

STUDIES

IN INTELLIGENCE | Vol. 68, No. 3 (September 2024)



The OSINT Challenges in China

Debating Open Source
Roundtable Discussion
Practitioner's Perspective
Open Source Agency

Intelligence in Public Media

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

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

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

Requests for subscriptions should be sent to:

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

ISSN 1527-0874

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

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

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

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

Cover image: An ancient Chinese city wall.

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 also includes the CIA's History Staff, Lessons Learned Program, and the CIA Museum.

Contact The *Studies in Intelligence* staff welcomes proposals for articles, book reviews, or commentaries and other communications from outside of the Intelligence Community. Proposals may be sent to the *Studies* staff through "Contact CIA" on cia.gov or mailed to:

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

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

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

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

EDITORIAL POLICY

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

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

The criterion for publication is whether, in the opinion of the board, the article makes a contribution to the literature of intelligence. Board members are all active or former Intelligence Community officers.

EDITORIAL BOARD

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

EDITORS

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

Contents

Vol. 68, No. 3 (Extracts, September 2024)

Perspectives on Open Source Intelligence

Debating How the IC Should Approach Open Source Intelligence: A Roundtable Discussion
John Pulju 1

Debating Open Source: A Practitioner’s Perspective
Amelia Favere 15

The Case for Creating an Open-Source Intelligence Agency
William Usher 23

Open Source at a Critical Point in History: The View from CIA’s Directorate of Digital Innovation
Daniel L. Richard 29

China’s Thickening Information Fog: Overcoming New Challenges in Analysis
Jonah Victor 31

Intelligence in Public Media: Reviews

Open Source Investigations in the Age of Google
Reviewed by Stephen Mercado 51

Counter-Intelligence: What the Secret World Can Teach Us About Problem-Solving and Creativity
and
Challenger: A True Story of Heroism and Disaster on the Edge of Space
Reviewed by John Ehrman 53

The Last Honest Man: The CIA, the FBI, the Mafia, and the Kennedys—and One Senator’s Fight to Save Democracy
Reviewed by David Robarge 59

The Achilles Trap: Saddam Hussein, the CIA, and the Origins of America’s Invasion of Iran
Reviewed by Brent Geary 63

Zhou Enlai: A Life
Reviewed by Matthew J. 67

(Continued on following page.)

Intelligence in Public Media (cont.)

Bombing Hitler's Hometown: The Untold Story of the Last Mass Bomber

Raid of World War Two in Europe

Reviewed by David A. Welker

71

The Suicide Museum: A Novel

Reviewed by Graham Alexander

73

Intelligence Officer's Bookshelf

Compiled and reviewed by Hayden Peake and others.

75



Contributors

Article Contributors

Amelia Favere is an open-source expert and member of the Lessons Learned Program in CIA's Center for the Study of Intelligence.

John Pulju is director of the Center for the Study of Intelligence and chair of the *Studies in Intelligence* Editorial Board.

Daniel L. Richard is the Associate Deputy Director of CIA for Digital Innovation.

William Usber is a retired CIA senior intelligence analyst. He is now senior director for intelligence with the Special Competitive Studies Project.

Jonah Victor is a Visiting Research Fellow at the Institute for National Strategic Studies of the National Defense University. He has served as a senior China analyst at the Department of Defense. The author thanks Phillip Saunders and Joel Wuthnow for their support and advice on this project.

Reviewers

Graham Alexander is the penname of a CIA operations officer,

John Ehrman is a retired Directorate of Analysis officer and frequent contributor to *Studies*.

Brent Geary is a member of CIA's History Staff and a member of the *Studies* Editorial Board.

Matthew J. is a CIA analyst. He previously taught and researched East and Southeast Asian politics and PRC foreign policy.

Stephen Mercado is a retired CIA open-source officer and frequent contributor to *Studies*.

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

David Robarge is the chief of CIA's History Staff.

David Welker is a member of CIA History Staff.





Debating How the IC Should Approach Open Source Intelligence

A Roundtable Discussion

John Pulju

John Pulju is director of the Center for the Study of Intelligence and chair of the *Studies in Intelligence* Editorial Board.

Experts have been debating how the US Intelligence Community should approach open-source collection and analysis for decades. This debate has intensified as the information revolution has gathered pace. Commentators have advocated for approaches ranging from creating an open-source agency to relying almost entirely on the private sector. The debate may even intensify as artificial intelligence (AI) capabilities expand and the IC's budget environment tightens. In this context, a group of two dozen IC and private sector open-source practitioners

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

and thinkers met in June 2024 to discuss four possible approaches. The roundtable began with opening remarks by this author and IC OSINT Executive Jason Barrett, who both noted the event was intended to compare the approaches and tease out assumptions, tradeoffs, and practical implications—such as resource needs—that would help future decisionmakers grapple with how to proceed.

Four Approaches

Private-sector thinkers who also have extensive experience in the IC and US government took the lead in laying out the case for each of the approaches. Following this, Randy Nixon, the director of the Open Source Enterprise (OSE), engaged the speakers and other participants in a wide-ranging discussion. To aid debate, CSI asked the speakers to push the bounds in making the case for each approach while also addressing pros, cons, and tradeoffs. Speakers and other participants understand there are many potential variants of each approach as well as the possibility of mixing and matching elements.

Reinforce Federated Programs

Emily Harding made the case to reinforce current IC programs, centered around OSE leading a federated IC-wide effort to aggressively implement the new OSINT strategy. This approach

Roundtable Speakers

Sam Gordy is President, Janes Group U.S. with 40 years' experience working with defense, intelligence, and civilian government customers in the United States and abroad. Before joining Janes in 2023, Sam spent the bulk of his career at SAIC-Leidos and five years with IBM. Throughout his career he has focused on providing clients with information technology products, services, and solutions in areas ranging from cyber security to exploiting cognitive systems. He has served as an adjunct lecturer at Georgetown University and began his career as an intelligence officer in the US Navy.

Emily Harding is Director of the Intelligence, National Security, and Technology Program at CSIS and Deputy Director of the International Security Program. She has served in a series of high-profile positions, notably including Deputy Staff Director of the Senate Select Committee on Intelligence, Director for Iran on the National Security Council Staff, and Deputy Chief of CIA's Iraq Group during the attempted ISIS takeover. She is an adjunct lecturer at the Johns Hopkins School of Advanced International Studies.

William "Chip" Usher is Senior Director for Intelligence at the Special Competitiveness Studies Project. Prior to SCSP, Chip served 32 years at CIA, where he held a variety of executive positions and was a member of the Senior Intelligence Service. He has expertise on East Asia, the Near East, and Eurasia as well as IC modernization. He is passionate about enhancing the IC's ability to provide timely, relevant intelligence insights to US decisionmakers. Before joining the US government, Chip ran an import-export company in Nagoya, Japan.

Kristin Wood is CEO and Co-Founder of August Interactive, a deep-tech start-up that is building immersive games and experiences. She serves on the advisory boards of numerous tech start-ups and venture capital firms. In her 20 years at CIA and in the Senior Intelligence Service, she served as a PDB briefer, led the team assessing whether Iraq had a role in the 9/11 attacks, and was a Deputy Chief of a Middle East division in the National Clandestine Service. In her final CIA position she served as the Deputy Director of Innovation and Technology at the Open Source Center.

would expand use of AI tools like OSIRIS to summarize, translate, and disseminate open-source data, including identifying source biases and identifying new insights. Dissemination of OSINT products would be across the IC and beyond. She noted the ODNI OSINT strategy hits the right key areas: structuring and sharing

data; developing data-science tools and rigorous tradecraft standards; and integrating open source fully into the IC's work, particularly all-source analysis. She argued this approach is preferable to creating an Open Source Agency (OSA), which would be disruptive as it stood up and create more complexity in an already sprawling IC.

She also assessed it would be no more likely to receive adequate resources or authority than current IC components—both of which she believes need to be increased. The federated approach also offers flexibility for IC components to tailor their OSINT activities to needs ranging from tactical support to combat forces to all-source assessments for national-level policymakers.^a

Adopt a Surgical Approach

Kristin Wood argued that the IC should create a non-profit Public-Private Consortium to leverage the rapidly growing number of firms, individuals and organizations that are exploiting the explosion of information.^b With digital information now counted in zettabytes—one trillion gigabytes—across a dizzying array of media the IC cannot hope to keep up with the thousands of entities that have emerged to capture and analyze it. Instead, the consortium would leverage what has become a \$58 billion industry to glean what the IC needs to accomplish its mission. The consortium would scan the horizon for useful content and tools. It would foster common tradecraft standards among its members, vet sources, set prices, and provide data to components across the IC. It might create

The IC OSINT Strategy, 2024–2026

The Strategy aims to build an integrated and agile OSINT community that can extract insights from the vast amounts of open source data to both deliver unique intelligence and enable other collection disciplines.¹ It terms OSINT “the INT of first resort” and defines it as “intelligence derived exclusively from publicly or commercially available information that addresses specific intelligence priorities, requirements, or gaps.” The Strategy aims to bolster IC effectiveness in the current federated approach with the DCIA as the Functional Manager while also boosting partnerships with industry, academia, and foreign counterparts. It lays out four areas of strategic focus:

- **Coordinate Open Source Data Acquisition and Expand Sharing.** Avoiding redundancy and expanding sharing of open source data and tools are priorities, as are ensuring the most efficient use of IC resources.
- **Establish Integrated Open Source Collection Management.** A priority is developing processes, tools, and metrics to align collection efforts to ensure they meet priority needs, cover gaps, avoid duplication—including with sensitive collection efforts—and comply with privacy and civil liberties.
- **Drive OSINT Innovation to Deliver New Capabilities.** A priority is accelerating development and adoption of tools to exploit open source data and information, particularly in areas like AI, machine learning and human language.
- **Develop the Next-Generation OSINT Workforce and Tradecraft.** Priorities include establishing common tradecraft standards needed to exploit the digital environment, updating them regularly, and training both a cadre of highly skilled OSINT specialists and the IC workforce.

CIA’s Open Source Enterprise executes the DCIA’s responsibilities as Functional Manager. CIA leads the National Open Source Committee, an IC group that shares best practices, identifies gaps, and develops joint solutions to common challenges. The Committee has made notable achievements in areas like aligning and deconflicting purchases of CAI, building an inventory of OSINT tools and technology, and establishing common tradecraft and training.

an automated OSINT feed—a *Drudge Report* for the IC—and

could broker ad hoc taskings and data acquisitions. Wood noted that

a. OSIRIS is an OSE tool available to the IC that applies generative AI to develop insights from a wide range of open-source material. It reached initial operational capability in 2023.

b. William Usher also advocates for a consortium, which could be tied to an Open Source Agency. For further details, see Wood and Usher’s article, “The Intelligence Community Can Tackle Open-Source Data in a Hyper-Connected World,” *Cipher Brief*, December 21, 2023, and “Intelligence Innovation: Repositioning for Future Technology Competition,” Special Competitive Studies Project Interim Panel Report, April 2024.

keys to success would be flexibility, agility, and “living” in the open-source world. The Consortium would be small—\$20 million might be enough to operate it, at least initially.

Rely on the Private Sector

Sam Gordy advocated privatizing the overwhelming bulk of OSINT collection and analysis. He argued that the information revolution has given the private sector capabilities not only in areas like social media and AI, as Harding and Wood argued, but also in areas that historically were restricted to government, such as IMINT and SIGINT. At the same time, commercial analytic capabilities have matured to “turn open-source information into OSINT.” He argued that relying on the private sector would reduce costs, whether for people or facilities. It would offer an increased ability to surge globally and take advantage of cultural expertise, language skills, and real-world experience with the systems, doctrine, and tradecraft of our adversaries. He said challenges include counterintelligence and OSINT tradecraft—including detecting disinformation—and linking to the classified “high side.” Firms that specialize in OSINT, however, are able to overcome these challenges through coordination with the IC and other government customers.

Create an Open Source Agency

William Usher made the case for consolidating IC OSINT programs and resources in an Open Source Agency (OSA). He argued this would be surest path to ensuring the necessary funding is devoted to OSINT, to developing a sizable cadre of officers who are skilled in “living” in the open-source world—most would not have security clearances—and to giving open source a strong voice in driving how the IC will satisfy intelligence requirements. OSA’s primary purpose would be to quickly obtain, curate, and share commercially and publicly available datasets across the IC. It would be the “one stop” shop for commercial vendors, set standards for incorporation of OSINT data, and evaluate platforms and tools to get and exploit it. Like NRO for overhead collection and NSA for SIGINT, it would have authority to approve and guide any individual agency OSINT efforts. As it became established, OSA could also add in-house analytic capabilities and develop unclassified collaboration spaces with US and foreign partners. And, it would work with other IC officers to incorporate OSINT into all-source products while training them in basic techniques—“teaching them to fish.” [See Usher’s separate article in this edition of *Studies* for more details on his proposal.]

Key Themes

The speakers and other participants agreed that whatever approach the IC takes, it needs to improve its exploitation of open source. Much of the debate was about resources and how to change the culture of the IC so that OSINT could become truly the “INT of first resort.” Beyond the basic differences among the four approaches, participants suggested different ways to tackle this goal. The debate also revealed differing approaches to topics like security and clarified some choices decisionmakers would need to make if they decided to pursue one or more of the approaches.

Untapped Potential

The speakers and other participants in the roundtable all agreed that the Intelligence Community is not taking enough advantage of OSINT. They added that urgent action is needed. IC OSINT executive Jason Barrett said that OSINT could satisfy 60–70 percent of US intelligence requirements. Brad Ahlskog, director of DIA’s OSINT Integration Center (OSIC), suggested the share might be as high as 80 percent. Nixon said the gap between what the IC is doing and could be doing is growing because funding does not match the ability of the IC to take advantage of commercially available information (CAI). Usher echoed this view, noting that the explosion of data is the story; both

Debating How the IC Should Approach Open Source Intelligence

Approach	Features	Resources	Practicalities & Areas to Clarify	Arguments For	Arguments Against
Federated	<ul style="list-style-type: none"> Drive IC OSINT Strategy Keep Separate Components OSINT Champion (Directorate?) Set Standards, Tradecraft Expand OSINT Dissem 	<ul style="list-style-type: none"> More Funds More People 	<ul style="list-style-type: none"> AI Critical-Tools, Skills 	<ul style="list-style-type: none"> IC on Right Track Already Minimal Disruption of Change Components Can Tailor to Needs Protects Security/CI Meets Consumer Need 	<ul style="list-style-type: none"> Informal authority insufficient Doesn't make OSINT equal "INT" Local decisions hurt efficiency, quality Components raid OSINT resources Feckless to compete with private sector
Consortium "Surgical"	<ul style="list-style-type: none"> Public-Private 501c3 Scan horizon for data, tools Build Partnerships Foster standards, sharing One-stop shop to reach IC 	<ul style="list-style-type: none"> \$20 million to run A few IC officers 20-30 private sector 	<ul style="list-style-type: none"> Highly flexible on size, topics Could fit with other approaches POC for procurement? 	<ul style="list-style-type: none"> Keeps up with Info Revolution Ingest, acquire only what needed Cost-federated buying Private sector entre to IC 	<ul style="list-style-type: none"> Minimal impact if small Cost savings unclear Greater CI, security concerns Drift into topics of marginal FI value Potential privacy issues Privatization Outsource
Privatization	<ul style="list-style-type: none"> Outsource almost all OSINT Most collection, analysis private IC focus on sensitive collection Components drive what needed 	<ul style="list-style-type: none"> Fewer IC officers More Funds 	<ul style="list-style-type: none"> Keep small IC unit for niche topics How to organize procurement 	<ul style="list-style-type: none"> Cost-unclassified cheaper Ingest, buy only what needed Flexibility – surge, tailor to user Eases privacy issues 	<ul style="list-style-type: none"> Cost savings illusory (profit) Deconflicting procurements & ops No objective IC OSINT experts Greater CI, security concerns
OSINT Agency	<ul style="list-style-type: none"> Consolidate OSINT in new Agency Director OSINT Champion Set standards, tradecraft Emphasize acquiring, sharing Control procurement funds 	<ul style="list-style-type: none"> Large 2000-3000 people Billion \$+ 	<ul style="list-style-type: none"> Authority over other IC agencies Cost-Federated buying Promotes quality Deconflict security, CI issues 	<ul style="list-style-type: none"> Elevates OSINT as Equal "INT" Cost-Federated buying Promotes quality Deconflict security, CI issues 	<ul style="list-style-type: none"> New IC stove-pipe; overlap with others Long, disruptive period to create Feckless to compete with private sector Components lose ability to tailor to needs

he and Wood said the US is getting crushed by China, Russia, and other adversaries that are investing heavily in exploiting OSINT. Gordy agreed with this.

The speakers commented that former IC officers are often stunned by the volume and variety of OSINT that is available. Harding gave an example of a 1,000-page SSCI report on Russian election meddling that drew on a million pages of open-source material. She also noted that the social media platform X provides early detection of events ranging from natural disasters to the US raids that killed Usama bin Ladin and ISIS leader Abu Dua. Wood flagged the growing importance of virtual reality for communications, relationship building, and even business. She said the IC has barely tapped this “fusion world” and needs to understand it to avoid surprise. Gordy noted the proliferation of private intelligence, marketing, and other firms that are exploiting “adtech,” commercial imagery, and other open sources to track the war in Ukraine. The speakers also stressed the utility of OSINT in providing timely insights to US officials and partners. Harding commented that it offers the potential to provide instant delivery via mobile devices to intelligence consumers anywhere, anytime. Several participants cited the

advantages of OSINT in allowing the IC to push insights to foreign partners, local governments, and the public. They see this as a growing part of the IC’s mission.

Coverage

The four approaches emphasize different aspects of open source and different roles for IC OSINT components. All focus on digital data generated by the information revolution—both the mass of data and metadata available in social media, virtual reality, the “internet of things,” and elsewhere as well as the tools that have been developed to extract intelligence from digital information, ranging from basic search tools to AI applications. However, the IC would probably end up ingesting and processing much less digital information under the Privatization and Surgical approaches because these rely much more heavily on the private sector to extract insights.

Privatization would also give greater weight to commercially available imagery, SIGINT, HUMINT, and all-source analysis. Gordy termed OSINT “the INT of INTs,” echoing views Mark Lowenthal expressed in his 2001 *Studies* article about how open-source information is pervasive with other INTs.^a He gave examples of Jane’s global network

of employees—essentially providing open-source HUMINT. Participants also noted the ability of firms and people to track battlefield movements in Ukraine and Gaza with commercial imagery and “adtech.” Gordy argued that the IC should concentrate on areas where clandestine and other sensitive collection are truly needed. He said clandestine HUMINT should be the INT of last resort, given the risks to the people involved.

None of the speakers discussed where the boundary would be defined between OSINT and other unclassified IC activities, such as internet research, analytic outreach, or purchase of CAI. The discussion suggested they would want to minimize overlap and conflict, while recognizing that boundaries might be fuzzy. Usher, for example, proposed that an OSA would only gradually begin producing analytic products to minimize conflict with all-source agencies. (Ahlskog and Nixon noted that their components already produce OSINT-only analytic products.) Privatization might ease the problem by leaving it up to a wide range of IC components to decide what activities to retain and what to outsource.

