issue. Kovacevic points out that Vladimir Putin was himself shaped by the Andropov-sponsored fiction, and he and the KGB veterans with whom he surrounds himself "have identified with these fictional characters to such an extent that they see them as authoritative guides on what it means to live and act as true Soviet (now Russian) patriots." (141) Looking at KGB spy fiction, Kovacevic continues, provides an unexpected source for insights into Putin's foreign policy views and potential actions. Indeed, given the prominence of Nazi revenge plots in the KGB novels and Putin's accusations that present-day Ukraine has fallen into the hands of Nazi revanchists, it is hard to argue with Kovacevic.

Many of the books about Putin's reign stress the continuities with Soviet-era views and practices. *KGB Literati*, besides providing an informative review of Soviet spy fiction, fits well within this analytic school. For this reason, it is doubly worth reading.■

intelligence in public media

Operation Wrath of God
The Secret History of European Intelligence and Mossad's Assassination Campaign

Reviewed by John Ehrman



Editors:	Aviva Guttmann
Published By:	Cambridge University Press, 2025
Print Pages	336; notes, bibliography, index
Reviewer:	John Ehrman is a retired CIA officer.

How lucky can a researcher get? In a paragraph at the very end of *Operation Wrath of God*, Aviva Guttmann describes how she stumbled across a cache of Club of Bern cables in the Swiss National Archives. No endless FOIA process or blacked-out passages; rather, some 40,000 operational cables hiding in plain sight, waiting for someone to pore over them. Ultimately, they enabled Guttmann to piece together what she says is an entirely unknown dimension of the otherwise familiar story of Israel's revenge campaign against the Black September terrorists who carried out the Munich Olympic massacre in 1972.[a]

Guttmann starts her story with the founding of the Club of Bern in 1969 to provide a forum for the major West European internal intelligence services to swap information on counterterrorism and counterintelligence issues.[b] Although not part of the original group, the United States, Israel, and other West European states became involved with the club during the next few years. They were not formal members but had a type of associate's role that enabled them to join in the information exchanges, through a cable channel called Kilowatt. By the time of the Munich attack, writes Guttmann, the Kilowatt services had been working together for several

a. In the early morning hours of September 5, 1972, eight Black September terrorists broke into the Israeli Olympic team's quarters, killing two athletes and taking nine more hostage. Ultimately, five of the terrorists and all nine hostages were killed in a botched rescue attempt by the West Germans. For previous accounts of Mossad's post-Munich operations see Ronen Bergman, *Rise and Kill First* (Random House, 2018), reviewed in *Studies* September 2018; Aaron J. Klein, *Striking Back* (Random House, 2005); and Simon Reeve, *One Day in September* (Skyhorse, 2011).
b. The founding states were Belgium, France, Britain, Italy, Luxembourg, the Netherlands, Switzerland, and West Germany.

years and through the exchanges had built a solid foundation of trust.

The club swung into action immediately after the massacre in Munich. Guttmann details their exchanges, with each following investigative leads on the terrorists and then sending their findings to the others, including Israel, via Kilowatt. These, of course, generated more leads and exchanges, which led to an increasingly detailed picture of Black September's European network and operations. Not coincidentally, their efforts helped foil a number of other Palestinian terror plots.

Meanwhile, and unknown to club members, Israeli Prime Minister Golda Meir had given Mossad secret orders to find and kill the terrorists who had planned and carried out the attack. The effort eventually came to be known as Operation Wrath of God. It soon expanded to target Palestinians who had not been in the Olympic raid but were involved in planning, supporting, or executing other terrorist plots and activities. Through the Kilowatt exchanges, club members unwittingly provided Mossad's operations with targeting information that filled Israel's collection gaps; while they likely would have identified and tracked down the surviving Munich perpetrators and others on their own, Guttmann's detailed reviews of the Kilowatt reporting show how it enabled Mossad to speed up and refine its targeting.