Nixon commented that many participants are defining OSINT narrowly as social media or that which is only digital. He noted

a. Lowenthal wrote, “OSINT is the most pervasive of the INTs, rather than a separate category. It occupies its own niche as well as some part of each of the other INTs (HUMINT, IMINT, MASINT, SIGINT). Beyond the textual sources of OSINT, the only aspect that differentiates it from other collection disciplines is the fact that it is not clandestine in nature.” “OSINT: The State of the Art, the Artless State,” *Studies in Intelligence* 45, No. 3 (September 2001).

Studies Articles on Open-Source Intelligence

Open source has been a recurring topic in *Studies in Intelligence* from the 1950s through today, including most recently roundtable participant Chris Rasmussen's article (June 2024) on the need for an open-source agency. Early articles highlighted the amount and variety of open sources as well as their importance, particularly in the absence of other intelligence on hard-target countries. J.J. Bagnall (1958) and David Moore (1963) detailed open sources including "gray literature" (not quite public, not quite secret) to periodicals, books, radio, television, émigrés accounts, and Western academics. They describe these sources as "many and varied." Open sources accounted for the majority of intelligence on such topics as Soviet military doctrine, weapons programs, research and development, and order-of-battle. Both authors noted challenges that persist today—lack of foreign language and translation services, the scattered nature of sources, the difficulty of validating materials, and the need to process vast amounts of data.

Although the increasing availability of satellite photography undoubtedly reduced the IC's reliance on open sources for Soviet military topics, Herman Croom (1969) noted they were still important—often providing the first indications of research and development of military significance—as well as being key in other areas, such as leadership plans and intentions. Gail Solin (1975) stressed not only the criticality of open sources but also the development of "Sinology" and "Kremlinology" to tease insights from fragmentary and opaque sources. For example, she noted that counting uniform pockets was a key to identifying officers in the People's Liberation Army after insignia were abolished during the Cultural Revolution. Croom and Solin both emphasized the need for deep expertise to make sense of open sources and cut through propaganda—what today might be termed disinformation. Croom also dwelt on implications of the information explosion—an explosion that the IC has seen as both an opportunity and a challenge ever since.

As the Cold War gave way to 24/7 cable news, commercial satellite imagery, and the "cyberworld," David Gries (1991) and David Overton (1992) saw open sources as critical to intelligence during the 1990s. Gries argued that open sources already provided 80 percent of analysts' information and that this would grow. Mark Lowenthal (2001), John Gannon (2001), and Stephen Mercado (2004) continued this theme in their articles of the early 2000s; they stressed the need to develop ways to collect and process the huge amounts of data that were being made available by the internet and to develop strong tradecraft for OSINT—a term that had come into vogue. Many of their recommendations on organization, resources, and tradecraft resonate with the debate that continues today. Among many other articles that touch on OSINT, one with particular relevance is Marty Petersen's argument (2003) that effective political analysts must have language skills and deep country knowledge—in his case, China—to ensure they can exploit open sources.²

that the vast amount of publicly available and often most useful data remains print, broadcast, and radio. He speculated that this publicly available information (PAI) is often taken for granted because OSE and its predecessor FBIS have provided it to the IC free of charge since 1941. He noted, however, that collection, processing, and analysis of this PAI require large resources.

Resources

There was general agreement that the IC needs to devote more resources to OSINT, whether to acquire, process, and share open-source material or to develop AI and other tools to extract insights from it. Wood commented that OSINT will not be the INT of first resort unless it is resourced that way. Barrett described the 2010 to 2020 period as a "lost decade" from a budget perspective

as fewer IC components associated their activities with OSINT even amidst the rapid growth and value of commercial information. Nixon added that budgets devoted to OSINT have actually been declining even amidst the information explosion. Both Barrett and Nixon acknowledged that there may be other spending on open source that is captured in budgets as something else—e.g., publication or data procurement.

There was less consensus about how much more the IC needs to invest in OSINT. The varied approaches suggest large differences in financial and human resources. Several participants argued that producing OSINT is inherently less expensive than clandestine human and technical collection and that their recommended approaches would make it even more efficient.

Gordy argued that privatization would provide large cost savings. Companies operating at the unclassified level have far lower personnel and security costs than IC components and could rapidly surge to provide tailored OSINT in response to US government needs, which would reduce fixed costs of maintaining large programs covering topics or countries “just in case.” Wood’s consortium concept incorporates some of these features and also offers the potential that participating firms and organizations would provide some OSINT to the IC free of charge. Usher’s version of an OSA might offer some of the same savings, given that it would operate largely at the unclassified level and have a mainly unclassified staff. Several participants argued that the IC could cut the costs of acquiring CAI by centralizing procurement.

Other participants who have experience in acquiring open-source data were skeptical that major gains in OSINT could be made without large increases in

spending, particularly on CAI. Nixon and Ahlskog noted that they already cannot afford all the CAI that IC components want to exploit and that previous efforts to drive down costs by centralizing procurement have had little success. Privatization also might cost more as the IC would be paying for PAI it now collects on its own. That said, they believe significant increases in greater spending on OSINT would be worthwhile because it provides more bang for the buck than other INTs. Reducing spending on other INTs to increase spending on OSINT would improve the IC’s ability to meet customers’ intelligence requirements.

There was little discussion about human resources, but the varying approaches might drive sharply different requirements—some might even lead to IC cuts. Reinforcing the current IC approach implies increasing the number of OSINT specialists. Similarly, Usher suggests an Open Source Agency would need 2,000–3,000 people; some would be transferred from CIA and DIA. By contrast, the Privatization approach raises the potential of sharp cuts in OSE, OSIC, and other IC components.

Authorities

There was a strong consensus that OSINT practitioners need more authority to compete with other INTs in resource allocation and other decisions, such as

balancing openness and security. All speakers called for a clear, strong OSINT leader—“a champion” or “the person” overseeing OSINT. They saw a need for this champion to advocate for OSINT across the IC, Congress, and the public.

Speakers said that the DCIA, as functional manager of OSINT, has too many other responsibilities to be the champion. Harding argued that symbols and rank matter in Washington and that this was more important than formal authority over IC budgets and programs. She suggested elevating OSE to the directorate level—making its chief a direct report to the DCIA and a peer of the chiefs of its operational and analytic components. An alternative would be to create a presidentially appointed, Senate-confirmed position in ODNI. In contrast, Gordy argued that an OSINT leader should have the formal authority to move resources. Usher agreed; he would centralize most funding and people in OSA and give its director authority to approve open-source activities by other IC components.

Culture

The discussion on authority reflected another area of consensus: all participants emphasized that major change in IC culture would be needed to take advantage of OSINT’s potential. Although the IC OSINT Strategy calls for it to be “the INT of first resort”

participants noted a pervasive emphasis across the IC on clandestine collection of all sorts. One argued that most all-source analysts gravitate to HUMINT and SIGINT and lack the language skills and substantive expertise to fully exploit open source. This is true even though for decades open sources have often been the dominant source of intelligence. Some participants see a “not invented here” attitude to OSINT as well as a bureaucratic impulse among components to contribute secretly acquired intelligence even when it is not needed.

One participant commented that OSINT officers are treated as “second-class citizens.” Their contributions are belittled as “clipping newspapers,” rather than seen as making sense of huge datasets. Elsewhere, officers have noted that the needs of other INTs are given priority; for example, in engagement with outside experts and private firms. Another participant commented that the bias can be subtle. He said that templates to source PDBs and other products, for example, encourage listing only a few sources and favor those that have been “serialized”—formally disseminated. Not surprisingly, analysts and editors typically list a few secret, serialized sources rather than a large number of OSINT sources, many of which are not formally disseminated. Nixon noted that OSE is increasing its dissemination of serialized products. Other participants said

that the OSINT enterprise lacks a compelling product line for decisionmakers.

Harding suggested some ways to change the culture, most of which could be done under any of the four approaches. These including having the “champion” regularly tout OSINT successes that would resonate with Congress and the public. Successes could range from breaking new substantive ground to saving money or expanding public-private partnerships. She also suggested that deploying “rock star” OSINT officers to other components would increase IC officers’ respect for the discipline, while expanding work-from-home options for OSINT employees could attract high-quality experts. Usher suggested that a major advantage of creating an OSA would be elevating respect for its officers; if nothing else, its director would be a peer of other agencies’ directors.

Participants discussed the potential that giving IC components “budgets” to buy OSINT would promote its use across the IC. Reflecting their view that IC officers devalue OSINT, most were skeptical that this would work. They worried that components would find ways to divert OSINT funds to other purposes and noted that fee-for-service models have a poor track record of success in the IC. This view also suggests that broad cultural change would be particularly critical to the success

of the Privatization and Surgical approaches if these involved a large shift of resources from current IC OSINT components. In these cases, funding would depend on other components’ views of the value of OSINT.

The speakers and many participants argued that there is less need for cultural change among consumers of intelligence—policy-makers, military and law enforcement officials, and others. They live for the most part in the open-source world and want intelligence they can use and share widely. Participants commented that consumers’ key concerns are accuracy and timeliness.

A few participants were more skeptical, citing consumer comments that suggest what they most value from the IC is clandestine human and technical reporting—the “good stuff,” as President George W. Bush once put it. Nixon commented that there is a tendency for new administrations and officials to want the “good stuff” early in their tenures, but that this fades as they gain experience. They learn to recognize when they do and do not need precise or highly reliable intelligence that can be gathered only clandestinely.

Tradecraft

Most of the speakers and several other participants stressed that the IC needs to expand its cadre of experts with strong

OSINT tradecraft skills. Harding and Usher, echoed by Nixon and Ahlskog, argued that this cadre should be concentrated in components that are dedicated to OSINT. The cadre would also have the responsibility to set standards for OSINT tradecraft, to teach at least the basics to other IC officers—“teach them to fish”—and to team with them on joint projects. One participant commented that this would help deal with the numerous “OSINT amateurs” around the IC. Gordy and Wood also stressed the importance of tradecraft, although it was not clear whether the number of IC OSINT specialists would increase or decrease under the Privatization and Surgical approaches.

Discussion on tradecraft concentrated on two areas: discovering, processing, and sharing data; and, validating information. Participants commented that much of the huge volume of digital data needs to be put into a form that is exploitable before any intelligence value can be gained. Harding and Usher cited the need to structure or curate data. Ahlskog commented that DIA put its OSINT unit in its technical-data-collection directorate because the officers’ skills fit better there than in an analytic unit and doing so helps minimize analytic biases. On validation, speakers and other participants saw spotting disinformation or misinformation was one challenge; another is understanding the sources to be able to judge their access and credibility.

Nixon noted that a key element of OSINT tradecraft is learning techniques to discover useful data, particularly data that may not be readily discoverable.

Gordy said Janes and other private firms have developed rigorous OSINT tradecraft that parallels many IC best-practices in scoping an intelligence problem, determining how to solve it from available and potential sources, validating and fusing reporting from different sources, and preparing a final report. Gordy sees this tradecraft as key to giving governments confidence in outsourcing OSINT. He noted that Janes has developed criteria for rating the access and credibility of some 700 people who provide it information, including keeping a track record of their reliability. Gordy, Wood, and other participants also commented on the skill firms, individuals, and organizations like Bellingcat have developed to extract intelligence from digital sources.

None of the speakers or other participants discussed overlap between OSINT tradecraft and data science or other “tradecrafts,” such as targeting, GEOINT, or all-source analysis. Clarifying the core elements of OSINT tradecraft might help change IC culture by highlighting its distinct value. (In his article for *Studies* in June 2024, Chris Rasmussen argues for a professionalization of OSINT. He addresses some aspects of

tradecraft, although he does not use the term.)

Security and Counterintelligence

Security and counterintelligence came up as concerns throughout the discussion. Participants expressed differing levels of concern about the risks, whether to the ability to collect OSINT or to the safety of people who collect it. These views had implications for which approach they favored. In general, the greater the perceived risks, the more likely participants were to favor retaining robust IC open-source components with cleared staff.

Some speakers argued that the overwhelming amount of CAI and PAI already has made it almost impossible for any government, organization, or firm to hide all but the most sensitive secrets, greatly reducing the need for clandestine collection. Technical barriers like China’s “Great Firewall” present challenges but there are myriad avenues to get needed intelligence, mitigating the risk of discovery and of damage if one is lost. Other participants were more skeptical of the availability of digital information, particularly on topics of priority intelligence interest, and of the ability of non-government actors to get more sensitive data without tipping the owner. Jonah Victor’s article in this edition of *Studies* on diminishing access to information in China suggests that

adversaries may increasingly avoid exposing sensitive information digitally, forcing more OSINT into a gray area more closely resembling clandestine collection.

Gordy expressed confidence in the personal security of people who provide information to Janes and other firms around the world. Several other participants suggested he was underrating the individual risks, including blowback on the US government if private citizens were arrested for undertaking what would seem to other countries like outsourced espionage. The risks extend beyond HUMINT; private cyber efforts could invite retaliatory cyberattacks or even physical attacks on hackers, for example. Targets also might respond by taking security measures that would cut off access to other intelligence streams.

All participants saw the hand-off between the unclassified and classified domains as a manageable challenge. With the exception of proponents of reinforcing the IC's Federated Approach, they all favored having OSINT practitioners "live" as much as possible in the unclassified world, to include not having security clearances. They acknowledged that securely passing intelligence requirements from the classified to the unclassified domains would be a challenge but thought this should not be overstated; one participant quipped that it would take about 10 minutes for a person to guess the

topics on the National Intelligence Priorities Framework. OSINT collectors could take measures to obscure priorities, although doing so would increase cost.

CI and security challenges would be most muted in the Federated Approach. Current OSINT officers are fully cleared. They can work with other IC officers on the handoff challenges and are well positioned to deconflict with other IC components when OSINT and clandestine activities might intersect.

Privacy and Civil Liberties

All participants agreed that it is critical for policymakers to decide where to set the line in the inherent conflict between protecting US persons' privacy rights and fully exploiting digital information. This is a decision for the White House and Congress. It goes beyond the debate over Section 702 authorities in the Foreign Intelligence Surveillance Act, which will be up for renewal in two years, to the implications for privacy of AI, the internet of things, and other advances in technology. Where policymakers draw the line will have implications for which approach to OSINT they want the IC to pursue.

Wood argued that the IC needs to have access to CAI that contains US persons data to ensure the United States has the intelligence it needs to compete with

China and to tackle challenges that cross borders, such as counterintelligence, human and narcotics trafficking, and technology. US firms—and even US adversaries—have access to this data, which is critical to drawing insights from the massive amounts of digital information that is available. She added that major US firms want to help tackle the challenges and suggested they might help find ways to ease privacy concerns. Even if they cannot, she said the need is important enough to amend the 1947 National Security Act. She suggested that this might include creation of a domestic intelligence agency, in part to address concerns about law enforcement access to intelligence on US persons.

Harding argued that US persons' privacy is a "third rail" with Congress that the IC should not touch. This implies that the IC would not delve as deeply into some topics and issues as Wood suggests it needs to cover. Barrett commented that he tended to agree with Harding. He suggested that a Consortium might offer ways to fully exploit OSINT sources while protecting privacy. Gordy noted that Janes follows EU privacy law, which restricts its ability to prepare intelligence on individual people. This suggests some limits on the ability of private firms to satisfy intelligence requirements as well as the potential that privacy concerns in other countries will lead to further restrictions, including on the availability of OSINT.

Looking Beyond OSINT

Resource Tradeoffs

As noted, Roundtable participants all agreed that more resources need to be devoted to OSINT and that it could more efficiently satisfy many intelligence requirements than other INTs. They also agreed that a top-line increase in the IC's budget is improbable. This means that money and perhaps people would need to be shifted from other INTs to successfully pursue any of the OSINT approaches. However, beyond a quip that perhaps the IC could forego building another satellite, participants did not have proposals on what resources to shift.

This was not surprising given that making tradeoffs among programs and INTs is a longstanding IC challenge. There are minimal mechanisms beyond the budget process and common sense to divvy up responsibility and resources among INTs and the IC components that pursue them. There is no way to determine how many resources of whatever type should be devoted to each topic other than its prioritization in the NIPF or similar guidance documents. And, there is no way to measure the inherent "value for money" policymakers place on satisfying each requirement.

OSINT's overlap with all the other INTs and its ability to provide insights on all NIPF topics from the lowest priority global coverage issue to the highest priority hard target suggest it may be particularly difficult to specify tradeoffs. Success implementing the IC OSINT strategy or a well-constructed Consortium pilot might eventually point to tradeoffs some topics. However, unless mechanisms to implement tradeoffs are created, it is more likely that other components would continue to cover the same topics like little kids playing soccer. At most, those components would seek to shift their resources to close gaps on other topics rather than ceding them to OSINT components.

Role and Structure of the IC

Participants' comments on the volume of PAI/CAI and the private sector's ability to exploit it suggest that resource tradeoffs may include consideration of fundamental change in the IC. The IC that has grown up since World War II is largely structured and resourced to uncover secrets clandestinely through a range of human and technical means. These were developed largely because there were no open sources or other ways to uncover the secrets. The information explosion at least raises the potential that much of what the IC does is outmoded or soon will be.

None of the speakers or other participants suggested the IC be abolished or revert to its pre-World War II scope, but several comments suggested the IC risks consumers seeing it as not providing "value for money." If so, its future might be in question. Usher commented, for example, that it would be very bad for the IC if Congress could meet its need for intelligence on Gaza by turning to Janes, while Gordy noted his firm already sells intelligence directly to several parts of the Joint Staff, bypassing the J-2.

Gordy came closest to offering a way forward in his argument that the IC should focus on niches where exquisite clandestine human and technical collection is needed while relying on the private sector to provide OSINT on everything else. He did not suggest any niches or other changes in IC structure and resources. These could vary based on such factors as the overall size of the niches, the resources needed to provide intelligence on them, and whether consumers saw getting the intelligence as worth the investment.

Peak OSINT?