The Kilowatt information was important not only for the Wrath of God operations. Perhaps the best example, which Guttmann details, is the hunt for Mohamed Boudia, a major Palestinian terrorist coordinator in Europe. An Israeli tip in early 1973 about a terrorist plot set off a Kilowatt investigation that eventually uncovered Boudia's networks and locations. While long known to the Europeans and Israelis, he moved constantly and used disguises to change his appearance, making him exceptionally hard to track down. The Israelis took advantage of the investigation to levy requirements and gather information on Boudia. As Guttmann notes, they used a "current investigation as a pretext to ask a partner to help find a terrorist who was on its kill list." (192) Eventually, the Swiss learned Boudia's Paris address and details about his car. Passed to the Israelis, the information enabled Mossad in June 1973 to place a bomb under Boudia's driver's seat and blow him and his car to pieces.

Similarly and especially in early operations, Mossad took advantage of Kilowatt's post-assassination reporting. Whenever a terrorist in Europe was mysteriously shot or blown up, the Kilowatt services began swapping information to support the ensuing investigation. Guttmann describes how these reports provided Mossad with an invaluable feedback loop, enabling it to identify and correct weaknesses in their tradecraft and thereby improve future operations. Among the lessons Mossad learned were that parking a rented getaway car too close to the scene of a shooting helps police obtain physical descriptions of team members and that fabricating a car bomb to appear like a homemade design that went off by accident will deceive investigators. It did not take the Europeans long to suspect that Mossad was behind the rising body count but, Guttmann concludes, they were content to look past the mounting evidence of Israeli culpability and let them get on with their dirty work.

Mossad enjoyed this best of all worlds for almost a year, with eight successful targeted killings in eight operations. Then, notoriously, it all unraveled in late July 1973, when, in Lillehammer, Norway, Mossad killed an innocent Arab waiter it had mistaken for a terrorist leader. Guttmann believes the misidentification was the result of Mossad becoming overconfident—the Lillehammer team had been composed of inexperienced officers operating in a country in which Mossad had no support infrastructure. The team members were wrapped up quickly. In the weeks that followed, the campaign was exposed in the press, making it impossible for the Europeans to continue to pretend Operation Wrath of God wasn't happening. Thus, Mossad had to end the operation and close down its networks across the continent. Tel Aviv, moreover, absorbed a wave of international condemnation. Interestingly, however, Guttmann demonstrates how the cables show how day-to-day Mossad–Club of Bern cooperation continued uninterrupted after Lillehammer, as if nothing had happened.

Guttmann, a former Swiss diplomat who teaches strategy and intelligence at Aberystwyth University in Wales, tells this story in a style that can only be

described as Germanic-academic. Starting with thorough research—beyond the cables, the 70 pages of notes and bibliography show an impressive mastery of the secondary literature—Guttman proceeds in meticulously organized chronological order, recounting each operation and investigation at length and in fine detail, frequently going Kilowatt cable by Kilowatt cable. The result is a wealth of information, but hardly a spy thriller. Guttmann's prose is dense, often repetitive, and tends toward no small amount of self-congratulation for having uncovered and used the Kilowatt cables. *Operation Wrath of God* is for specialists, not the general reader.

The book works best when Guttmann's claims are modest. That is, by filling in and expanding the historical record—demonstrating that no, Mossad is not a superhuman organization in need of no help from others—Guttmann does a service to historians of the post-Munich campaign. Her descriptions of how liaison relationships operate at the working level, too, are spot-on: it's the low- and mid-level officers who build trust by talking to one another every day that make the relationships work. Liaison work can be frustrating and time consuming, but *Operation Wrath of God* shows the potential of focused, long-term efforts.