A final area that bears more research and discussion is whether OSINT will continue to explode in quantity and availability. All four approaches take as a given that the quantity of information will continue to grow over the next

two decades and that the rate of expansion will even accelerate as AI tools mature. They also agree with private sector experts that it will be available to exploit as PAI or CAI.^a Victor's article should raise some doubts, however, on both quantity and availability. China is not the only country that is improving digital security, not least by exposing less sensitive information in the

first place. In July 2024, for example, Russia banned use of personal cell-phones by its military on the frontlines with Ukraine in response to press reports that indicated metadata was being used to track battles.^b

The balance in the race between cyber defense and offense may shift, and the ability of private firms and

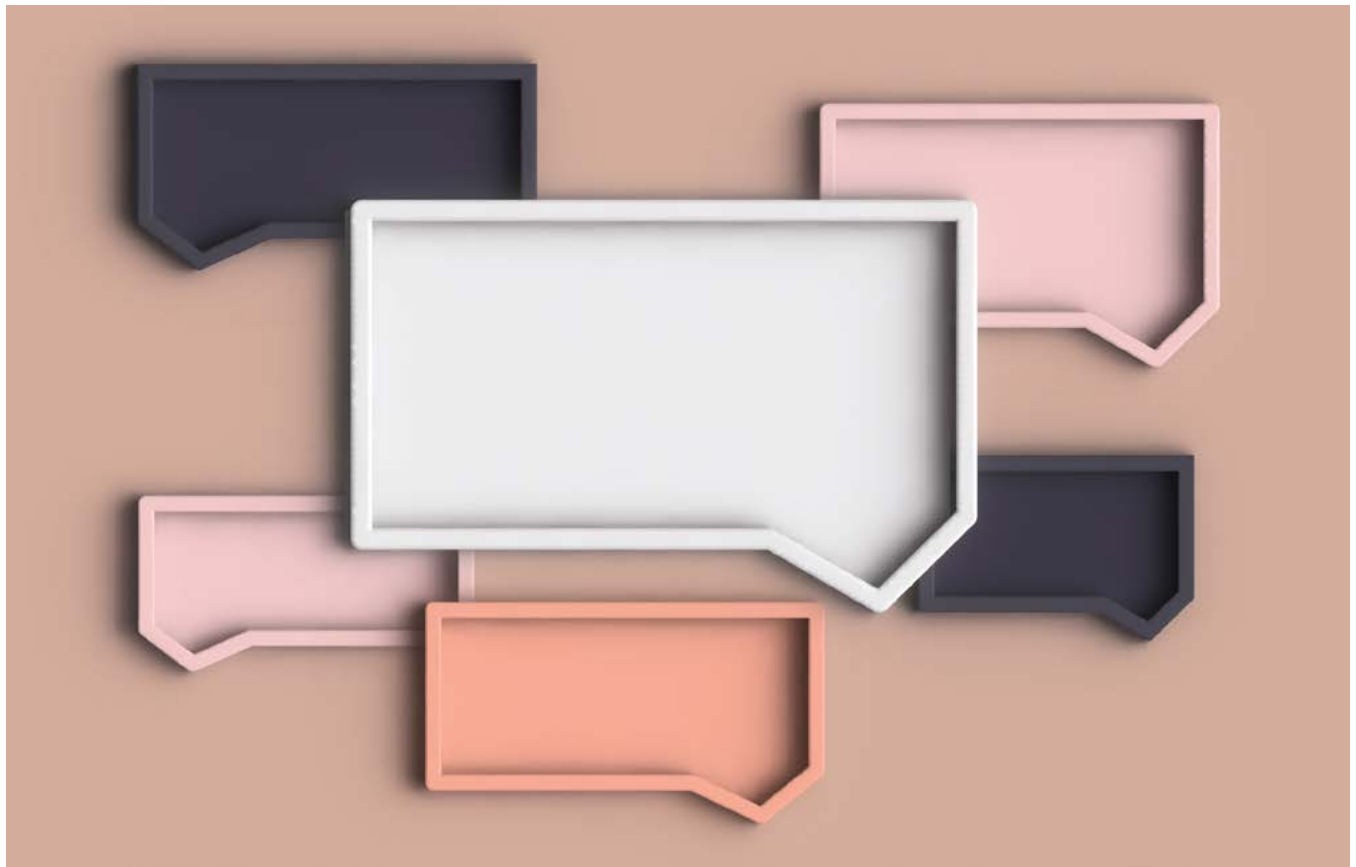
individuals to ferret out useful intelligence may decline. The impact of privacy safeguards is another uncertainty. Legal safeguards and encryption are likely to grow in the West and perhaps spread more broadly. If safeguards expand or enough people take actions to secure their privacy, the availability and utility for intelligence of at least some types of digital data might decline. ■

a. See Emily Harding, "Move Over JARVIS, Meet OSCAR," January 19, 2022. <https://www.csis.org/analysis/move-over-jarvis-meet-oscar>.

b. Veronika Melkozerova, "Russia Cracks Down on Personal Cell Phones on the Front Line," *Politico*, July 24, 2024. <https://www.politico.eu/article/russian-duma-adopts-law-on-punishment-for-soldiers-using-gadgets-on-the-frontline/>.

Endnotes

1. Link to Strategy. <https://ddi.cia/odni-and-cia-release-the-intelligence-community-osintstrategy-for-2024-2026/>
2. J.J. Bagnall, "The Exploitation of Russian Scientific Literature for Intelligence Purposes," Vol. 2, No. 3 (1958), declassified September 18, 1995; Davis W. Moore, Jr., "Open Sources on Soviet Military Affairs," Vol. 7, No. 2 (1963), declassified September 18, 1995; Herman L. Croom, "The Exploitation of Foreign Open Sources," Vol. 13, No. 3 (1969), declassified August 25, 1997; Gail Solin, "The Art of China Watching," Vol. 19, No. 1 (1975), declassified July 2, 1996; David Gries, "Intelligence in the 1990s," Vol. 35, No. 1 (1991); David Overton, "The DI Ten Years After Reorganization," Vol. 36, No. 5 (1992); Mark Lowenthal, "The State of the Art, the Artless State," Vol. 45, No. 2 (2001); John Gannon, "The Strategic Use of Open-Source Information," Vol. 45, No. 3 (2001); Martin Petersen, "The Challenge for the Political Analyst," Vol. 47, No. 1 (2003); Stephen Mercado, "Sailing the Sea of OSINT in the Information Age," Vol. 48, No. 3 (2004); Chris Rasmussen, "How the Intelligence Community Has Held Back Open-Source Intelligence, and How it Needs to Change," Vol. 68, No. 2 (2024).



Debating Open Source

A Practitioner's Perspective

Amelia Favere

The author is an open-source expert and member of the Lessons Learned Program in CIA's Center for the Study of Intelligence.

Introduction

The US government has collected, processed, and analyzed open-source intelligence (OSINT) longer than the CIA has existed, and this venerable art has seen an explosion of attention in recent years.¹ Prominent voices such as former Principal Deputy Director of National Intelligence Sue Gordon and former National Geospatial-Intelligence Agency (NGA) Director Robert Cardillo have advocated publicly for more investment in technologies that enable OSINT.^{2 3} Several member organizations of the Intelligence Community have set up efforts to gather and process open-source information, including the US Army, State Department, and NGA.^{4 5 6 7} Most recently, the Office of the Director of National Intelligence released an OSINT strategy to establish IC-wide governance.

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

These official efforts parallel public calls from think tanks, academics, and the media for more robust and sophisticated approaches to OSINT. Those calling for change in the US government's approach generally agree on three points:

- Open source is critical to intelligence work;

- Massive amounts of information are available; and
- Burgeoning technologies like artificial intelligence are required to triage and parse data.

The greater attention to OSINT in recent years comes in part from greater public awareness of the issue, as advocates for OSINT point to media reporting on China's

investment in its own open-source intelligence approach and to the utility of open-source research in exposing Russian military actions in Ukraine. Publicity of the work by independent investigative organizations like Bellingcat have popularized OSINT tradecraft and further democratized its use among a growing number of citizen journalists.⁸

Looking to OSINT's Future

Visions of OSINT's future within the IC articulated in the public sphere tend to fall into three camps:

- outsourcing open-source collection and analysis;
- increasing the resources of existing open source intelligence efforts throughout the IC; and
- creating a new agency dedicated to OSINT.

Outsource OSINT

Proponents of outsourcing OSINT argue the private sector can do the job better. Taking for granted that open-source environment is constantly and rapidly evolving, this camp argues that the IC is less adaptable than private industry and less adept at recognizing trends on the horizon. As Jake Harrington, former intelligence fellow at the Center for

Strategic and International Studies (CSIS), articulated the problem: "Intelligence success in this environment requires imagination, flexibility, resilience, and risk tolerance. These are not characteristics of today's IC."⁹ Advocates argue that private industry can offer more robust and agile resources to focus on open source technology while often controlling the infrastructure and intellectual property underlying open-source architecture.¹⁰

Some proponents of outsourcing point out that the IC is unable to devote attention to OSINT because of competing priorities baked into its organizations. For example, former CIA officer Jeffrey Stoff argues the US government is ill positioned to conduct open-source research because it would take away from other missions"

[N]o government agency or program can overcome their structural limitations without a

radical transformation of their missions, priorities, and resources. That would be a difficult task and could create zero-sum game effects; other missions would need to be descoped that could have unintended or dangerous consequences.¹¹

He argues that because Title 50 agencies are limited in the type of data that can be collected regarding US persons, the IC is unable to legally collect large portions of commercially available information (CAI), hamstringing the IC's ability to replicate what private industry can do. He and other former CIA officers have proposed an open-source consortium model, essentially a government-funded, public-private partnership that provides OSINT research, tools, sources, and data technology for the IC.^{12 13}

Embrace Open Source

Advocates for this second approach argue that OSINT is too essential to the IC's mission to take outside of government and that the IC needs to evolve in its structure, culture, and workflows to integrate OSINT more fully into its tradecraft. This camp tends to focus on the IC's demonstrated capability in open-source collection; believes that the IC can evolve tradecraft, technology, and bureaucratic structures; and asserts that OSINT expertise needs to be integrated within the IC alongside the other intelligence sources (or INTs) to be effective.

Authors involved in a CSIS Technology and Intelligence Task Force in 2021—initially chaired by now DNI Avril Haines—fleshed out recommendations for this approach.¹⁴ Advice from these authors include tactical solutions, such as empowering indigenous innovators to find small-scale technological solutions, and solutions at scale, such as funding an IC-wide OSINT collection and processing system fueled by artificial intelligence/machine learning (AI/ML).^{15 16}

The CSIS authors note that existing IC culture—as in all large organizations—is resistant to adopting new technologies and the workflow changes that come with them. Brian Katz writes:

*The challenge to U.S. intelligence, however, will come not only from U.S. adversaries but from the IC itself, as organizational, bureaucratic, and technical hurdles slow technological adoption.*¹⁷

Emily Harding asserts that the likely unwillingness of all-source analysts' to adopt technology enabled by AI/ML for OSINT research is a critical barrier for change.¹⁸

Research by RAND, long a keen observer of US government functions, suggests ways to combat this cultural resistance to open source information. In addition to commonsense advice to invest in better tools and tradecraft to support the OSINT mission,¹⁹ RAND researchers identified one key lever to bring about the systemic changes needed to make the IC more effective in the open-source realm: leadership messaging:

*To effect the cultural change, the IC leadership must issue multiple messages to the IC workforce, develop new tradecraft, and train a new generation of intelligence professionals on how to meet the warning challenge.*²⁰

There is also a perceived analytic bias against open sources in all-source work. One RAND study argued that "IC organizations often treat both PAI [publicly available information] and OSINT

as another stovepipe, similar to other INTs, rather than a resource for foundational use in all analytic products."²¹ These authors argue that addressing the cultural barriers within the IC to working with open sources and large datasets is critical to user adoption.

Create an OSINT Agency

The argument for an independent open-source agency refutes the current IC federated approach to OSINT collection, arguing that OSINT is a complex system that needs a dedicated structure. Former CIA officers Peter Mattis and Rodney Faraon argue that the

volume and variety of open and commercial source materials, urgency of the geopolitical rivalry, and continued development of tools to exploit the data all necessitate a systematic effort to harness open and commercial source to support decisionmaking.^{22 a}

Several advocates for an open-source agency argue that OSINT cannot thrive in an organization dedicated to secrets. Stanford professor Amy Zegart and former Acting CIA Director Michael Morell, in recommending an independent open source agency, assert:

Currently, [OSINT] collection runs through the CIA's Open Source Enterprise, but this setup is akin to keeping the air force

a. See in the issue retired CIA officer William Usher's case for a separate OSINT agency, "The Case for Creating an Open-Source Intelligence Agency," beginning on page 23.

What Do We Mean When We Say “Open Source”?

While the concepts comprising “open-source intelligence” have been well defined for some time—notably publicly available information (PAI) and commercially available information (CAI)—the lack of familiarity with these terms in the general IC population prevents deep conversations. As one open-source advocate explained: “It’s almost like a bureaucratic maneuver to slow down whatever conversation we’re having. And I’ve been in tens of conversations, meetings, inside the government, inside industry, around industry. And we’re starting to make progress. We’re talking about tough issues, talking about the value of open source. And it almost never fails, someone sort of leans back in their chair, sort of stretches their decades of experience comfortably in government, and they ask, ‘Well, what does this mean? What is open source? What is PAI?’ And then we end up admiring the problem and progress halts.”²⁶ To coin a phrase, the low level of “open-source acumen” within IC agencies is dragging down the IC’s ability to move forward in properly resourcing and using OSINT.

*within the army, hobbling a new mission by putting it inside a bureaucracy that naturally favors other priorities. Secrets still reign supreme in the CIA, relegating open-source information to second-class status. Open-source intelligence will never get the focus and funding it requires as long as it sits inside the CIA or any other existing agency.*²³

Similarly, former military intelligence officers Mark Quantock, David Dillow, and McDaniel Wicker recommend a new IC agency to truly professionalize OSINT as a discipline and to move away from what they call an ad hoc approach in IC and Defense Department components, arguing, “Credibility as a discipline comes with expertly trained and educated professionals.”²⁴

NGA officer and OSINT practitioner Chris Rasmussen, who spearheaded NGA’s unclassified reporting effort known as Tearline, goes further by advocating for an independent OSINT agency outside the IC.^a This separation is necessary, in his view, because the IC will always prioritize classified programs:

*The classified core is becoming increasingly irrelevant but sunken cost fallacies and cultural inertia overstate its importance internally. The only way to break free of this budget subordination and classified-first resource mentality is independence or removing protecting secrets as a condition of employment. An independent agency’s entire top-line budget would be OSINT or unclassified operations which would reduce anchoring or subordinating OSINT under classified or other line items.*²⁵

What’s Holding Us Back?

The recent public literature on OSINT provides commonsense solutions based on sound reasoning. Unfortunately, most of these authors ignore the issues that open-source practitioners have wrestled with in recent memory. What I did not see expressed so prominently in the public debate are the persistent questions that have driven conflict

and change within the IC OSINT community, at least as I experienced it for 15 years at the Open Source Enterprise and its predecessor organization, the Open Source Center.

In recent years, we asked questions such as: What level of curation does open-source data need to be of use to our IC colleagues? What

formats and delivery systems fit best into our customers’ workflows so they have OSINT just when they need it? How can we leverage subject-matter expertise to identify collection gaps at scale? And the big question: should OSINT tradecraft be centered on data analysis or should it draw on media, cultural, linguistic, and historical expertise?

a. See Chris Rasmussen, “How the Intelligence Community Has Held Back Open-Source Intelligence, and How It Needs to Change,” *Studies in Intelligence*, Vol. 68, No. 3 (June 2024).



Lewis Carroll, *Through the Looking Glass, and what Alice found there*, Macmillan & Co, 1872 © Macmillan & Co Ltd. © thanks to Macmillan Children's Books

These fiercely debated questions remain absent from the public discourse, which is largely driven by nonpractitioners and is focused more on technological or high-level organizational solutions. Few prominent advocates of changes in open-source of one variety or another have served as OSINT officers, rendering opaque the realities of roadblocks to innovation within the discipline to those who have not walked in our shoes.

And it is this opacity of open-source intelligence to nonpractitioners that is the key obstacle to OSINT's evolution within the IC. An issue with confusing terminology, which has multiple seniors nominally in charge of it, and which lacks a clearly defined mission does not inspire bold action, particularly

if that action requires significant investment of money and people in a time of scarcity. The dazzle of AI/ML technologies—genuinely promising approaches that few genuinely understand—means that AI-enabled OSINT is both the proverbial shiny object that attracts attention and is worthy of healthy skepticism. The IC functions well when the need for mission and its solution are clear and obvious to the majority, and the failure of senior leadership across the IC to resolve the open source intelligence problem so far is a healthy symptom of a functioning system. No clear solution exists and the mission need has not been articulated clearly enough for senior leaders, middle management, or line officers across the system to support the disruption

and expense needed for meaningful change.

It is for this reason that the question at the heart of this debate is the most difficult to resolve: How can IC leadership justify taking decisive action on open source intelligence?

The belief that something about OSINT is *probably* useful seems to be present in the current zeitgeist. (While skeptics of open source certainly exist, they are not a very vocal minority. I could find only a couple of authors disparaging open source for intelligence work altogether, mostly those pointing out how enemies can use open-source information as part of denial and deception techniques.) But that “something”

remains difficult to articulate in all mission spaces.

Speaking as one of those weary open-source evangelists who for years has failed to explain its critical relevance to audiences within the IC, I can only make this appeal: that today's OSINT leaders in the IC take forceful action to press for a solution rather than wait for mainstream understanding that will never come without top-down guidance.

"Now, here, you see, it takes all the running you can do, to keep in the same place," observed the Red Queen in Lewis Carroll's *Through the Looking-Glass*. First applied to evolutionary theory by Leigh Van Valen, the Red Queen hypothesis holds that organisms must continuously evolve to keep up with their adversaries, who are also evolving. OSINT has been held back by conflicting visions, diffident leadership, and disparate initiatives.

At this point, taking half measures is unlikely to move the needle. Our adversaries are taking bolder, more aggressive approaches. As this review of the literature reveals, the only thing everyone agrees on is that we must again become a world-class player in the open-source realm to maintain our edge in intelligence—whatever path the IC chooses. ■

Endnotes

1. The Franklin D. Roosevelt administration established the Foreign Broadcast Monitoring Service on February 26, 1941, modeled after BBC Monitoring. "FBIS Against the Axis, 1941–1945," CIA.gov, accessed July 22, 2024. <https://www.cia.gov/resources/csi/static/fbis-against-the-axis.pdf>.
2. "Event Recap: 'The Present and Future of Intelligence with Susan M. Gordon' – Michael V. Hayden Center for Intelligence, Policy, and International Security," February 14, 2020. <https://haydencenter.gmu.edu/2020/02/14/future-and-present-in-intelligence-susan-m-gordon/>. Theresa Hitchens, "IC Must Embrace Public Data to Use AI Effectively: Sue Gordon," *Breaking Defense*, September 25, 2019. <https://breakingdefense.com/2019/09/ic-must-embrace-public-data-to-use-ai-effectively-sue-gordon/>.
3. Warren P. Strobel, "Rise of Open-Source Intelligence Tests U.S. Spies," *Wall Street Journal*, December 11, 2022. <https://www.wsj.com/articles/rise-of-open-source-intelligence-tests-u-s-spies-11670710806>. "Role of imagery in support of OSINT – Part One," *The World Of Intelligence*, Janes, July 22, 2024. <https://podcast.janes.com/public/68/The-World-of-Intelligence-50487d09/a14fad3d>.
4. Justin Doubleday, "Army to treat OSINT as 'intelligence discipline of first resort' under new strategy," *Federal News Network*, September 11, 2023. <https://federalnewsnetwork.com/inside-ic/2023/09/army-to-treat-osint-as-intelligence-discipline-of-first-resort-under-new-strategy/>.
5. "Open Source Intelligence Strategy," Bureau of Intelligence and Research, US Department of State, accessed July 22, 2024. <https://www.state.gov/open-source-intelligence-strategy/>.
6. "About the Tearline Project," Tearline.mil, accessed July 22, 2024. <https://www.tearline.mil/about-tearline>.
7. "THE IC OSINT STRATEGY 2024–2026," Office of the Director of National Intelligence, March 8, 2024. <https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2024/3785-the-ic-osint-strategy-2024-2026>.
8. See J.E. Leonardson review of *We Are Bellingcat: An Intelligence Agency for the People* in *Studies in Intelligence* 65, no. 1 (March 2021)
9. Jake Harrington, "Thinking Small: How the Intelligence Community Can Catalyze Digital Transformation," CSIS, May 24, 2021. <https://www.csis.org/analysis/thinking-small-how-intelligence-community-can-catalyze-digital-transformation>.
10. Michael Allen, "Does best intel come from public or private sector?," *Federal Times*, September 12, 2016. <https://www.federaltimes.com/2016/09/12/does-best-intel-come-from-public-or-private-sector/>.
11. Jeffrey Stoff, "Reassessing Threats to US Innovation Posed by China and Implications for Safeguarding Future Supply Chains" Testimony Before the U.S.-China Economic and Security Review Commission, Hearing on 'U.S.-China Competition in Global Supply Chains,'" June 9, 2022. https://www.uscc.gov/sites/default/files/2022-06/Jeff_Stoff_Testimony.pdf.
12. Chip Usher and Kristen Wood, "The Intelligence Community 'Can' Tackle Open-Source Data in a Hyper-Connected World," *The Cipher Brief*, December 23, 2023.

13. Jeffrey Stoff, "Reassessing Threats to US Innovation Posed by China and Implications for Safeguarding Future Supply Chains" Testimony Before the U.S.- China Economic and Security Review Commission, Hearing on "U.S.-China Competition in Global Supply Chains," June 9, 2022. https://www.uscc.gov/sites/default/files/2022-06/Jeff_Stoff_Testimony.pdf.
14. CSIS Technology and Intelligence Task Force, CSIS, accessed July 22, 2022. <https://www.csis.org/programs/international-security-program/csis-technology-and-intelligence-task-force>.
15. Jay Harrington, "Thinking Small: How the Intelligence Community Can Catalyze Digital Transformation, CSIS, May 24, 2021. <https://www.csis.org/analysis/thinking-small-how-intelligence-community-can-catalyze-digital-transformation>.
16. Emily Harding, "Move Over JARVIS, Meet OSCAR: Open-Source, Cloud-Based, AI-Enabled Reporting for the Intelligence Community," CSIS, January 2022. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/220118_Harding_MoveOverJARVIS_MeetOSCAR.pdf?OhpTTFfEInMGwk3Y78lUTyS.2ZueJWMJ.
17. Brian Katz, "Maintaining the Intelligence Edge: Reimagining and Reinventing Intelligence through Innovation," CSIS, January 13, 2021. <https://www.csis.org/analysis/maintaining-intelligence-edge-reimagining-and-reinventing-intelligence-through-innovation>.
18. Harding, "Move Over JARVIS, Meet OSCAR."
19. Heather J. Williams and Ilana Blum, *Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise*, RAND Corporation (2018). https://www.rand.org/pubs/research_reports/RR1964.html.
20. Cortney Weinbaum, John V. Parachini, Richard S. Girven, Michael H. Decker, and Richard C. Baffa, "Reconstituting Strategic Warning for the Digital Age," in *Perspectives and Opportunities in Intelligence for U.S. Leaders*, RAND Corporation (2018). <http://www.jstor.com/stable/resrep20002.7>.
21. Cortney Weinbaum, John V. Parachini, Richard S. Girven, Michael H. Decker, and Richard C. Baffa, "Better Utilizing Publicly Available Information," in *Perspectives and Opportunities in Intelligence for U.S. Leaders*, RAND Corporation (2018). <http://www.jstor.com/stable/resrep20002.7>
22. Rodney Faraon and Peter Mattis, "We need an open source intelligence center," *The Hill*, January 20, 2023. <https://thehill.com/opinion/national-security/3821075-we-need-an-open-source-intelligence-center/>.
23. Amy Zegart and Michael Morell, "Spies, Lies, and Algorithms: Why U.S. Intelligence Agencies Must Adapt or Fail," *Foreign Affairs* (May/June 2019). <https://www.foreignaffairs.com/united-states/spies-lies-and-algorithms>.
24. Mark Quantock, David Dillow, and McDaniel Wicker, "Promote Open Source to a Full Member of the Intelligence Community," *Defense One*, July 21, 2021. <https://www.defenseone.com/ideas/2021/07/promote-open-source-full-member-intelligence-community/183829/>.
25. Chris Rasmussen, "Avoiding the Secrecy Trap in Open Source Intelligence," *The Cipher Brief*, March 21, 2023. https://www.thecipherbrief.com/column_article/avoiding-the-secrecy-trap-in-open-source-intelligence.
26. Lindy Kyzer, "Are We Ready for an Open Source Revolution?" *ClearanceJobs*, February 1, 2023. <https://news.clearancejobs.com/2023/02/01/are-we-ready-for-an-open-source-revolution/>. ■



The Case for Creating an Open-Source Intelligence Agency

William Usher

The author is a retired CIA senior intelligence executive. He is now senior director for intelligence with the Special Competitive Studies Project.

Editor's Note: This article was adapted from a response to a request by the Center for the Study of Intelligence, which for the purposes of a panel discussion specified that the author make the case for creating a new OSINT agency. The recommendations do not necessarily reflect the views of the Special Competitive Studies Project or any element of the US government.

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

In 2001, John Gannon—former chair of the National Intelligence Council and deputy director for intelligence at CIA—wrote in this journal that open-source intelligence (OSINT) had become “indispensable to the production of authoritative analysis,” yet he noted that the Intelligence Community (IC) faced “an avalanche from both open-source and classified collection sources.” He went on to write that, “By itself, the IC simply cannot stay ahead of the technological curve and it knows it.”¹

Almost a quarter of a century later, the promise of OSINT to expand the scope and impact of IC work, as well as the critical challenge the IC faces when working with OSINT—volume, velocity, and veracity—have only become starker. A dynamic ecosystem of national security-focused companies, non-profits, and academia have developed specialized expertise and products by focusing on specific elements of the open-source space. This ecosystem covers nearly every topic of US government concern: human trafficking

networks, China’s attempts to steal intellectual property from US firms, trends in global public opinion, and nuclear proliferation, just to name a few. The private sector has found tools and strategies to absorb and analyze new data and to push out products at speed.²

In this arena, speed to insight—understanding the data faster than others do—is necessary for the United States to respond first to the risks and opportunities the data present. By 2025, it is projected that there will be more than 180 zettabytes of data available, up from 64.2 zettabytes in 2020.³ Many other countries, including our adversaries, are much less complacent than the IC in leveraging commercially available information (CAI) and/or publicly available information (PAI) for their advantage. For example, China’s People’s Liberation Army partners with at least five private OSINT providers to collect intelligence on a variety of relevant issues, including foreign military capabilities and deployments.⁴

The IC appears to recognize that integrating data and insights from this world at speed, scope, and volume will be increasingly necessary to continue to offer decision advantage to national security leaders. Solving the IC’s OSINT problem has been the subject of many data calls, conferences, academic papers, and op-eds over the past decade. After so many studies, however, an all-encompassing solution has not yet been implemented.

Some senior national security officials believe the way forward remains within the community’s current construct. The IC OSINT strategy recently promulgated by the Office of the Director of National Intelligence would appear to support this line of thinking.^a Others argue that the IC should get out of the OSINT business altogether, on the theory that the government can never match the speed and resources of the private sector and instead should position itself as a good customer of this data. Still others urge a bolder, more transformative approach.

What are We Trying to Solve?

Despite these efforts, the IC is in danger of falling behind on OSINT for a variety of reasons. Taken together, these obstacles are the OSINT problem that any new approach needs to solve,

and proposed solutions should be measured by how effectively and efficiently they address these challenges.

The amount of CAI/PAI is exploding, and the IC is not keeping pace to make proper use of it. Data is going undiscovered and underutilized. Relatively few IC officers know what data exists and they

a. The ODNI’s IC OSINT Strategy 2024–2026 defines OSINT as intelligence derived exclusively from publicly available information or commercially available information that addresses specific intelligence priorities, requirements, or gaps.



face myriad financial, security, and bureaucratic obstacles to obtaining it. Even if they succeed, IC officers often lack the data management and OSINT tradecraft skills or access to cutting-edge analytic tools to effectively utilize the data.

The IC has a poor understanding of the data it holds, how valuable it is, where it is kept, and how it is used. The new DNI OSINT strategy admirably calls attention to these shortcomings, but IC agencies are still not incentivized or required to share the CAI/PAI they have acquired and the Community often pays multiple times for access to the same data. This challenge is compounded by the extremely dynamic nature of the global data market, which

continues to grow exponentially in aggregate but with a great deal of volatility. The quality and availability of individual datasets are constantly shifting; commercial vendors rise and fall; datasets are created, then bought and removed from circulation, or priced expensively; academic-created datasets are often closely held so that the original creator can fully exploit it before making it more accessible; adversaries are closing off access to their domestic data ecosystems while they actively try to pollute our datasets.

While it is generally less expensive and risky for the IC to gather open-source data, the IC under invests in OSINT capabilities in favor of its more traditional

collection capabilities and methods. Existing OSINT entities, such as CIA's Open Source Enterprise, are subordinated within existing bureaucratic structures, impeding their ability to harness resources and exert influence.⁵

As a consequence, even as policymaker demands on the IC for intelligence insights continue to increase, the IC fails to deliver OSINT-derived assessments and other products at scale and at speed. Because the IC generally relies on its all-source analytic cadre to filter the assessments that reach its seniormost customers, and because most IC analysts remain relatively poor consumers and users of CAI/PAI, OSINT-derived insights often do not reach key

decisionmakers in a timely fashion, if at all. Moreover, the IC's small

cadre of dedicated OSINT analysts

are not well-integrated into all-source analytic teams.

The Case for a New Agency

To fully address the OSINT problem and maintain the IC's relevance and strategic edge with decisionmakers, the United States should create a new, 19th agency within the IC dedicated to the task. The new Open Source Agency (OSA) should be a standalone and independent member of the IC; its principal purpose would be to acquire, curate, develop, employ, and share CAI and PAI data sources for intelligence purposes.

At least initially, its function would be to deliver OSINT to other IC members (and, selectively, to foreign allies and partners, the private sector, and to the public) for them to analyze and make use of. Just as the National Reconnaissance Office builds and operates the US constellation of satellites but relies on the National Geospatial-Intelligence Agency and other IC agencies to analyze the data they collect, OSA would focus on accelerating and streamlining the acquisition of PAI/CAI that other agencies would make use of.⁶

OSA employees would “live” in the unclassified realm, spending much of their time in unclassified workspaces and on low-side unclassified systems, freeing them up to have regular access to and

collaboration with the private sector. As with In-Q-Tel, OSA would have designated secure spaces for classified work and secure communications with the rest of the IC to solicit intelligence requirements, disseminate information, and collaborate on classified projects to include targeting studies and collection planning.

OSA would be established using IC authorities and would become the IC's “functional manager” for OSINT in the same way the NSA director is the functional manager for SIGINT and the CIA director (DCIA) is the functional manager for HUMINT. OSA's director would report to the DNI, and it would be subject to congressional oversight by the HPSCI and SSCI and have its own budget appropriation.

OSA would apply and enforce ODNI-established standards for incorporation of CAI/PAI data with regards to privacy and security compliance, quality, IC-wide availability, and pricing. OSA would act as the contractor and go-between connecting data vendors with IC agencies, which would store and analyze the take.

OSA would ensure consistency, interoperability, and life-cycle

monitoring and accounting for CAI/PAI datasets that were acquired, and it would be responsive to NIPF priorities and IC requirements and tasking. It would offer commercial vendors a reliable one-stop point of entry to sell their data and analytic tools to the IC, making it easier and more efficient for the private sector to partner with the IC. Because it would look across IC equities and requirements, OSA should be able to exert its market power to drive down costs and increase interoperability and access to commercially-developed solutions.

OSINT Tradecraft

OSA's second principal mission would be to cultivate, develop, and teach OSINT tradecraft to elevate the acumen of the entire IC. OSA would have the IC's experts on the CAI/PAI information domain—including the commercial marketplace, vendors, datasets, and commercially sold analytics and platforms. OSA would become the data partners to the IC's cadre of all-source analysts and collectors, helping them incorporate OSINT to meet mission requirements.

OSA's capabilities would be available to all the other 18 IC agencies and would include acting

as the IC's trusted evaluator of commercial tools and platforms, and the focal point for CI and supply-chain vetting of commercial data vendors and their capabilities. OSA, for example, could maintain the IC's catalog of proven and vetted commercial datasets that IC agencies could tap into when mission requirements demand. Eventually, OSA could develop AI-driven API platforms to integrate valued datasets and simplify the process for IC agencies to tap into them.

It could also act as the IC arm for discovering, evaluating, and advertising open source-derived assessments by the private sector (commercial vendors, academics, or think tanks experts) of relevance to US national security priorities. It could publish a regular compendium of the best commercial OSINT tradecraft and tools (including data management, visualization, augmented and virtual reality, and storytelling) to educate other IC offices and promote their use.

As it matures, OSA should develop in-house analytic capabilities, focused on topics that most readily lend themselves to unclassified open sources, such as politics and foreign policy, transnational issues, economic trends, or technology assessments. At the direction of the president, ODNI, and DCIA, the Open Source Agency could further develop cloud-based unclassified online collaboration spaces

to enable broader IC analytic outreach with the private sector, state and local authorities, foreign intelligence liaison services, and the general public.⁷

While other options for solving the OSINT problem have their individual merits, creating a new dedicated agency offers the best, achievable, and sustainable path for success. It is the one solution that would give OSINT greater stature across the IC and better enable Congress and the White House to direct greater resources toward it. Because the new agency would not produce assessments, this approach would avoid creating duplicative and wasteful analytic capabilities and minimize the chances of debilitating bureaucratic infighting for analytic access to policymakers while OSA and its IC partners determine where its analytic capabilities are best deployed.

Maintaining the all-source analytic community's purview over the delivery of insights to policymakers also keeps the intelligence "conversation" with senior intelligence customers focused and vibrant. In this author's experience, customers rarely demand unclassified assessments and instead want the best analysis using whatever sources are available. Development missions would be made available IC-wide to enhance the work done by all-source analytic units.

Just as the NRO influenced the direction of commercial space

development to ensure US national security requirements were prioritized and addressed, so would OSA for OSINT. As the IC's OSINT functional manager, OSA would have the writ and budget to identify, acquire, and promote which CAI and PAI sources the IC should acquire. Organizing OSINT efforts under OSA would give the IC greater market power to generate supply of relevant CAI and spur innovation in the private sector. In the long run, it would be cheaper and more efficient to do this in-house.

As it gains experience and proves its worth, OSA would be positioned to drive OSINT resources and tradecraft forward, enlarging and accelerating OSINT's ability to close intelligence gaps and deliver strategic insight, thereby allowing for more efficient use of classified collection capabilities and reserving them for the truly hard targets that only they can penetrate. OSA would be an ideal sandbox for the IC to experiment with large-language models, other forms of generative artificial intelligence, and machine learning tools, applying them to deliver intelligence insights in new and innovative ways.

Oversight

The White House would need to request, and Congress would need to authorize and appropriate funds to establish a new agency. It probably would take considerable

time to hire and onboard staff and identify suitable physical space. One way to speed up the process would be to identify certain roles within OSA that would not require a security clearance, or a basic secret-level clearance. To be fully successful, OSA would need to be invested with requisite authorities over the application of OSINT and enjoy sufficient standing in the IC to deliver insight to customers.

Just as Executive Order 12333, the Foreign Intelligence Surveillance Act, and National Security Directive 42 authorize NSA to collect foreign signals intelligence and protect national

security systems, OSA would need strong executive authority to approve, modify, or disallow CAI/PAI acquisitions across the IC. Agencies would need to be incentivized (and, in turn, create incentives for their officers) to make better use of CAI/PAI data and to adopt OSA's recommended tradecraft.

As its analytic capabilities grew, OSA would need an online dissemination capability, along with representation on the President's Analytic Support Staff to feed into the PDB process and at the National Intelligence Board to

contribute to the production of national intelligence estimates.

OSA would need empowered, layered, and independent oversight mechanisms to ensure compliance with US law and established IC privacy protection practices. In line with other IC agencies, OSA's inspector general should be a presidential appointee confirmed by the Senate; the IG should report regularly to the White House and to Congress on OSA's performance and handling of PII compliance. Finally, the ODNI's Office of Civil Liberties, Privacy, and Transparency should conduct regular, independent reviews. ■

Endnotes

1. John Gannon, "The Strategic Use of Open-Source Information," *Studies in Intelligence* 45, No. 3 (September 2001).
2. See Jami Miscik, Peter Orszag, Theodore Bunzel, "Geopolitics in the C-Suite," *Foreign Affairs*, March 11, 2024.
3. Petroc Taylor, "Amount of Data Created, Consumed, and Stored 2010–2020, with Forecasts to 2025," *Statista*, November 16, 2023. <https://www.statista.com/statistics/871513/worldwide-data-created/>.
4. Zoe Haver, "Private Eyes: China's Embrace of Open-Source Military Intelligence," *Recorded Future*, June 1, 2023. <https://www.recordedfuture.com/research/private-eyes-chinas-embrace-open-source-military-intelligence>.
5. Cortney Weinbaum, Bradley M. Knopp, Soo Kim, Yuliya Shokh, "Options for Strengthening All-Source Intelligence: Substantive Change is Within Reach," RAND Corporation, February 28, 2022.
6. This concept was first put forward by Kevin Johnston in "It's Time to Give OSINT Its Own Agency," *Fair Observer*, February 25, 2022. https://www.fairobserver.com/region/north_america/kevin-johnston-osint-us-intelligence-community-international-security-news-35271/ [sic].
7. For more on IC's partnerships with state and local authorities, academia, the private sector and the public, see the description of "intelligence as a service" for the US public in Weinbaum, et al., *Options for Strengthening All-Source Intelligence*. ■

Open Source at a Critical Point in History

The View from CIA's Directorate of Digital Innovation

Daniel L. Richard

The author is the Associate Deputy Director of CIA for Digital Innovation.

In a world of constantly evolving technology and exploding open-source data, the Intelligence Community has a rare opportunity—and obligation—to transform our support to critical national security interests. This opportunity could not have emerged at a more significant time in our history. With the Chinese leadership using coercive measures to increase China's influence in the Indo-Pacific region, it is incumbent on CIA and the IC to produce the all-source intelligence necessary to effectively inform policymakers and help them adopt policies to minimize threats and avoid conflict.

Exploited effectively, the data-rich, open-source environment will provide a tactical advantage to US leaders during a period of escalation or even conflict. For example, commentators and everyday online users can provide near real-time alerts and contextualized OSINT insights on PRC naval movements in the South China Sea or flag possible Chinese preparations for conflict. Providing important datapoints such as these in timely, standalone OSINT intelligence products and as contributions to in-depth finished all-source analysis for policymakers could assist in enhancing

the US government's overall deterrence posture in the Indo-Pacific.