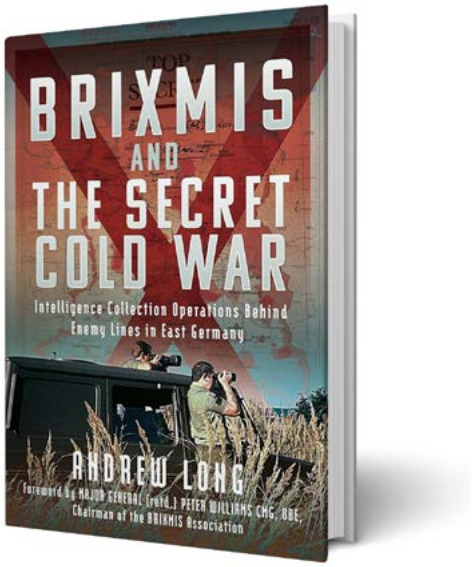
It is when Guttmann tries to draw additional lessons from the Kilowatt cables that the book disappoints. No doubt Guttmann is correct when she observes that Kilowatt cooperation continued post-Lillehammer, despite the Europeans' condemnations of Israel, because all parties gained from it. She also is correct in noting that governments often say one thing while they do another, and that intelligence services will work to advance their own interests, even if they might conflict with their governments' stated policies. But these behaviors have long been known and documented; while Guttmann is right to take note of them in this context, she spends too many pages on these familiar points.

Overall, *Operation Wrath of God* is a solid contribution to the history of counterterrorism operations and liaison relationships, and especially useful for revealing an unknown side of Mossad's post-Munich targeted killing operations. As a theoretical work, however, its claims are somewhat overstated. ■

intelligence in public media

BRIXMIS and the Secret Cold War
Intelligence Collection Operations Behind Enemy Lines in East Germany

Reviewed by Graham Alexander



Author:	Andrew Long
Published By:	Pen & Sword Books, Ltd., 2024
Print Pages:	244; appendices, endnotes, bibliography, photos, index
Reviewer:	Graham Alexander is the pen name of a CIA officer.

Author and Cold War historian Andrew Long has delivered, with *BRIXMIS and the Secret Cold War*, a fascinatingly thorough volume on British efforts to conduct intelligence reconnaissance missions throughout East Germany from 1946 through Germany's 1990 reunification and even beyond. The fulcrum of this effort was the British Commanders'-in-Chief Mission to the Soviet Forces in Germany (BRIXMIS), which operated on the basis on the Robertson-Malinin Agreement. Said accord, concluded among the Allied Powers in September 1946, permitted the reciprocal establishment of military missions in each country's German occupied zone. All four occupying powers exploited the nebulous description of "maintaining liaison" to conduct increasingly sophisticated intelligence-collection operations that continued even past the conclusion of the Cold War.

Long is nothing if not thorough when cataloguing even the most minute details of how BRIXMIS operated. Intrepid British military officers used a variety of automobiles and planes to photograph Warsaw Pact installations, arms, and movements, acting as a vital tripwire in a key Cold War fissure point. Interwoven in the chronicle are intriguing, sometimes hair-raising stories, that make a credible case about the exceptional value that BRIXMIS provided. Simultaneously, Long also shows how BRIXMIS's unorthodox operation, one outside the boundaries of more traditional collection vectors (HUMINT, SIGINT, IMINT), has meant that many analyses of Cold War intelligence have overlooked its contributions.

Long's BRIXMIS history flows forward in sometimes dense prose, but nevertheless rewards the diligent reader.

This is, in part, no fault of the author. One glossary at the front of the book listing acronyms comprises nine whole pages, meaning that some sentences are all but unintelligible to all but the most seasoned historian or military aficionado.

Nonetheless, there are fascinating accounts of how BRIXMIS officers moving through the German Democratic Republic managed to elude surveillance, surreptitiously enter sensitive facilities, and even escape pursuit during high-speed chases. One stomach-wrenching, but still insightful, section details how BRIXMIS personnel collected sensitive notes in rubbish piles outside Soviet military facilities. These notes, as BRIXMIS discovered, performed ancillary duties as toilet paper for often supply-starved Red Army conscripts.