The CIA/Center for the Study of Intelligence June 2024 roundtable discussion, in which participants debated how the IC should optimize open-source collection, and its coverage in this special issue of *Studies in Intelligence* is recognition of the criticality of open-source collection. As the Open-Source Enterprise (OSE) is housed in the Directorate of Digital Innovation (DDI) in CIA and currently serves as the IC's Open-Source Functional Manager, the DDI leadership supported this roundtable as a healthy reflection on the open-source mission and its impact, notwithstanding the prospect that discussants might offer approaches, as they did, that challenge DDI organizational and resource decisions. This is especially true as the DDI leadership views our current national security environment as presenting a critical moment for the open-source community, even as budgets are under increasing strain.

DDI believes that the IC can best leverage its unique open-source capabilities under the existing

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

federated structure, with OSE housed in the DDI. As we focus on CIA provision of the digital capabilities necessary to meet our urgent global challenges, we must be mindful that any significant bureaucratic change to current open-source efforts will take critical time and energy away from the underlying open-source mission. Based on our experience of standing up other new IC organizations, it is likely that six months to a year will be required to clarify roles and build new structures. Given today's circumstances, we are in a critical period in our competition with the PRC, and we do not have time to lose. So, it is important that any discussion be tethered to this geopolitical reality. Even so, we need to remain open to change and to approach the use of open-source differently than we had considered it in the past. Determining how best to unleash the true capability of OSINT should drive our thinking. This roundtable was one step in DDI's effort to be open to innovation in this space.

As readers consider the different views found in the discussion here, they should reflect on how OSE has already been working to transform IC capabilities. OSE is no longer the FBIS structure of years gone past. Under current OSE leadership, OSE has made significant changes by making open-source information more discoverable, useable, impactful, and relevant to national security priorities. At the end of FY 2023, OSE launched a transformational platform for real-time and tailored situational awareness of world events that enables both the CIA and IC to view generative artificial intelligence-curated events and summaries based on OSE's global collection. OSE's work has been lauded by commercial AI thought leaders as one of "the best use of large language models." OSE's reporting on public unrest, coups, conflicts and

humanitarian disasters often provides the early warning and most detailed insights into these breaking events. As DNI Open-Source Executive Jason Barrett noted, "OSINT can help address 60 to 70 percent of our intelligence requirements." DDI believes OSE can turn that potential into a reality.

DDI's vision is to leverage our existing expertise both inside CIA and with our partners outside the agency to meet these opportunities and surpass expectations by developing novel ways to tap into the exponential growth in publicly and commercially available data. Partnering with the private sector, academia, and foreign partners to more efficiently collect and process the data that is most relevant to our mission. Focusing on tools to detect synthetic media and mis/disinformation in the open-source collection and identifying novel ways to integrate AI/ML capabilities to automate workflows and enhance expertise. We cannot do this alone and we cannot, and should not, strive to collect everything. Instead, we should be ruthless in focusing on that segment of publicly and commercially available information that can provide unique insights to our policymakers. We should seek to recruit and retain officers who see the transformational potential of open-source activities and can provide diverse and creative ways to innovate in this space.

We look forward to continued discussions on these issues in the weeks and months ahead and welcome views from inside and outside the government on how best to seize the moment and truly make OSINT the INT of first resort. The demands on the CIA and the Intelligence Community during this critical time in our history deserves nothing less. ■



A portion of the Simatai section of the Great Wall, about 75 miles northeast of Beijing—looking roughly southeastward into a cloud-shrouded China. Image by Wu Qiang, 2021.

China's Thickening Information Fog

Overcoming New Challenges in Analysis

Jonah Victor

The author is a Visiting Research Fellow at the Institute for National Strategic Studies of the National Defense University. He has served as a senior China analyst at the Department of Defense. The author thanks Phillip Saunders and Joel Wuthnow for their support and advice on this project.

Introduction

China has been a “hard target” for the Intelligence Community (IC) since the founding of the People’s Republic of China in 1949. Escalating demand for assessments of China since the 2010s has spurred the IC to expand its analytical and collection efforts. Last year, Director of National Intelligence Avril Haines

identified China as the IC’s “unparalleled priority.”¹ CIA Director William Burns asserted this year that his agency has more than doubled its budget for China-related intelligence collection, analysis, and operations during his tenure, extending work on China to “every corner of the CIA.”² Even as the IC buckles down on

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

China work, warning signs are emerging that the world is changing in ways that could disrupt business as usual. Washington's ability to anticipate developments in the US-China relationship and assess risks and threats to national security is likely to get harder.

Amid heightened tensions with Washington, Beijing has redoubled efforts to stiffen controls on information to prevent access by its potential adversaries. PRC authorities are mounting increasingly conspicuous counterintelligence activities, issuing public warnings of infiltration attempts by foreign spies and restricting the use of US technology, like iPhones and Teslas, due to purported surveillance threats.³ While heightened counterintelligence will concern operational elements of the IC, intelligence analysts are likely to be most aware of the mounting problems they face in accessing open-source information. Open source, while usually easier and cheaper to obtain than other intelligence sources, has gotten harder to gather when it comes to China.

Notably, journalists are struggling to obtain PRC entry visas, US researchers are confronted with more scrutiny and hurdles in their field work, non-governmental analysts have faced police investigations and even detentions, and their access to several essential databases has been limited by the PRC government. China specialists warn that their ability to gather

and evaluate information on China is constrained by Beijing's growing restrictions on data dissemination and international access to China.⁴ In 2023, historian Odd Arne Westad judged that "insights into decisionmaking in Beijing are harder to get than they have been for 50 years."⁵

These developments are alarming, but in historical context, hardly comparable to conditions 50 or more years ago. American journalist Edgar Snow, favored by Mao Zedong and granted extraordinary access to the inner circle of the Chinese Communist Party (CCP), wrote in 1962:

*Gaps in our information on present-day China seem limitless. The true state of China's industrial and agricultural economy, the general standard of living, rural and urban communes and the degree to which they may have added tension to her straining efforts to catch up, developments in science, education and cultural life, how China is governed and security measures used against anti-Communist opposition, the extent of China's military preparedness and self-sufficiency, are all in dispute abroad.*⁶

The IC, lacking Snow's access inside China, did not fare much better at the time. A study of declassified National Intelligence Estimates (NIEs) on China concluded that "in the early years

of the PRC, intelligence analysts enjoyed few advantages over their academic and journalistic counterparts on the inner workings of the Chinese Communist Party."⁷ Neither Snow nor the IC would anticipate the economic catastrophe resulting from Mao's Great Leap Forward.⁸ Storied CIA officer James Lilley recounted that his agency relied on anecdotal accounts from PRC refugees fleeing to Hong Kong and smuggled PRC newspapers to assess the deteriorating conditions in China.⁹

While IC and public insight into China increased after Mao's death in 1976, former State Department analysts Batke and Melton still observed in 2017 that "we know shockingly little about the men ... making decisions in Beijing."¹⁰

The IC, of course, is chartered to delve beyond publicly available information. The open-source world, albeit vast, will rarely provide insight on state secrets such as classified war plans and weapons systems or PRC activities in cyberspace, outer space, or underwater, activities that often require technical means to detect and evaluate. But for intelligence mysteries—those abstract puzzles without a concrete answer—open-source information usually contributes the foundational evidence for assessments. These include PRC leadership intentions, economic conditions, social-political trends, and military capabilities—the

essential context for evaluating national security threats.¹¹ With the executive branch, armed forces, and Congress increasingly making high-stakes decisions on China issues, the need for this information to inform public debate is greater than ever.

I argue here that China's recent restrictions on open-source information are significant and likely to increase further, but near-term actions by individual analytic units and longterm efforts at the federal

level could build resilience into US analytic capabilities. The following sections address:

- recent changes in information availability,
- drivers of further PRC restrictions,
- specific implications for IC analysis, and
- opportunities for analysts to thrive in changing conditions.

I interviewed specialists from federal agencies, nongovernmental organizations, news media, universities, and private sector firms. They included junior, senior, and veteran analysts with decades of experience and areas of expertise across PRC political, economic, technological, and military/security issues. This article was informed by their experience and perspective, but it does not necessarily represent a consensus view.

Indicators of an Information Lockdown

For years, any anecdote of a CCP information crackdown could be rationalized as a temporary adjustment, part of a historical cycle during which PRC leaders relaxed or tightened controls to suit shifting political objectives. Today's China may be breaking from this pattern: indicators are emerging of secular tightening across different information domains – a trend toward ultimately greater restriction.¹² To be sure, today's conditions are being compared to a recent high baseline in information openness. China analysts often recall the 2000s and early 2010s as the best period for obtaining open source information on China.

Restrictions during the Cultural Revolution of the 1960s and 1970s far exceeded in intensity and violence today's repressive measures against people and the spread of

information. The 1980s were a period of relative openness, up until the suppression of the Tiananmen Square protests in 1989, when unflattering international coverage provoked a media clampdown. But that was temporary, and Beijing relaxed many restrictions in the lead up to its entrance into the World Trade Organization in 2001. The expansion of the internet also led to a proliferation of online media and information resources. At the time of Xi Jinping's ascendancy in 2012, a tension existed between Beijing's efforts to increase restrictions in some areas of the expanded information environment, while in other areas making new efforts at government transparency.¹³ By the time of Xi's second term in 2017, his choice to restrict overall information flow had become clear.

Collapse of Domestic Journalism

Under Xi, the PRC news media, once a basic resource for tracking developments in China, has suffered heavily, experiencing a clear qualitative decline. In the Jiang Zemin and Hu Jintao eras, the CCP encouraged an active news media to help hold local officials to account.¹⁴ Since Xi's ascent, the CCP's influence on journalism has become increasingly oppressive and overt, pushing news outlets to highlight the positive role of the Communist Party, restricting topics permitted for public reporting, and removing editors and reporters who crossed into sensitive issues.¹⁵

Some observers highlight Xi's 2016 tour of state media outlets as a clear turning point, when he demanded "absolute loyalty."¹⁶ While to some extent this resembled

practices of previous PRC leaders, the CCP subsequently increased routine content filtering and instructions to news outlets on censorship, content removal, and bolstering positive narratives about China's governance.¹⁷

Between 2011 and 2017, 40 percent of Chinese investigative journalists left their jobs and 40 percent of those who remained were considering other careers, a phenomenon that scholar Maria Repnikova attributed to widespread professional disillusionment.¹⁸ Since then, space for investigative reporting and critical opinion in China has sharply diminished. Even reporting on pollution and environmental issues—once areas of vibrant media coverage—had come under pressure from central and local authorities by 2019.¹⁹

Still, PRC media remains essential for tracking breaking news, like natural disasters, and interpreting the CCP's intended message underlying often-turgid official statements. The silver lining of the regime's control over media means that content it allows will closely reflect CCP preferences and can serve as an indicator of change in policy.

Muzzled Voices in Hong Kong

The dwindling autonomy of Hong Kong—which intelligence officers once considered “the best listening post into Red



Hong Kong democracy advocate and media mogul Jimmy Lai was arrested under the PRC's new National Security Law in August 2020. He was charged with conspiracy to collude with foreign governments (including the United States) and to publish seditious material. © ZUMA Press Inc./Alamy.Stock Photo.

China”—deserves special attention.²⁰ Its vibrant and critical news media survived the early Xi era, continuing to offer a steady stream of “leaks, rumors, anecdotes, speculations, and sometimes fantasies and outright fabrications” on PRC politics, according to former CIA analyst Alice Miller.²¹

Press freedom began eroding in the early 2010s when PRC-based Alibaba purchased the mainstay *South China Morning Post* and then sharply declined with Beijing's forceful response to the 2019 protests in Hong Kong, including detention of opposition political leaders, and the application of the stifling National Security Law in 2020. That year, Hong Kong authorities arrested the owner and

chief editor of independent newspaper *Apple Daily*, which had been habitually critical of Beijing and Hong Kong leaders. The act led to the shutdown of the paper, television channels, and social media accounts.²²

The disappearance of the *South China Morning Post's* military reporter in 2023 after she had traveled to Beijing for an international security forum raised further uncertainty over the CCP's tolerance for the Hong Kong press.²³ Hong Kong reporters still operate with more independence than their mainland China counterparts, but their unique voice and insight is greatly diminished.

Reporting China by Zoom

Foreign journalists may have less fear of spoiling Beijing's favored narratives, but fewer can access China in person. Pandemic travel restrictions and the expulsion of 18 reporters from the *Wall Street Journal*, *New York Times*, and *Washington Post* in early 2020 left the US media footprint diminished.²⁴ The *New York Times*, which in 2008 could boast it had 12 correspondents in the country, had only two left by 2024.²⁵

In 2022, nearly 40 percent of foreign correspondents in China said that their sources were harassed, questioned, or detained, a figure up from 25 percent the year before.²⁶ Journalists faced increasing public hostility and warnings that their reporting may expose them to legal sanctions, civil lawsuit, or national security investigations.²⁷

With a diminished presence, the *Wall Street Journal* still managed to publish more accurate reporting on the CCP's plans for leadership appointments at the 2022 National Congress than any other major media outlet in China or elsewhere.²⁸

Sustaining such journalistic excellence will be a challenge, with many top reporters on China now based outside the PRC. Taiwan gained 63 foreign correspondents and 22 additional news organizations between 2020 and 2022,

largely due to PRC restrictions.²⁹ While this has increased media attention to Taiwan, Taipei does not offer the same perspective as reporting in Beijing. Reporters with prior experience in mainland China can stay in touch with their PRC contacts, but eventually they will likely be succeeded by journalists with little or no time on the ground.³⁰

Social Media that's Safe for Xi

China's media landscape is not just shaped by the quality of journalism, but by the efforts of PRC authorities to flood outlets with propaganda and censor unfavorable reporting. In 2013, Xi declared public opinion to be "a battlefield" and subsequently prioritized management of information and public opinion through coercion, censorship, and propaganda.³¹

Beijing, already well-practiced in managing traditional media, improved its ability to shape social media by centralizing internet management and regulation under the Cyberspace Administration of China, directly responsible to CCP leadership. Authorities reduced online anonymity, banned influential accounts with many followers, and even detained social-media users accused of spreading false information. Much of the candid social and political discourse in China moved from widely accessible platforms like Weibo (similar to then Twitter) to private discussions on WeChat (similar to WhatsApp).³²

Beijing's enhanced information capabilities were revealed during its response to the COVID pandemic, when the government manipulated social media discourse in ways that were complex, immediate, automated, and obvious to many PRC citizens.³³ Political scientist Jennifer Pan observes that the CCP mobilized state and party organizations to fabricate social media posts as if they were the opinions of ordinary people. Douyin (the PRC's version of TikTok) circulated "trending" videos that featured 40-percent CCP or state media content.³⁴

Beijing not only manages domestic voices but also controls content flowing into China. China's "Great Firewall" had blocked PRC-based access to many Western websites by 2010, including Google, Facebook, and Twitter.³⁵ More recently, Lu Yingdan and colleagues found quantitative evidence that the Cyberspace Administration encourages circulation of Western social media content in PRC channels when it expresses antagonism toward China and its people, seemingly to support the CCP's narrative that the United States and its allies seek to contain China.³⁶

Disrupting Desktop Research

Beijing's management of cyberspace goes beyond curating public perceptions to dynamic restrictions on online access and

official dissemination of data and information. This is particularly evident for researchers outside of China, who experienced a series of new disruptions in 2023. That year, foreign subscribers found their access blocked or limited to China National Knowledge Infrastructure—an archive of thousands of PRC-based academic journals, conference proceedings, statistical yearbooks, and graduate theses across all disciplines. Although some access was restored in 2024, it set back researchers and analysts who benefit from studying PRC-based scholarship. Some national security-related journals remained inaccessible.³⁷

Beijing also limited some foreign access to the Shanghai-based Wind Information database, which compiles PRC corporate registry information.³⁸ PRC sources that track data on vessels in Chinese waters reduced their input to global ship-tracking platforms, reducing a source for corroborating official data.³⁹ Chinese books with unique insight into the CCP and military became more elusive.⁴⁰

Beijing's changing policies have also disrupted the routine dissemination of official government data. From 2021, only a fraction of PRC judicial rulings continued to be published in Court Judgements Online.⁴¹ The Berlin-based MERICS think tank found that PRC ministries reduced their rate of publishing top-level policy documents from 88 percent in

2015 to 68 percent in 2022.⁴² This includes the decision to withhold public disclosure of the new Five-Year Plan on Science and Innovation.⁴³ MERICS also found that the volume of official government statistics is gradually receding after a huge expansion of PRC data dissemination in the 2010s that was meant to improve policymaking and attract foreign investment.

Beijing stopped publishing China's youth unemployment rate in mid-2023, attracting particular notice after the last data release showed joblessness of young adults jumping to a record 21.3 percent in June.⁴⁴ Data publication resumed in January 2024, showing a 14.9 percent youth unemployment rate.⁴⁵ Economic analysts disagree whether China's new data represent a better calculation method or obscure an important indicator of China's economic health.⁴⁶

Don't Pack Your Bags

Getting on-the-ground insight in the Xi era is much harder than it used to be. Beijing has restricted, disrupted, or discouraged foreign academic, corporate, and non-governmental researchers from conducting fieldwork and data collection in China. The 2018 arrest of two nongovernmental researchers from Canada (the "Two Michaels") and their nearly three-year detention cast a chill on the willingness of Western researchers to travel to China.⁴⁷ In 2021, Beijing banned MERICS, which employs about 20

full time China researchers, from travel to China or engagement with PRC entities.⁴⁸

Before the pandemic, academic researchers traveling to China already experienced increased restrictions, with about a quarter being denied access to archives and 9 percent approached by security officials.⁴⁹ American scholars returning to China since 2023 have encountered increased local hostility, fear, and distrust.⁵⁰ In 2023, only 700 American students visited China, down from 15,000 per year in the early 2010s.⁵¹ Scholars who attempt to conduct their research outside China are facing increased obstacles to accessing PRC data, statistics, and academic literature. Princeton Professor Rory Truex warns that this environment will inevitably "erode the quality of research on China."⁵²

Even the international business community—once warmly welcomed by the CCP—perceived new levels of hostility in 2023. Firms were reportedly concerned about new 2021 data security laws disrupting the exchange of routine financial information between PRC and foreign firms, exit bans placed on some foreign business executives in China, and the heightened scrutiny of corporate research.⁵³ Last year, the US Chamber of Commerce warned of heightened risk for doing business in China after PRC police questioned staff at the Beijing office of a US consulting firm and detained

staff at the Shanghai office of a US due-diligence firm.⁵⁴

Beijing is further disrupting dialogue and relationships between US and PRC citizens by restricting

engagement by PRC scholars and analysts. Since 2016, China's education ministry has required PRC academics to seek university approval for overseas trips and

collaborations. In 2020, universities began applying these rules even to online events held by international organizations, often barring scholars from virtual attendance.⁵⁵

More Restrictions: Raindrops or a Coming Downpour?