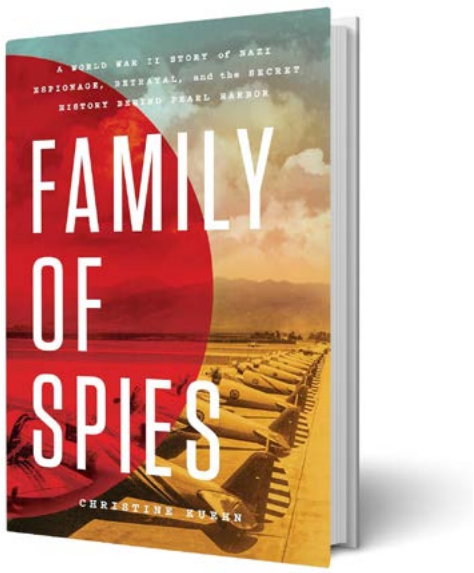
Long also details many of the hard lessons that BRIXMIS personnel learned as they concocted a kind of intelligence collection operation without clear precedent. The early years were clearly the least structured, but BRIXMIS officers gradually learned ways of map making, driving, preparation, and security practices, to name only several, which eventually solidified into an efficiently running machine. Long leaves no detail from the BRIXMIS side untouched. He discusses, for example, the furniture layout in BRIXMIS spaces as well as the specifications for the cameras and automobiles in extraordinary detail. Simultaneously, he makes important digressions into the ways that BRIXMIS intelligence proved its worth as part the Western Allies overall intelligence collection efforts. One passage details, for example, how one BRIXMIS mission succeeded in catching details on a surface to air missile system that had never been seen before in Germany—an intelligence coup of strategic significance to NATO.

Two elements could have transformed Long's work from worthwhile into essential for interested intelligence professionals. The goes back to Long's organization of the material. *BRIXMIS and the Secret Cold War* is organized in encyclopedic fashion, breaking down the BRIXMIS experience schematically before concluding with details on how it ultimately ceased. This is regrettable inasmuch as organizing events chronologically while treating various aspects of collection, tools, and opposition could have transformed the story into a true-life, page-turning spy thriller.

Separately, Long's impressive dedication to British sources does not apply with respect to East German or Soviet ones. Long makes references throughout to revelations culled from Eastern Bloc archives without ever fully committing to a thorough treatment of their operations, perspectives, and methods in response to BRIXMIS. Unquestionably, this examination would have contained valuable takeaways on the ways that perception and reality color the relationship between intelligence collectors and their counterintelligence adversaries. These critiques aside, *BRIXMIS and the Secret Cold War* remains a valuable source of information on an often overlooked facet of Cold War intelligence operations whose lessons remain applicable in the present. ■

intelligence in public media

Family of Spies
A World War II Story of Nazi Espionage, Betrayal, and the Secret History Behind Pearl Harbor



Reviewed by John Ehrman

Author:	*Christine Kuehn*
Published By:	Celadon Books, 2025
Print Pages	272; notes, index
Reviewer:	The reviewer is a retired CIA officer.

Finding out that your spouse or another close family member is a spy is a standard plot for an espionage novel. But what happens when you make that discovery in real life? That's what we learn in Christine Kuehn's *Family of Spies*, a combination of memoir and family research. Let's just say it's not pretty.

The story begins in 1994 when Kuehn, a journalist living in the Maryland suburbs of Washington, DC, received a letter from a screenwriter asking for information about her paternal grandfather, Otto, who he said had been a spy for the Nazis and aided the Japanese attack on Pearl Harbor. Kuehn's father, a German immigrant named Eberhard, had talked little about his family's past, and she had grown up understanding that her queries would be met with evasive responses. Nor did her father's sister, Ruth, ever talk much. "You have a good life," she told Kuehn, "you don't want to ruin it with the past." But the letter spurred Kuehn's curiosity and, after checking Gordon Prange's authoritative *At Dawn We Slept* (1981), she learned that, indeed, Otto had been a spy in Hawaii for the Japanese. From there, Kuehn began tracking down the details of her family's secret past.

Much of Otto's biography turned out not to be unusual for a German male of his generation. Born in 1895 to a prosperous family in Berlin, he grew up at a time when Germany led the world in science, technology, industry, and military power. Lacking direction after high school, however, Otto joined the navy and, in 1915, was taken prisoner by the British after his ship, the battle cruiser *Blucher*, was sunk at Dogger Bank. He would spend most of the rest of the war as a POW. Things did not go much better for Otto after the war—still "aloof and unfocused," as Kuehn describes him, he sought to make money fast and took his chances on a series of high-risk business ventures. Each failed, and he gradually ran through his inheritance. In the late 1920s, however, he hit on a winner when he opened a coffee-importing business in Berlin. Stability and prosperity soon followed, and his wife, Friedel—who already had a daughter, Ruth, from a previous relationship—gave birth to Eberhard in 1926.

Bourgeois respectability turned out to be boring, however. In 1928, Otto began working part-time in the German navy's secret police, hunting communists in the service. He turned out to be good at clandestine work and running agents. After attending one of Hitler's rallies, he also joined the Nazi party. Soon the family was all-in: Friedel joined the Nazi women's auxiliary, and Ruth, too, in 1930 entered the *Bund Deutscher Madel*. This level of commitment placed Otto in just the right position when Hitler took power in 1933, and he soon was an up-and-coming officer in the party's secret police.

But, once again, things went south for Otto. Tasked with pursuing corruption in the party, he actually tried to do so. Otto soon made enemies of high-ranking officials and narrowly escaped being murdered. But worse was to come. Otto's brother Leopold had become a deputy in Joseph Goebbels' Ministry of Propaganda,[a] and in early 1935 he brought Ruth, now a gorgeous 19-year-old, to a reception, where she was introduced to Goebbels, a notorious womanizer. An affair soon ensued, but ended suddenly when Goebbels found out that Ruth's birth father was Jewish.

This created problems for everyone. Goebbels had to make sure no one learned of the affair which, in the Germany of 1935, easily could have meant having Ruth killed and the rest of the family shipped off to concentration camps. But Goebbels was more clever than that and, instead, saw an opportunity to use Otto to nurture Germany's nascent alliance with Tokyo. Accordingly, he offered Otto—by now an experienced intelligence officer who also spoke English—to the Japanese and sent him and his family to Hawaii, where they could spy on the US military on Tokyo's behalf. Getting Otto to agree to the assignment was easy, as he was promised a salary and bonus totaling $30,000 per year (about $700,000 in 2026 dollars). Otto and Friedel left Germany in the spring of 1935, and the children followed a few months later. Everyone's problems seemed solved.

As spies, however, Otto's and Friedel's performances were decidedly mixed. They used the time-honored strategy of setting themselves up as a wealthy couple and then befriending local and military officials by inviting them to lavish dinners and parties. They became prolific reporters, helped by Otto's winning of a US Navy contract that gave him access to Pearl Harbor. But Otto's cover businesses, like so many of his ventures, went bust, and he and Friedel began badgering the Japanese for more money to finance their high living. This, in turn, created additional problems. Their "over-the-top galas, thin covers, and suspicious trips to Tokyo" and visits to the Japanese consulate attracted the attention of military intelligence and the FBI which, aided by codebreakers' clues about an unidentified German spy in Hawaii, began an investigation. The couple soon was under comprehensive surveillance; the only thing the FBI could not determine was whether they were spying for Germany or Japan. Clueless about their exposure, Otto and Friedel carried on to the point that a Honolulu newspaper could speculate about the true nature of their activities.

Ruth, in contrast, turned out to be a natural at espionage. Then in her early twenties and a full partner in her parents' efforts, she used her looks and charm to full effect. Young and beautiful, she was in demand with US Navy officers who, Kuehn writes, "played tennis with [Ruth], took her sailing and to dances … [and] unwittingly provided her with a good deal of information about the American Pacific fleet."