Most China analysts and scholars are concerned by Xi's restrictions but remain undaunted, often insisting that workarounds exist to obtain essential information.⁵⁶ But even if analysts and scholars are adapting to the current situation, this doesn't reckon with the prospect of Xi implementing further information restrictions. The underlying drivers of the restrictions—Beijing's and Washington's pursuit of security and a regime in China centralizing around the CCP and Xi himself—seem certain to continue.

Locking Down China

Xi Jinping's emphasis on China's internal security is the first main driver of PRC information control. He is not the first PRC leader to take on such security challenges or to manipulate the information environment. But Xi's smothering of freedoms in the financial hub of Hong Kong and drastic COVID lockdowns across Chinese society showed his willingness to risk China's economic growth and global influence to ensure absolute security.⁵⁷ Since the Tiananmen Square protests of

1989, PRC leaders have paid closer attention to the effect of news media on social and policy stability. China scholar Susan Shirk asserts that the CCP routinely manipulates the media to support its strategy of preventing large-scale social unrest, avoiding public leadership splits, and maintaining the loyalty of the military.⁵⁸

While Hu Jintao introduced some information restrictions, Xi's appointment in 2012 as CCP general secretary commenced an era of ever expanding propaganda and secrecy efforts, based on Xi's warning that the break-up of the Soviet Union was caused by a loss of belief and faith in its Communist Party.⁵⁹ Within a few years, the news media were cowed to strict adherence to Party lines – or silence – on top security issues including Tibet, Xinjiang, Taiwan as well as the tumultuous events of 1989. Pro-democracy protests in Hong Kong in 2019 and anti-COVID lockdown protests across China in 2022 spurred expansions of information control.

PRC restrictions on information have not been steady and

continuous, even in the Xi era.⁶⁰ In his first term, Xi implemented a new CCP transparency initiative, increasing the online publication of less sensitive official policy documents, judicial proceedings, and statistical indicators.⁶¹ Beijing even increased transparency on military affairs to encourage public support for the PLA's military modernization, and tolerated an online community of PRC defense wonks sharing intriguing insight into China's military activities.⁶² But these trends reversed by the 2020s, with PRC authorities expanding the boundaries for what constitutes "sensitive" information that should be kept from public view.

China's post-pandemic economic recovery disappointed many citizens, leading CCP leaders to perceive even sterile reports of negative economic data as a potential trigger of public discontent. Ironically, Beijing placed a public spotlight on the Ministry of State Security, China's main intelligence agency, which emerged in 2023 as a prominent social media voice for government policy, commenting even on economic matters. This sent an implicit signal that PRC

leaders perceived all manner of public discourse to be a potential national security issue.⁶³

Fear of Foreign Information Weapons

The second driver of information restriction is Beijing's perception of a heightened external threat, reinforced by Washington's explicit elevation of security concerns about China under the Trump and Biden Administrations. Xi declared that "Western countries—led by the US—have implemented all-round containment, encirclement, and suppression against us, bringing unprecedented severe challenges to our country's development."⁶⁴ Xi's concept of an "Overall National Security Outlook" sees internal and external security as interconnected, fearing that foreign forces might seek to stoke insurrection in regions like Xinjiang and Hong Kong, or stunt China's economic progress.⁶⁵

This reinforces Beijing's concern that information could be weaponized by China's adversaries. Beijing has claimed that foreigners are using open information to smear China, including publicized claims of human rights violations against Uyghurs, theories of a lab-leak origin for COVID, analysis of China's "Made in China" strategy for technological competition, and reports on China's military ambitions.⁶⁶ A new data security law in 2021 restricted transfer of potentially sensitive data abroad, with the Cyberspace Administration of

China directing data providers to restrict overseas access to information involving corporate-registration information, patents, procurement documents, academic journals and official statistical yearbooks.⁶⁷

US-China Security Spiral

Washington has also placed barriers on information flow between the United States and China out of concern for PRC espionage, and legal and illegal access to dual-use and commercially viable technologies. This third driver of restrictions is closely linked to the second, as China has responded to US restrictions with its own new barriers, either in purposeful retaliation or using the excuse to tighten security. For example, Beijing's limits on journalist visas for Americans were nominally a response to Washington's imposition of limits on the number of journalists from state and CCP-sponsored media allowed in the United States.⁶⁸ Beijing's restrictions on science and technology information coincided with Washington's expanded technology export regulations.⁶⁹ Increased federal scrutiny, and even espionage investigations, of students and researchers in the US who might be collaborating with PRC state entities has dampened US appetite for academic exchange and China studies as well as PRC citizens' comfort with US travel and study.⁷⁰ In 2021, Presidents Biden and Xi agreed to roll back some limits on journalist visas, but levels of news media access—especially by

Americans in China—is still greatly reduced.⁷¹

Who's in the Loop?

The fourth, and perhaps most important, driver of information restrictions are changes to the PRC political system, which is evolving to offer fewer sources of information and insight to begin with. Xi's tenure has seen Beijing move away from post-Mao efforts to strengthen state institutions alongside the party apparatus and develop a system of "collective leadership" that includes many officials in decision-making and consultations with non-governmental institutions and experts. The resurgence of party dominance, and the centralizing of power around Xi as CCP general secretary, means that important policies are decided in a smaller circle, and fewer individuals inside and outside the CCP having insight into leadership perceptions and policy deliberations.

US officials, journalists, and researchers used to obtain considerable value from interacting with PRC academics, diplomats, think tank researchers, party leaders, and senior bureaucrats who frequently had real insight into the thinking of top leaders.⁷² The access of these interlocutors (and their willingness to talk to foreigners) has declined as policy planning has been increasingly centered in secretive CCP organs like the Central National Security Commission.⁷³ Xi also prized centralization in his military reforms, reorganizing the PLA into

a tighter joint command structure. Among other things, this eliminated the seven military regions and their individual newspapers, which used to offer insight into lower-level PLA operational matters that is usually absent in the national-level PLA media.⁷⁴

The CCP has bucked procedural conventions since its last national congress in 2022, including unexpected personnel appointments and timing of party meetings that

have confounded even seasoned China analysts.⁷⁵ This year, Beijing declined to offer an annual press conference with Premier Li Qiang (the official PRC head of government) disrupting a 30-year practice.⁷⁶ Credible press outlets have published thinly-sourced, uncorroborated stories to shed light on the murky political situation, which risks potentially spurious claims filling Beijing's information vacuum.⁷⁷ The stranger mainstream articles

include accounts that Xi faced a reprimand from "party elders" over his policy choices, speculation that Xi schemed to publicly embarrass the elderly Hu Jintao when he was awkwardly escorted out of the party congress during a health event, and claims that Xi had commenced a "Stalinesque purge" across the CCP after the congress that demonstrated "feverish paranoia."⁷⁸

Maintaining Deterrence Amid Misperceptions

Losing independent insight into China, while facing a flood of state-sponsored information has real consequences for Washington's ability to navigate relations with Beijing. The US Defense Department claims to be increasing military and diplomatic activities along China's periphery and making major investments to support an "integrated deterrence" strategy.⁷⁹ The 2022 National Defense Strategy says this requires "tailored approaches to assess and manage escalation risk in both crises and conflict, including conducting analysis of escalation pathways and thresholds."⁸⁰ Xi's information control and increasingly centralized and secretive policy processes makes it harder to corroborate non-public sources and understand PRC thinking, perceptions, and red lines, posing a major challenge to satisfying this requirement. In a crisis, varying signals from different parts

of party, state, and military entities could be misinterpreted.

Evaluation of the perceptions and intentions of PRC leaders is already a contentious areas of analysis and scholarship. Should we focus on China's words or its actions? Should we highlight the CCP's internal messages or external messages? Does Xi reference Marxist doctrine to guide policy decisions or only to justify them? Should original Chinese texts or official English translations be authoritative? Analysts energetically debate these questions, even as they may be false choices. Ultimately, we will rarely know with confidence whether Beijing's decisions and statements reflect the view of individual officials, a consensus across leaders, or pragmatic reactions to a changing situation.⁸¹

On the other side of the deterrence equation is the potential for Xi and other PRC leaders to misperceive and misinterpret US words, actions, and intentions. In his 2023 study of Beijing's historical management of international crises, political scientist Tyler Jost finds that PRC leaders were more likely to miscalculate on use of force when they received poor information across fragmented or siloed institutions.⁸² Extensive censorship, information filtering, and discouragement of alternative views is likely to contribute to a worsening information environment in Beijing and increasing prospects for misperceptions.⁸³ US scholars report that their Chinese civilian and military counterparts acknowledge self-censorship and reluctance to report bad news to senior officials.

Searching for Money in the Shadows

Economic analysis provides insight into China's wherewithal and resource priorities for potentially challenging US interests, as well as Beijing's view on its expectations for prosperity and its influence on PRC economic actors. This requires having a good sense of growth rates and economic targets, where Beijing is making investments and subsidies, and sectors that Beijing is seeking to stimulate or slow down. Our ability to assess China's macroeconomic conditions and prospects depends on access to good data, and analysts worldwide depend on national and sub-national governments to collect, calculate, and report most data that bear on macroeconomic analysis. The late economist David Dollar said he primarily depended on IMF reports on China, and the IMF in turn depends on data from PRC authorities, which are affected by Beijing's openness and statistical capabilities.⁸⁴ Economists wage energetic debates over the extent to which China's GDP figures are accurate and reliable.⁸⁵ One consultancy with a particularly skeptical view estimated that China's economic growth in 2023, announced at 5 percent, was actually closer to 1.5 percent.⁸⁶

Some PRC government budgets are quite obfuscated; most analysts judge that publicly announced figures for the defense budget are a significant undercount.⁸⁷ At the

firm-level, recent PRC restrictions on corporate registry databases present obstacles for ascertaining the ownership structure and state/party connections of Chinese firms.⁸⁸ Even international firms operating in China are diminishing as a fruitful source for information and insight, given new data transfer regulations and discouragement of corporate research in China.⁸⁹

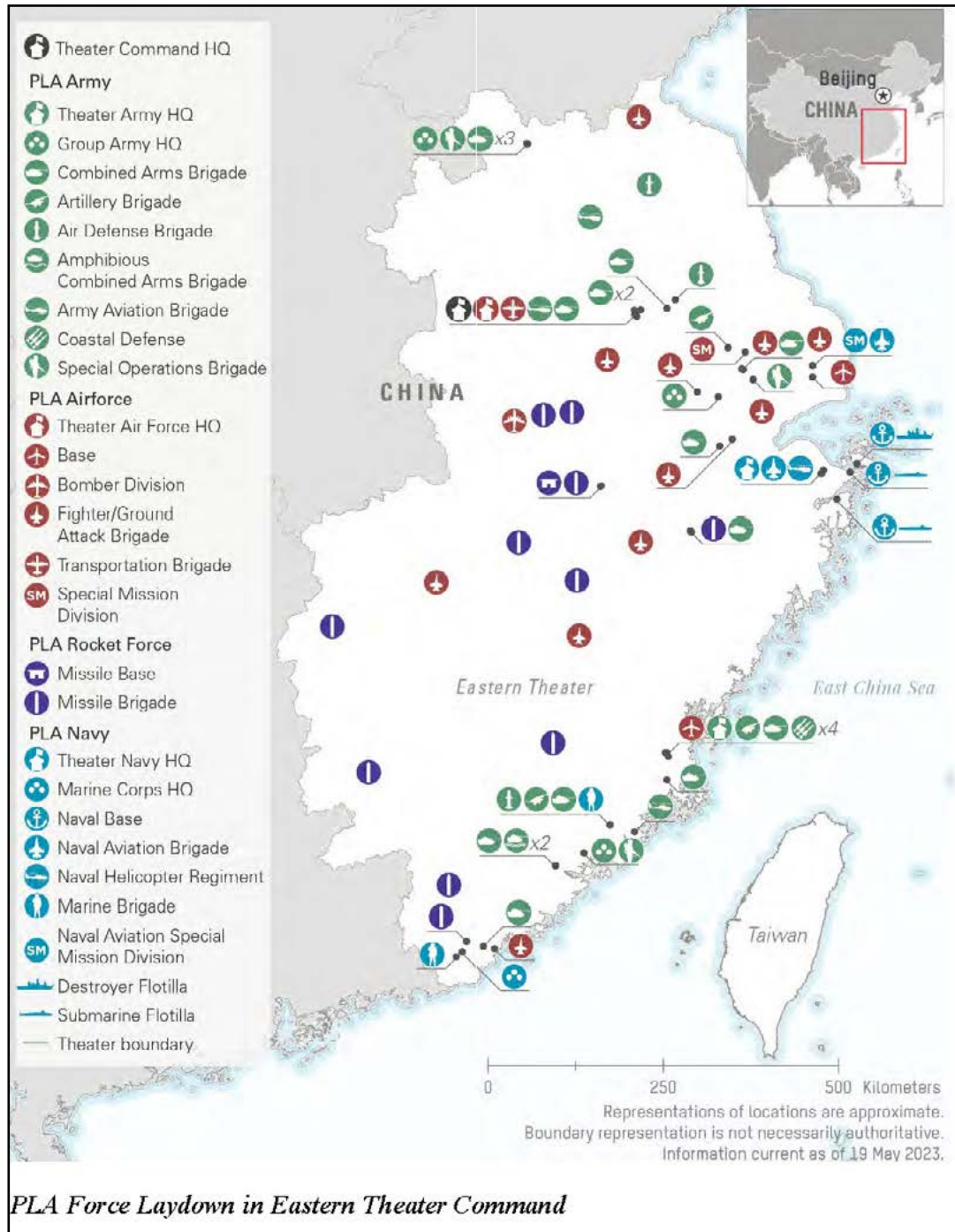
Roughly Estimating the Military Balance

Military analysis is an area where the IC and adjacent agencies of the US government can truly shine compared to analysts at non-governmental organizations. The Department of Defense, in particular, enjoys clear advantages in its ability to conduct accurate assessments of PRC military operations and capabilities highlighted by its annual release of a China Military Power Report (CMPR). (See following page.)⁹⁰ Beijing, once eager to show off advancements in PLA capabilities, has curtailed public knowledge of even routine exercises. Books and articles on Chinese military thought and doctrine have disappeared from bookstore shelves in China and online access since the 2010s.⁹¹ As of mid-2024, Beijing had not released a white paper on PRC defense policy since 2019, the longest gap to date between editions.⁹²

Some of the best public insight is available when the PLA conducts multinational exercises

or conducts operations directed at its neighbors. Mirrored data and reporting then becomes available from third-country sources, such as the Taiwan defense ministry's frequent press releases on PLA activity in the Taiwan Strait or reports from journalists on Philippine coast guard vessels who observe the PRC Coast Guard's intimidating actions in the South China Sea.⁹³ But this is insufficient for assessing developments in China's military capabilities, even for major weapons systems. Declassified NIEs indicate that the IC struggled to anticipate China's first nuclear test in the 1960s, and the 2023 edition of the CMPR revised upwards the Defense Department's projection for the size of the PLA nuclear arsenal.⁹⁴

Beijing's perception of Chinese capabilities and the military balance between the PLA and opposing forces is essential for its calculus on use of force.⁹⁵ This goes back to accurately understanding the perceptions and intentions of PRC leaders, which can mean the difference between judging China's emerging capabilities to be one risk among many for US interests, or a direct and urgent threat. The absence of routine public data on the PLA often leads to wildly variable speculation on intentions and capabilities.



This graphic is from the Defense Department’s CMPR (page 120), the annual congressionally-mandated unclassified assessment of military and security trends in China. The report is intended to inform public debate on relevant policy and legislation.

Getting Smarter on Open Sources

Policymakers look to the IC to be resourceful, clever, and responsive to their needs. Persistence in producing policy relevant insights in spite of Xi’s information control

is not only necessary and possible, but will increasingly distinguish the skill of the best China analysts and researchers. IC analysts and analytic units can take action in the

immediate to near term to enhance their resilience and success in a changing open-source environment.

Summary of Findings

Indicator	Trend since 2018	Likely Drivers	Major Impact	Opportunities for resilience
News media	More CCP influence on reporting, sharp increase in restrictions on foreign and Hong Kong media	Internal and external security concerns, centralization of decision making	Harder to anticipate leadership dynamics and policy adjustments across many sectors	Enhance tradecraft, adopt cyber tools, and emphasize rigor of analysis on existing information
Online access, social media	Dynamic and increasing restrictions on foreign access to PRC data and documents; increased CCP control of social media content	Internal and external security concerns	Diminished insight on PRC elite and mass perspectives and scholarship across issues of national security interest	Improve archiving, machine translation, and dissemination of digital material; enhance tradecraft, cyber tools, and rigor of analysis on existing information; protect fragile sources
Official data and documents	Declining dissemination of official information after a peak in 2010s	Mostly external security concerns	Challenges economic forecasts and anticipation of change across a range of policy areas	Methodically archive and analyze existing material; identify alternative economic indicators

But the prospect of non-IC analysts falling behind in their ability to assess important questions about China also needs to be addressed as a problem of national interest. The 2023 National Defense Authorization Act assigned at least five tasks to the IC to provide unclassified assessments on China, indicating the demand for cogent analysis to support public debate on the legislative process.⁹⁶ Some allied and partner governments may also struggle to stay aligned with Washington's perspectives, especially if they lack a deep bench of China experts, their Chinese and English language capabilities are limited, and credible information

on PRC risks and threats is not being communicated with their publics. There are some opportunities for policy, legal, and legislative action that Washington might consider to not only bolster governmental insight on China over the long term, but also to benefit non-governmental researchers and China knowledge among the general public.

Knowing What to Look for and Where to Find It

China analysts can become more productive with specific training in open source research. A massive amount of open source content

on China remains available and is almost certainly underexploited by the IC. Not all information is valuable; social media can offer insight into sentiment across Chinese society and favored CCP narratives while having limited relevance to analyzing PRC leadership and decisionmaking.⁹⁷ But PRC media can still alert the IC to breaking developments and indicate change in CCP policy. Chinese diaspora media, while uneven in reliability, sometimes publicizes activity that Beijing would rather keep quiet. One open-source training class does not prepare an analyst for life: data availability is dynamic and evolving, and one source may disappear just

as an alternative, perhaps better, source or analytic tool emerges.⁹⁸

With a little regular training and some incentive, analysts can become adept at knowing where and how to seek information relevant to their areas of expertise. Few will have time for comprehensive searches and daily browsing with an inbox full of taskings and demand for getting products to clients. But most analysts could implement a strategy for identifying indicators of change and a protocol for monitoring relevant sources, integrating open source tools into their normal research practices, balancing authoritative and non-authoritative information. This includes knowing how to distinguish between independent information and propaganda and how to evaluate each for meaning and insight.⁹⁹

Older methods of China analysis might be revived, according to former CIA media analyst Alice Miller, “by rigorously scrutinizing the content of [PRC] media, one could infer the regime’s goals and strategies.”¹⁰⁰ Today, data tools such as generative AI could be trained or customized to rapidly parse official documents and speeches, identify changes in language and substance, and propose initial interpretations. Such tools can aid productivity and identify areas for investigation but cannot yet substitute for an analyst’s expert knowledge, their ability to put datapoints into appropriate context, and make decisions on which sources to highlight in their analysis and why.¹⁰¹

Leaning into Analytic Tradecraft

Expert knowledge and analytic skills can derive cogent assessments from a fragmentary evidentiary base. But the IC’s messages and argumentation are going to be closely scrutinized and even criticized by some clients in the midst of high-stakes policy and budget debates on US-China relations. The IC can build resiliency by leaning into its tradecraft. This includes being explicit in the sourcing of information, identifying assumptions underlying analysis, and stating why alternative conclusions are ruled out.¹⁰²

Even if analysts apply rigorous tradecraft, use sophisticated tools, and enjoy wide access to data, subject matter expertise is still essential to putting datapoints into context. While urging technological and institutional innovations, former CIA analyst Peter Mattis reminds us that “the intelligence community will not be able to make reliable assessments of Chinese intentions without the input of the best strategic minds and close students of China.”¹⁰³ With fewer American students of China and the Chinese language, recruitment and retention of such talent may require greater effort.