All this happens in the first half of the book but, while readers will know what's coming, Kuehn is a skilled writer who maintains the suspense of the spy story and keeps readers absorbed in the family drama. She is not an academic historian and, while her summaries of world events give the context for Otto's and Friedel's espionage, they are brief and superficial. That matters little, however, as this is a book about spies not 20th-century geopolitics, and Kuehn knows how to tell a page-turner of a story.

The best reason to read *Family of Spies* is not for the actual espionage—though Otto provides good lessons on how not to be a spy—but for the human side of the Kuehn family story. Much of this revolves around Otto, who seems mostly to have drifted through life

a. A dedicated Nazi to the end, Leopold died in the Battle of Berlin in 1945.

as a lost soul. From the start, in Kuehn's description, he not only was unable to figure out what to do with himself but also had a reckless, gambling personality. These traits led first to his failed ventures in the 1920s and then to the behaviors that attracted the FBI's attention; the time in his life that Otto had the most stability was when he was subject to the discipline of the Nazi party, although there, too, his inability to read situations and navigate party infighting nearly cost him his life. Friedel, too, comes across as a complex but weak character, by turns maternal, supportive of Otto, manipulative, paranoid, and finally foolish. Otto's and Friedel's ultimate fates, readers will not be surprised to learn, were pathetic. Ruth, who married an American after the war and returned to the United States, turned out to be the most resilient of the bunch.

Otto's espionage echoed through the generations. Eberhard was 15 at the time of the Japanese attack on Pearl Harbor and, unaware of his parents' and sister's spying, had turned into a typical American teenager. He was horrified when he learned the truth and testified for the prosecution at Otto's trial in February 1942. Allowed to stay in Hawaii with a foster family, Eberhard joined the US Army as soon as he graduated from high school and fought on Okinawa. But after the war Eberhard had almost no contact with his parents and for the rest of his life felt he had to hide a shameful, much larger truth, inventing explanations and changing the subject whenever Christine asked about his parents or growing up in Hawaii.

At bottom this is what *Spies in the Family* is about—not only how espionage can tear a family apart, but how each member copes with its aftermath. For Eberhard and Ruth, it was pretending the past did not exist. For Christine, however, it was about uncovering and confronting the past, and asking hard questions about her family's enthusiastic Nazi record and how she might have behaved had she been in Otto's, Friedel's, or Ruth's shoes. She has no definite answers, but *Family of Spies* is worth reading for anyone interested in such issues.■

intelligence in public media

The Mysterious Virginia Hall
World War II's Most Dangerous Spy

Reviewed by Hayden Peake

Authors:	*Claudia Friddell*
Published By:	Calkins Creek, 2025
Print Pages:	156; endnotes, bibliography, photos
Reviewer:	Hayden Peake has been contributing reviews to *Studies* since 2002.

Searching CIA's public website for "Virginia Hall' results in a series of pages and pictures that summarize the story of the agency's first female operations officer. In *The Mysterious Virginia Hall*, author Claudia Friddell, with the help of family recollections, artifacts, and archival documents, adds details about her early life and intelligence career.

A farm girl from Maryland, nicknamed Dinky by her family, Hall enjoyed horseback riding, hunting, sports, and academics. Her high school yearbook described her as a natural though cantankerous and capricious leader who was class-president, yearbook editor-in-chief, and "the most original of our class."

Friddell explains that it was during family trips to Europe that Hall decided she would become an ambassador one day. After completing university in France, she made multiple applications to the US Foreign Service. All failed for different reasons, and she accepted an offer to become a State Department clerk. During service in Turkey her ambitions suffered another setback. While bird hunting, she shot herself in the foot, and the complications led to the amputation of her left leg just below the knee.

Undaunted, after recovering at home, Hall returned to her job and was rejected once again for the Foreign Service, ironically this time because she was disabled. Frustrated, she resigned from State, returned to Paris and after the start of WWII, she volunteered to serve in the women's branch of the British Army. Rejected because the Brits weren't accepting foreigners, she became an ambulance driver in France, prosthetic leg—named Cuthbert—notwithstanding.

After France fell to the Nazis, Hall returned to Britain, a decision Friddell emphasizes, that changed her life forever. By August 1941, she had been recruited and trained by the Special Operations Executive (SOE), the covert action arm of British intelligence. Returned to France under journalistic cover, she eventually joined the French resistance "Heckler Circuit" where her performance amazed SOE. When in early 1943 the circuit was betrayed to the Gestapo, the "Limping Lady" as she was then known, escaped by crossing the Pyrenees on foot in the winter, and after a brief internment by Spain, returned to London.

When SOE refused to risk retuning Hall to French resistance work, she quit and enlisted in the OSS. Trained as a radio operator, Hall was sent to France disguised as an elderly woman. There she served until V-E Day.

By then, Hall had decided on an intelligence career, and Friddell explains how she kept her cover when Hall was awarded the Distinguished Service Cross—the only civilian woman so honored during WWII—in a private ceremony, and joined the Central Intelligence Group and then the newly created CIA.

She spent her CIA years working in covert action and retired at the then mandatory age of 60. Hall spent her retirement years in Maryland with her husband, a former agent himself, Paul Goillot. She died in 1982. ■

intelligence in public media

Two Streaming TV Series: *The Agency* and *The Day of Jackal*

Reviewed by Resolute Lee

The Agency: Central Intelligence

(10 episodes, streamed on Paramount Plus, 2025)

Whispers of John le Carré abound in this emotionally contemplative series that serves as a compelling exploration into the psychological aspects of espionage. *The Agency* is character-driven storytelling woven in threads of human frailty; frayed individuals threaten to unravel at the slightest pull. An adaptation of Eric Rochant's French series *The Bureau*, the series is thoroughly entertaining.

With a talented ensemble cast, including Michael Fassbender as the enigmatic Martian, the show explores the complexities of espionage and the blurred lines between identity and deception.

The series begins with the asocial Martian, a non-official cover officer, being thrust back into his true identity, after stepping off a black jet before being swept away to a desolate safe house under the cover of night. The next morning, Martian is in London after an unexpected exfiltration from a six-year undercover operation in Addis Ababa, Ethiopia, and is now forced to navigate a complex web of relationships and obligations. He must reconnect with his teenage daughter Poppy (India Fowler); come to terms with the loss of Sami (Jodie Turner-Smith), whom he left behind in Ethiopia; and respond to an emergent crisis in London, when a CIA asset suddenly goes missing in Belarus. Meanwhile, Martian is being surveilled by his own agency in a post-operation protocol designed to assist Martian's reintegration.

The Agency is analytic, striking a blend of exposition and silence that allows scenes to unfold with emotion and imagery, absent words or over explanation. Fassbender's untethered intensity is veiled beneath a fraying façade of calm as he guides CIA station colleagues through a perilous agent recovery operation. Martian navigates the professional obstacles with ease, while his personal life unravels in the shadows, or so he believes. In actuality the surveillance he's been under intercedes at key points, forcing Martian to employ his espionage tradecraft on his own agency as he maintains unauthorized contact with Sami, leaving the audience to wonder whether she was an asset, a lover, or an adversary.

Meanwhile, Martian's tradecraft does not go unnoticed. His boss, Deputy Chief of Station Henry, played by the versatile Jeffrey Wright, sees through Martian's subterfuge, offering candid and thoughtful mentorship in an attempt to ease Martian's internal turmoil. The arrival of Dr. Blake (Harriett Sansom Harris), a psychologist sent from headquarters to evaluate Martian's mental health further confounds his suppression and intensifies the agency's intrusions into his life. This subplot culminates in tense interview where Martian posits, "you're not trying to help me, doctor. You're worried I may have somehow become sane," a profound moment of self-reflection that leaves Dr. Blake speechless.