Protecting Sources

With Beijing continuing to plug gaps in their information wall, the IC probably should consider declaring publicly-available sources worthy of protection as are its private sources. In 2023, two Washington think tanks took fire from fellow

China analysts for citing PRC open sources that were subsequently restricted by Beijing after they were used to assess national security risks of PRC activities.¹⁰⁴ While few China scholars favor changing standards for citing sources in their papers, the IC and US government more broadly might consider obscuring open sources perceived as being weaponized against China.

Some, like former Office of Naval Intelligence commander Michael Studeman, call for the IC to play a greater role in publicizing PRC “malign” activities and rapidly disclose material as “information fire” to counter PRC narratives.¹⁰⁵ Open-source information may be seen as cheaper cannon fodder than declassified secrets for such information operations, but the expected benefits of its use still need to be weighed against the risk of losing access. Protocols for protection of fragile sources and methods should be strongly considered.

Getting up close and personal

Many analysts and researchers identify decreased travel between the United States and China and the decline of direct exchange, dialogue, and collaboration with PRC counterparts as the most significant disruptions to insight on China issues. An on-the-ground view of contemporary China provides essential context for accurately assessing the behavior of PRC officials. US observers are sometimes only able to get critical insight on

China through direct, non-public governmental and non-governmental dialogue and exchange. Although the substance of official and state-sponsored exchange can be stilted or even scripted, it seems telling that economists at the US Federal Reserve calibrate their economic estimates based on context explained by Chinese officials in counterpart meetings.¹⁰⁶

High-level agreements between Beijing and Washington, clarification on policy and legal guidelines, and in some cases new funding would be essential to a recovery of governmental and non-governmental exchange. First, Beijing and Washington need to jointly commit to the safety of authorized researchers and analysts, given new fears among both US and Chinese travelers of cross-border scrutiny—and even detention—by authorities. For instance, the Schwarzman Scholars program continues to be an effective channel for Americans to study and research in China because it has high-level CCP endorsement.¹⁰⁷ One university scholar who once traveled extensively in China said he would only return if he was part of an official delegation.¹⁰⁸

Second, Beijing and Washington need to clarify legal guidelines for permissible cross-border collaboration and data-sharing. While there remain valid security concerns in specific sectors and disciplines, recent legal action by both governments has chilled academic exchange well beyond the scope

intended.¹⁰⁹ Third, the federal government probably needs to direct funding to encourage a revitalization of exchanges. This includes specific exchange programs with an official mandate and research grants specific to collaborative projects, to authorize and incentivize collaboration by PRC scholars and institutions that also perceive risks.

Back to the Stacks?

Lastly, mastering the exploitation of open sources requires a systematic approach to data management, obtaining materials, and consolidating archives. Even traditional library practices—widely perceived to be antiquated in a digital world—should be valued when it comes to China material. Social media and web posts need to be archived before they disappear under the hand of PRC censors or when Beijing decides to revise official documents and websites to mesh with changing CCP narratives.¹¹⁰

Hard copies of books and periodicals need to be saved in case digital access becomes further restricted. There may be opportunities for government, academic, and private sector entities to collaborate on consolidating collections of China materials in publicly-accessible collections and revitalizing academic area studies. Recent legislative proposals have included establishing a federal center for translations and dissemination of open source PRC material, that could be both responsive to IC needs and make products available to the

public.¹¹¹ International cooperation with allies and partners could also offer unique opportunities.

Promoting Analytic Resiliency and Expertise

Assessing trends in China will get harder as client's questions become more urgent and Beijing further obscures its intentions, perceptions, and capabilities. Open sources of information, whether China-based or international, will be an essential source for IC assessments as well public debate in the United States and allied countries on the future of US-China relations.

Individual analysts and agencies have room to become more adept and systematic at compiling and exploiting information available in the open source world. Adapting AI and other emerging technologies will enhance productivity toward this end, but will not substitute for the skill of subject matter experts to judge the veracity of a given datapoint, and put it into cogent context. Xi's efforts to manage perceptions of China have been impressive, but they are not impenetrable. Cross-border information flow is a national security imperative, and the stakes are too high for Washington not to push past these new barriers and get smarter on China. If given the chance, China analysts will have the drive and resilience to meet the mission. ■

Endnotes

1. Julian E. Barnes and Edward Wong, "U.S. Spy Agencies Warn of China's Efforts to Expand Its Power." *The New York Times*: March 8, 2023. <https://www.nytimes.com/2023/03/08/us/politics/china-us-intelligence-report.html>.
2. William J. Burns, "Spycraft and Statecraft." *Foreign Affairs*: January 30, 2024. <https://www.foreignaffairs.com/unit-ed-states/cia-spycraft-and-statecraft-william-burns>. (February 22, 2024).
3. Yoko Kubota, "WSJ News Exclusive | China Bans iPhone Use for Government Officials at Work." *Wall Street Journal*: September 6, 2023. <https://www.wsj.com/world/china/china-bans-iphone-use-for-government-officials-at-work-635fe2f8>; Keith Zhai, "WSJ News Exclusive | China to Restrict Tesla Use by Military and State Employees." *Wall Street Journal*, March 19, 2021. https://www.wsj.com/articles/china-to-restrict-tesla-usage-by-military-and-state-personnel-11616155643?mod=article_inline; "China Tells Its Citizens to Be on the Lookout for Spies," *The Economist*: September 21, 2023. <https://www.economist.com/china/2023/09/21/china-tells-its-citizens-to-be-on-the-lookout-for-spies>.
4. Wei Lingling, Yoko Kubota and Dan Strumpf, "China Locks Information on the Country inside a Black Box," *Wall Street Journal*: 30 Apr. 2023, www.wsj.com/world/china/china-locks-information-on-the-country-inside-a-black-box-9c039928. Accessed 22 Mar. 2024; Scott Kennedy (ed.), *U.S.-China Scholarly Recoupling* (Center for Strategic and International Studies, 2024). <https://www.csis.org/analysis/us-china-scholarly-recoupling-advancing-mutual-understanding-era-intense-rivalry>.
5. Odd Arne Westad, "What Does the West Really Know about Xi's China?" *Foreign Affairs*: June 13, 2023. www.foreignaffairs.com/china/what-does-west-really-know-about-xis-china.
6. Edgar Snow, *The Other Side of the River, Red China Today* (Random House, 1962), 117.
7. National Intelligence Council, *Tracking the Dragon: National Intelligence Estimates on China During the Era of Mao, 1948-1976* (National Intelligence Council, 2004). Hardcopies are no longer available. Most easily read online version is at https://web.archive.org/web/20060619102912/http://www.dni.gov/nic/foia_china_content.html. Also available, but in individual files with no introductory material at <https://www.cia.gov/readingroom/collection/china-collection>. U.S. Government Printing Office 2004. This specific reference to pages xii and xvi are in the introduction appearing in the web.archive.org version.
8. Ibid.
9. James R. Lilley and Jeffrey Lilley, *China Hands* (Public Affairs, 2009).
10. Jessica Batke and Oliver Melton, "Why Do We Keep Writing about Chinese Politics as If We Know More than We Do?" in *ChinaFile*: October 16, 2017. <https://www.chinafile.com/reporting-opinion/viewpoint/why-do-we-keep-writing-about-chinese-politics-if-we-know-more-we-do>.
11. Joseph S. Nye, "Peering into the Future." *Foreign Affairs* 73 (4) (July–August 1994): 82. <https://doi.org/10.2307/20046745>; Peter Mattis, "How to Spy on China." *Foreign Affairs*, <https://www.foreignaffairs.com/china/how-to-spy-china-beijing-technology-mattis>. April 28, 2023.
12. Anne-Marie Brady, "Plus ça change? Media Control Under Xi Jinping," *Problems of Post-Communism*, 64: 3-4 (2017): 128–140.
13. Author interviews of multiple analysts. Unless otherwise noted, all interviews were conducted during January–April 2024.
14. Susan L. Shirk (ed.), *Changing Media, Changing China* (Oxford University Press, 2011), 21.
15. Wang Haiyan and Jing Meng, "The de-professionalization of Chinese journalism," *Chinese Journal of Communication*, 16:1 (2023): 1–18.
16. Wong Chun Han. "In Rare State Media Tour, Xi Jinping Takes the Anchor's Chair." *Wall Street Journal*, February 19, 2016. <http://blogs.wsj.com/chinarealtime/2016/02/19/in-rare-state-media-tour-xi-jinping-takes-the-anchors-chair/>.
17. David Bandurski, "China's Press Under Xi Jinping Thought." *China Media Project*, November 22, 2023. <https://chinamediaproject.org/2023/11/22/chinas-press-under-xi-jinping-thought/>; Maria Repnikova, "Media Politics Under Xi: Shifts and Continuities." *The SAIS Review of International Affairs* 38, no. 2 (2018): 55–67.
18. Ibid.
19. Genovese, Isabella. 2022. "Environmental Reporters Face Disinformation, Threats in China's Restrictive Political Climate." International Journalists' Network. November 18, 2022. <https://ijnet.org/en/story/environmental-reporters-face-disinformation-threats-chinas-restrictive-political-climate>.
20. Lilley and Lilley, *China Hands*, 84.
21. Alice Miller, "Valedictory: Analyzing the Chinese Leadership in an Era of Sex, Money, and Power." *China Leadership Monitor* 57, 2 (2018).
22. Angeli Datt, "The Impact of the National Security Law on Media and Internet Freedom in Hong Kong," Freedom House, September 8, 2021. <https://freedomhouse.org/article/impact-national-security-law-media-and-internet-freedom-hong-kong>.
23. Roy Chung and Yeung Lee Heung, "Hong Kong Journalist Incommunicado, Feared Detained in Beijing." *Radio Free Asia*, December 1, 2023. <https://www.rfa.org/english/news/china/hong-kong-journalist-minnie-chan-12012023155241.html>.

24. Marc Tracy, Edward Wong, and Lara Jakes, "China Announces That It Will Expel American Journalists," *The New York Times*, March 17, 2020": Business section. <https://www.nytimes.com/2020/03/17/business/media/china-expels-american-journalists.html>.
25. *The New Yorker*, "The Culture Wars Inside the New York Times: An Interview with NY Times Executive Editor Joe Kahn by Clare Malone, July 10, 2024; See also Mike Chinoy, *Assignment China: An Oral History of American Journalists in the People's Republic of China* (Columbia University Press, 2023).
26. The Foreign Correspondents' Club of China, "Media Freedoms Report 2022: 'Zero Covid, Many Controls: Covering China in 2022'" March 1, 2023. <https://fccchina.org/2023/03/01/media-freedoms-report-2022-zero-covid-many-controls-covering-china-in-2022/>.
27. Erin Hale, "China Media Freedom Declining at 'Breakneck Speed': Report." *Al Jazeera*, January 31, 2022. <https://www.aljazeera.com/news/2022/1/31/china-media-freedom>.
28. Josh Chin, "China's Xi Jinping Likely to Pack Party Leadership with Allies in Show of Strength." *Wall Street Journal*, October 17, 2022. <https://www.wsj.com/articles/chinas-xi-jinping-likely-to-pack-party-leadership-with-allies-in-show-of-strength-11666024652>; Author interview with analyst, March 22, 2024.
29. Lu Yi-hsuan and William Hetherington, "China, HK Crackdowns Drive Media to Taiwan," *Taipei Times*, May 18, 2022. <https://www.taipeitimes.com/News/front/archives/2022/05/18/2003778386>.
30. Author interviews with multiple analysts.
31. Reprnikova, "Media Politics Under Xi: Shifts and Continuities." 56.
32. Alison Killing, "The Challenges of Conducting Open Source Research on China," *Bellingcat*, April 18, 2023. <https://www.bellingcat.com/resources/2023/04/18/china-challenges-open-source-osint-social-media/>.
33. Ibid.
34. Jennifer Pan, "Controlling China's Digital Ecosystem: Observations on Chinese Social Media," *China Leadership Monitor* 72, June 2, 2022. <https://www.prleader.org/post/controlling-china-s-digital-ecosystem-observations-on-chinese-social-media>.
35. Paige Leskin, "Here Are All the Major US Tech Companies Blocked behind China's 'Great Firewall'" *Business Insider*. October 10, 2019. <https://www.businessinsider.com/major-us-tech-companies-blocked-from-operating-in-china-2019-5>.
36. Lu Yingdan, Jack Schaefer, et al. "How Information Flows from the World to China." *The International Journal of Press/Politics* 29 (2) (April 2024). <https://doi.org/10.1177/19401612221117470>.
37. Wei Lingling, "U.S. Think Tank Reports Prompted Beijing to Put a Lid on Chinese Data." *Wall Street Journal*, May 7, 2023. <https://www.wsj.com/articles/u-s-think-tank-reports-prompted-beijing-to-put-a-lid-on-chinese-data-5f249d5e>.
38. Ibid.
39. Liza Lin Wong and Chun Han, "China Increasingly Obscures True State of Its Economy to Outsiders." *Wall Street Journal*, December 6, 2021. <https://www.wsj.com/articles/china-data-security-law-ships-ports-court-cases-universities-11638803230>.
40. Interviews with multiple analysts.
41. Kai von Carnap, "The Increasing Challenge of Obtaining Information from Xi's China," *MERICs*, February 15, 2024. <https://merics.org/en/report/increasing-challenge-obtaining-information-xis-china>.
42. Ibid.
43. Ibid.
44. Claire Fu, "China Suspends Report on Youth Unemployment, Which Was at a Record High." *The New York Times*, August 15, 2023. <https://www.nytimes.com/2023/08/15/business/china-youth-unemployment.html>.
45. Zen Soo, "China Starts Publishing Youth Jobless Data Again, with a New Method and a Lower Number." *Associated Press*. January 17, 2024. <https://apnews.com/article/china-youth-unemployment-slowdown-321cd96377ee066915fc39232b9477c3>.
46. Stella Yifan Xie and Jason Douglas, "China Has a New Youth Jobless Rate. Some Economists Are Ignoring It." *Wall Street Journal*, January 19, 2024. <https://www.wsj.com/world/china/china-has-a-new-youth-jobless-rate-some-economists-are-ignoring-it-dc2827e5>; Interview with US government economic analyst, February 13, 2024; Interview with private sector economic analyst, February 23, 2024.
47. Chris Buckley and Catherine Porter. "Scholars and Ex-Diplomats Warn of Chill After Canadians Detained in China," *The New York Times*, January 21, 2019. <https://www.nytimes.com/2019/01/21/world/asia/china-canada-michael-kovrig-michael-spavor.html>.
48. Francesca Ghiretti, "How China Imposes Sanctions." *MERICs*. June 6, 2023. <https://merics.org/en/report/how-china-imposes-sanctions>.
49. Sheena Chestnut Greitens and Rory Truex, "Repressive experiences among China scholars: New evidence from survey data." *The China Quarterly* 242 (June 2020): 349–75.

50. Emily Baum, Emily, "Researching China in a New Era: Conducting Ethnographic Research in China," Long US-China Institute, January 24, 2024. <https://www.youtube.com/watch?v=zSzFJOqGx3k>; Author interview with academic scholar, March 12, 2024.
51. William Yang, "Bilateral Tensions Cause the Number of American Students in China to Plummet," VOA News, December 19, 2023. <https://www.voanews.com/a/bilateral-tensions-cause-the-number-of-american-students-in-china-to-plummet-7404085.html>
52. Rory Truex, 2024. "Researching China in Hard Times," *Political Science & Politics* 57, no. 1 (2024): 146–48.
53. Julie Zhu and Xie Yu, "China's Top Financial Data Provider Restricts Offshore Access due to New Rules." Reuters, May 4, 2023. <https://www.reuters.com/business/finance/chinas-top-financial-data-provider-restricts-offshore-access-due-new-rules-2023-05-04/>.
54. Joe McDonald, "Foreign Companies in China Face Growing Scrutiny, Pressure." Associated Press. April 28, 2023. <https://apnews.com/article/china-foreign-business-corruption-investigation-technology-113adfa55788aabb11896d8b059b32bc>.
55. Emily Feng, "China Tightens Restrictions and Bars Scholars from International Conferences." National Public Radio, March 30, 2022. <https://www.npr.org/2022/03/30/1089631713/china-tightens-restrictions-and-bars-scholars-from-international-conferences>.
56. Multiple governmental and non-governmental interviews conducted by author, January–May 2024; Killing, "The Challenges of Conducting Open Source Research on China"; Eduardo Jaramillo and Yi Liu, "Cut off from China's Data and Info, Overseas Academics, Analysts Get Crafty." The China Project. July 6, 2023. <https://thechinaproject.com/2023/07/06/cut-off-from-chinas-data-and-info-overseas-academics-analysts-get-crafty/>; Author interviews with multiple analysts.
57. Sheena Chestnut Greitens, "Xi's Security Obsession," *Foreign Affairs*, July 28, 2023. <https://www.foreignaffairs.com/united-states/xis-security-obsession>.
58. Shirk, *Changing Media*, 16.)
59. Ibid., 2; Brady, "Plus ça change? Media Control Under Xi Jinping," 2; Wei, Kubota and Strumpf, "China Locks Information on the Country inside a Black Box."
60. Wei, Kubota and Strumpf, "China Locks Information on the Country inside a Black Box."
61. Carnap, "The Increasing Challenge of Obtaining Information from Xi's China."
62. Author interview with senior think tank analyst, February 27, 2024; Isaac Kardon, "China's Emerging Debate on Military Transparency," *China Brief*. September 10, 2010. <https://jamestown.org/program/chinas-emerging-debate-on-military-transparency/>.
63. Joe Leahy, "China's Feared Spy Agency Steps out of the Shadows," *Financial Times*, January 22, 2024. <https://www.ft.com/content/f78c7243-2ff5-4f77-93d0-91c20f6b5548>.
64. Ian Johnson, "How to Read Xi's Muscular Message on China's Global Role," Council on Foreign Relations, March 17, 2023. <https://www.cfr.org/article/how-read-xis-muscular-message-chinas-global-role>
65. Greitens, "Xi's Security Obsession"; Jude Blanchette, "The Edge of an Abyss: Xi Jinping's Overall National Security Outlook." *China Leadership Monitor*, September 2, 2022: 73. <https://www.prcleader.org/post/the-edge-of-an-abyss-xi-jinping-s-overall-national-security-outlook>.
66. Carnap, "The Increasing Challenge of Obtaining Information from Xi's China"; Jaramillo and Liu, "Cut off from China's Data and Info, Overseas Academics, Analysts Get Crafty."
67. Wei, "U.S. Think Tank Reports Prompted Beijing to Put a Lid on Chinese Data."
68. Tracy, Wong, and Jakes, "China Announces That It Will Expel American Journalists."
69. Sujai Shivakumar, Charles Wessner, and Thomas Howell, "Balancing the Ledger: Export Controls on U.S. Chip Technology to China." Center for Strategic and International Studies, February 21, 2024. <https://www.csis.org/analysis/balancing-ledger-export-controls-us-chip-technology-china>.
70. Rory Truex, "Opinion | Where Have All the American China Experts Gone?" *Washington Post*, January 2, 2024. <https://www.washingtonpost.com/opinions/2024/01/03/us-shortage-china-experts/>; Virginia Gewin, "Why the US Border Remains 'a Place of Terror' for Chinese Researchers," *Nature* 626 (February 2024): 1149–51. <https://doi.org/10.1038/d41586-024-00546-2>.
71. Michael D. Shear, "U.S. And China Agree to Ease Restrictions on Journalists," *The New York Times*, November 16, 2021, <https://www.nytimes.com/2021/11/16/us/politics/us-china-journalists.html>.
72. Miller, "Valedictory: Analyzing the Chinese Leadership in an Era of Sex, Money, and Power."
73. Westad, "What Does the West Really Know about Xi's China?"
74. Interview of senior non-governmental analyst, March 18, 2024.
75. Bill Bishop, "Taiwan; WTO; Li Shangfu; US-China; E-Bikes" *Sinocism Newsletter*, February 27, 2024; Chun Han Wong and Liza Lin, "China's Opaque Decision-Making Confounds Business, Governments." *Wall Street Journal*, January 9, 2023. <https://www.wsj.com/articles/chinas-opaque-decision-making-confounds-business-governments-11673269970>.