The espionage tradecraft employed in the series is bounded within credulity and a heightened realism is achieved in scenes where the characters' emotions were a focal aspect while employing the tradecraft. For example, as Martian is organizing his alias and cover identification documents for return to the station, he decides to keep the cover driver's license, setting in motion a major plot line focused on maintaining a relationship with Sami even at peril to himself.

From the use of safe houses, to beaconing, surveillance, and countersurveillance techniques; the use of alias and cover identifications, including accountability of those documents; covert communications between assets and handlers, we are given more than a glimpse into the craft. The tradecraft and technology seemingly become tools used only to heighten the emotional aspects of what transpires on the screen. At a few points along the way the pacing slows with expanding subplots, which at first appear confusing or perhaps serve as red herrings. Though it becomes clear the plots are snapshots into world building, setting the stage for a follow-on season. *The Agency*, is a thoughtful depiction of the espionage genre, offering a story that is as much about the choices intelligence operatives' make as it is the psychological scars those choices leave behind. ■

The Day of the Jackal

(10 Episodes, streamed on Peacock 2024–25.)

This is a stylishly reimagined and contemporary adaptation of Frederick Forsyth's 1971 novel, also a 1973 film. Written by Irish novelist and screenwriter Ronan Bennett, the series opens with immediate tension revealing the Jackal, aka Alex Duggan (Eddie Redmayne), cleverly disguised with prosthetics, muttering German before a mirror. Having just killed a man to assume his persona and thereby his access, the Jackal has laid the foundation for a far more complex follow-on operation. The assassination of a divisive politician with a bespoke rifle from a distance that is seemingly impossible.

The Day of the Jackal is a gripping series with Jason Bourne-esque action sequences and stunning cinematography. The Jackal's European globetrotting does border on distracting, though it highlights specific aspects of his expertise, tradecraft, and extensive target research. Redmayne delivers an engaging performance, crafting Forsyth's Jackal as a cold predator fraught with moral ambiguity and a detail-oriented perfectionism.

Bennett's Jackal is a dispassionate, process-driven predatory chameleon who excels at stalking his prey while using others, mostly unwittingly, to achieve the ends. Steeped in the use of alias, disguise, and an array of tradecraft skills, the Jackal extensively researches his targets and carries out his operations all while anticipating his adversaries almost prophetically. Though the Jackal does make mistakes along the way, it adds to the character's frailty. He is an anti-hero for whom this reviewer routed. At times throughout the series the Jackal is forced to adapt plans on the fly, relying on honed escape and evasion tactics and when necessary eliminating those who threaten his mission or secrecy, even the innocent.

The Jackal's skills in the dark arts are unveiled with each episode of the series as he decisively solves problems that arise in his mission to assassinate a high-profile tech philanthropist whose pending software release, called River, threatens to reveal how billionaires spend their money. Prompting the ire of at least one global oligarch who's hired the Jackal to assassinate the philanthropist before the software's release. As the Jackal moves further along his operational timeline he is drawn into a cat-and-mouse game with a dogged MI6 intelligence officer, Bianca (Lashana Lynch), who will stop at nothing to capture the elusive Jackal even if it leaves a trail of death in the wake. The two are presented as flawed characters, both driven by mission at all cost, regardless of the destruction to themselves and others.

While some viewers may find adapting the novel into a 10-part series as being a tad drawn out, doing so does allow for subplots and backstory focused on the Jackal's origins and his relationship with his wife and child, which is an aspect of the character not seen in previous renderings. These subplots add to the character's dimensionality, but make no mistake, the Jackal is a hired killer who offers no apologies for his chosen profession. A highlight in the series is a flashback exploring the Jackal's military sniper experience in Afghanistan. The flashback episode unveils Duggan's experience with the horrors of war, and becomes the defining moment that prompts his escape from the military and the dispassionate manner in which he executes it, leading him to the path of an assassin. In sum, *The Day of the Jackal* is an engaging series from start to finish. ■