76. Vivian Wang and Chris Buckley, "China Scraps Premier's Annual News Conference in Surprise Move," *The New York Times*, March 4, 2024. <https://www.nytimes.com/2024/03/04/world/asia/china-premier-news-conference.html>.
77. Author interview with senior private sector analyst, March 20, 2024.
78. Katsuji Nakazawa, "Analysis: Xi Reprimanded by Elders at Beidaihe over Direction of Nation," *Nikkei Asia*, September 5, 2023. <https://asia.nikkei.com/Editor-s-Picks/China-up-close/Analysis-Xi-reprimanded-by-elders-at-Beidaihe-over-direction-of-nation>; Politico Staff, "China's Xi Goes Full Stalin with Purge," *Politico*, December 6, 2023. <https://www.politico.eu/article/chinas-paranoid-purge-xi-jinping-li-keqiang-qin-gang-li-shangfu/>; Wang Fan, "Hu Jintao: Fresh China Congress Footage Deepens Mystery over Exit." *BBC News*, October 25, 2022. <https://www.bbc.com/news/world-asia-china-63384608>.
79. C. Todd Lopez, "Allies, Partners Central to U.S. Integrated Deterrence Effort," U.S. Department of Defense, March 1, 2023. <https://www.defense.gov/News/News-Stories/Article/Article/3315827/allies-partners-central-to-us-integrated-deterrence-effort/>.
80. Department of Defense, *2022 National Defense Strategy*, 8. <https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF>
81. Batke and Melton, "Why Do We Keep Writing about Chinese Politics as If We Know More than We Do?"
82. Tyler Jost, "The Institutional Origins of Miscalculation in China's International Crises," *International Security* 48, no. 1 (2023): 47–90.
83. Dake Kang, "In Xi's China, Even Internal Reports Fall Prey to Censorship," Associated Press, October 31, 2022. at <https://apnews.com/article/health-china-beijing-covid-wuhan-3c199e3f1a084013da18fc9e6061e775>
84. Richard C. Bush, David Dollar, Ryan Hass, Jamie P. Horsley, and Shuxian Luo, "Commentary: Where Brookings Experts Read about China." November 10, 2021. <https://www.brookings.edu/articles/where-brookings-experts-read-about-china/>.
85. Benjamin Bernanke and Peter Olsen, "China's Transparency Challenges," Brookings, March 8, 2016. <https://www.brookings.edu/articles/chinas-transparency-challenges/>.
86. Rhodium Group, "Through the Looking Glass: China's 2023 GDP and the Year Ahead. December 29, 2023. <https://rhg.com/research/through-the-looking-glass-chinas-2023-gdp-and-the-year-ahead/>
87. Bartels, Fredrico. "Persistent Knowledge Gaps in the Chinese Defense Budget." *Joint Force Quarterly* 105, 2nd Quarter 2022
88. Author interview of analyst, February 13, 2024.
89. Author interview of private sector analyst, March 1, 2024.
90. Office of the Secretary of Defense. "DOD Releases 2023 Report on Military and Security Developments Involving the People's Republic of China," October 19, 2023. <https://www.defense.gov/News/Releases/Release/Article/3561549/dod-releases-2023-report-on-military-and-security-developments-involving-the-pe/>.
91. Author interviews of think tank analysts, February 27, 2024.
92. Andrew Erickson, "China Defense White Papers—1995–2019," posted in 2019 at <https://www.andrewerickson.com/2019/07/china-defense-white-papers-1995-2019-download-complete-set-read-highlights-here/>
93. Ben Lewis, "2022 in ADIZ Violations: China Dials up the Pressure on Taiwan," ChinaPower Project, March 23, 2023. <https://chinapower.csis.org/analysis/2022-adiz-violations-china-dials-up-pressure-on-taiwan/>; Rebecca Wright and Ivan Watson, "CNN Witnesses Maritime Confrontations between China and Philippines in the South China Sea," CNN, March 6, 2024. <https://www.cnn.com/2024/03/06/asia/philippines-china-south-china-sea-confrontation-intl-hnk-dst/index.html>.
94. National Intelligence Council, *Tracking the Dragon*, 25; Office of the Secretary of Defense. "DOD Releases 2023 Report on Military and Security Developments Involving the People's Republic of China."
95. Hal Brands and Michael Beckley, "How Primed for War Is China?" *Foreign Policy*, February 6, 2024. <https://foreignpolicy.com/2024/02/04/china-war-military-taiwan-us-asia-xi-escalation-crisis/>.
96. Fiscal Year 2024 National Defense Authorization Act (NDAA). 2023, Sec. 7401–7408. <https://www.congress.gov/bill/118th-congress/house-bill/2670/text>.
97. Miller, "Valedictory: Analyzing the Chinese Leadership in an Era of Sex, Money, and Power," 10.
98. The China Project. 2023. "Open-Source Intelligence in Crisis: Navigating China's Restrictions." September 22, 2023. <https://thechinaproject.com/2023/09/22/open-source-intelligence-in-crisis-navigating-chinas-restrictions-2/>.
99. Miller, "Valedictory: Analyzing the Chinese Leadership in an Era of Sex, Money, and Power," 10.
100. *Ibid.*, 9.
101. Ardi Janjeva, Alexander Harris, Sarah Mercer, Alexander Kasprzyk, and Anna Gausen, "The Rapid Rise of Generative AI Assessing Risks to Safety and Security," Alan Turing Institute, 2023. https://cetas.turing.ac.uk/sites/default/files/2023-12/cetas_research_report_-_the_rapid_rise_of_generative_ai_-_2023.pdf.
102. Batke and Melton, "Why Do We Keep Writing about Chinese Politics as If We Know More than We Do?"
103. Mattis, "How to Spy on China."
104. Wei, "U.S. Think Tank Reports Prompted Beijing to Put a Lid on Chinese Data.")

105. Mike Studeman, "The US needs a better strategic narrative or it will cede influence to China," *Financial Times*, February 18, 2024. <https://www.ft.com/content/b5987c48-cdb1-44f9-bf9c-55f6fe20ba12>
106. John Fernald, Israel Malkin, and Mark Spiegel, "On the Reliability of Chinese Output Figures," Federal Reserve Bank of San Francisco Economic Letter, March 25, 2013. <https://www.frbsf.org/research-and-insights/publications/economic-letter/2013/03/reliability-chinese-output-figures/>.
107. Kaiser Kuo, "Schwarzman Scholars Capstone Showcase," Sinica Podcast, March 7, 2024.
108. Interview with university professor, March 12, 2024
109. Kennedy (ed.), *U.S.-China Scholarly Recoupling*.
110. Killing, "The Challenges of Conducting Open Source Research on China"; Carnap, "The Increasing Challenge of Obtaining Information from Xi's China," 10.
111. US Senate. "Text - S.4118 - 118th Congress (2023-2024): Open Translation Center Authorization Act." April 11, 2024. <https://www.congress.gov/bill/118th-congress/senate-bill/4118/text>. ■

intelligence in public media

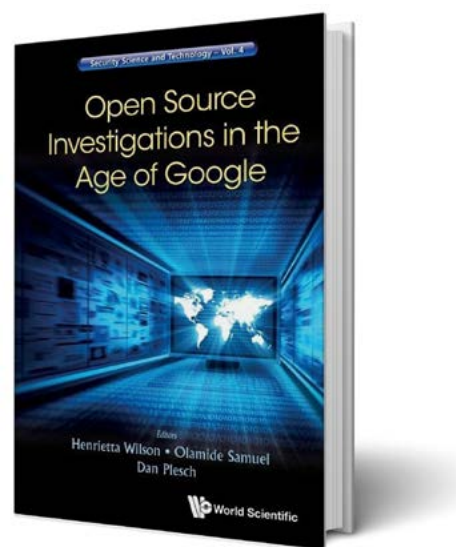
Open Source Investigations in the Age of Google

Author: *Henrietta Wilson, Olamide Samuel, Dan Plesch (eds.)*

Published By: Worldwide Scientific, 2024

Print Pages 388

Reviewer **Stephen Mercado**
The reviewer is a retired CIA open-source officer and frequent contributor to *Studies*.



In today's digital age, those who conduct the ancient art of open-source research benefit from technologies and techniques unknown to the medieval scribes who translated texts of classical Greek into Latin on parchment, or for that matter to the Cold War officers in the Foreign Broadcast Information Service (FBIS) who used typewriters to produce translations and analyses of Soviet media. The authors of *Open Source Investigations in the Age of Google* inform us of the modern ways and means to use open sources to investigate issues in human rights, military conflict, nuclear nonproliferation, and other issues of interest.

Advances in computer science and information technology have greatly changed the way we gather

and analyze open sources. The vast card catalogs of research libraries have given way in recent years to rows of computer terminals. The World Wide Web went public in 1991. Google, the world's most popular web-based search engine, dates to 1998. Space Imaging released the world's first high-resolution commercial satellite images in 1999.

More than 30 experts have contributed 18 articles on conducting open-source investigations today. Most of the contributors hail from Great Britain or the United States. Many are academics. Some work at prominent open-source organizations, such as Bellingcat and the Federation of American Scientists (FAS).

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

Open Source Investigations in the Age of Google

The authors highlight the myriad tools for open-source investigations. Beyond Google, notes Christiaan Triebert of the *New York Times*, stands Russia's Yandex search engine. Alternatives to Google Maps, writes digital investigator Benjamin Strick, include China's Baidu Maps, Microsoft's Bing Maps, Apple Maps, and HERE WeGo's mapping from the Dutch multinational Here Technologies.

With tools come techniques. Several authors mention geolocation, the identification of an object's location in a digital image. Hans M. Kristensen and Matt Korda of the FAS, explaining that geolocation is sometimes possible with Chinese videos of military content, write that the technique led in 2019 "to the discovery of the Jilantai training area" for Chinese missiles, which led the next year to uncovering new silos, "which led to the discovery of China's three large missile silo fields in 2021."

Another technique is chronolocation, a technique to determine the time and place of an event. Henrietta Wilson, Olamide Samuel, and Dan Plesch note in the book's first article that cross-checking information from different data streams, such as comparing videos from social media against satellite imagery, is one way to locate and date an event. One can even travel back in time. Rhona Michie, Paul Holden, Andrew Feinstein and Alexandra Smidman explain how investigators can use the Wayback Machine (<https://wayback-api.archive.org/>) to compare new versions of corporate websites against old ones to catch businesses that have erased incriminating information from their corporate websites.

Even in this digital era, time-tested methods still hold true. Experts in open sources still read print media and monitor radio programs. The twist today is that we likely go online rather than read paper or listen to a nearby radio broadcast on a physical receiver. Andrea Carboni and Clionadh Raleigh of Britain's University of Sussex write that the Armed Conflict Location and Event Data Project for monitoring military actions, other

violence, and protests, "collects reports from thousands of sources in over 75 distinct languages" as part of its intake of open sources.

Language, now as ever, remains important. As Triebert suggests in his article, when investigating an event in Yemen, conduct your search in Arabic. Remember that, even today, there is no standard transliteration for Arabic words in the Latin alphabet. Some aspects of open-source work remain the same today as in the era of typewriters.

The book's authors also point to the challenges and limits of open sources, including protecting the privacy of individuals in the course of investigations and sorting the real facts from disinformation. Within the US Intelligence Community, as Kathleen M. Vogel writes, open sources are at a disadvantage in organizations that prize secrets. Machine learning promises to take open-source investigations to an even higher level but, as Jamie Withorne notes, the emerging technology is not without limitations.

I could point out an isolated error here, a questionable assertion there, but my impression of the book is a positive one. A bibliography or guide to further reading would have made the book even better, but the copious footnotes effectively serve the same purpose. Contributions of open-source experts from China, Russia, and elsewhere outside the Anglo-American sphere would have given the book a more universal character.

Overall, the articles in this book provide much food for thought. Both students new to open-source investigations and experienced practitioners in the field will find material that is new and interesting. Much has changed in open-source investigations since the internet came on the scene in 1991. This book gives us a good idea of where we are today.

The book is available free of charge at <https://www.worldscientific.com/doi/epdf/10.1142/q0414>



review essay

Counter-Intelligence: What the Secret World Can Teach Us About Problem-Solving and Creativity

Robert Hannigan (HarperCollins, 2024, 336 pages)

Challenger: A True Story of Heroism and Disaster on the Edge of Space

Adam Higgenbotham (Avid Reader Press, 2024, 576 pages)

Reviewed by John Ehrman

The reviewer is a retired CIA Directorate of Analysis officer and frequent contributor to *Studies*.

You don't see too many books about the management of intelligence services, and for good reason. After all, how big is the audience for tales of the administrative side when there are thrilling operational stories to be told? But management is vital, for without it no exquisite human or technical ops are possible. That is why two new books, one specifically on intelligence and the other not, are worth reading for their insights on managing intelligence work.

Problem-Solving and Creativity

Let's start with the basics: how do you organize and staff an intelligence service? How can services create a culture in which unusual people doing unique work can succeed? Maybe most important, how do you do all this during a time of rapid technological change and organizational disruption? These are the questions that Robert Hannigan, former director of the UK's Government

Communications Headquarters (GCHQ) and now an academic at Oxford, addresses in *Counter-Intelligence*. It is an absorbing, perceptive, and challenging book that gives readers much to think about.

Hannigan answers these questions by looking at the history of GCHQ from its antecedents before World

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

War I through the Cold War and the recent establishment, on his watch, of the National Cyber Security Centre (NCSC). This is not a detailed linear history of British SIGINT, however. Instead, Hannigan tells short stories, focusing on the episodes that shaped GCHQ and created a culture that, he says, continues today. Most of his examples are familiar because, coming from the world wars, they were declassified long ago.

Within this framework, Hannigan pays most of his attention to the people who accomplished heroic feats when England was in peril. Codebreaking is an ancient practice, but in World War I, the interception and decryption of large numbers of radio transmissions was a completely new task, undertaken without an established corps of professionals or supporting infrastructure. Who, then, to hire or assign to invent intelligence gathering and analysis on an industrial scale?

The answer, says Hannigan, was not simply the mathematicians or linguists you would expect but, rather, people who enjoyed solving puzzles and playing difficult games. What they had in common were talents for spotting patterns and organizing data, which were critical skills for decryption in the pre-computer age. (During World War II, one recruitment test for Bletchley Park was to ask candidates to solve the *Daily Telegraph's* crossword puzzle.) Others, like Alan Turing, indeed were brilliant theoreticians, but most came from unexpected backgrounds and walks of life, with wide ranges of talents and outside interests. They were a collection of eccentrics with “random skills” and, Hannigan notes at several points, few would make it

through today’s corporate and government hiring tests, “which prioritize speed and practical focus.” (88)

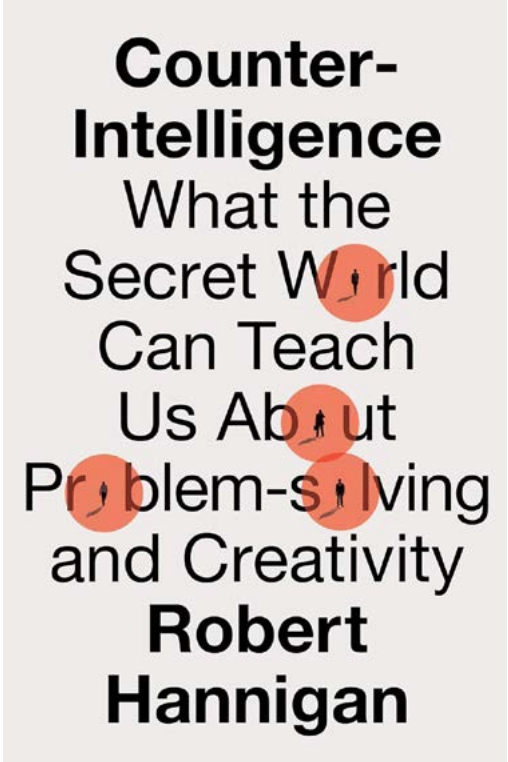
Counter-Intelligence abounds with stories of these ordinary-but-unusual people who did extraordinary things. One of the best known is Alfred Dillwyn “Dilly” Knox, who started as a papyrologist studying fragments of poetry by Herodas—a Greek poet of the third-century BCE—that had been found in the

Egyptian desert. Knox had no template to guide him in assembling the ancient fragments, which themselves contained mistakes made by scribes two millennia ago and shifted dialects within poems. Knox, however, knew that he faced not only a technical problem but a human one. “Deciphering the fragments therefore involved understanding both the poet and the idiosyncrasies of the scribe—the human errors,” Hannigan comments.

The British used Knox’s approach in World War II, getting to know the idiosyncrasies and weakness of individual German radio operators. This enabled them to predict the

mistakes the Germans would make and, in turn, gave the code breakers an important edge in their work. Once Knox had deciphered a passage of Herodas, it provided a key to others—and the same turned out to be true for the German codes. (Knox’s translations of Herodas remain in print today, and he used these methods to break Hungary’s diplomatic codes between the wars without ever learning a word of Hungarian.)

In contrast to Knox, few have heard of Geoffrey Tandy, a botanist and marine biologist working at the Natural History Museum in London at the start of World War II. He answered a misprinted ad, or so the



Counter-Intelligence
What the Secret World Can Teach Us About Problem-solving and Creativity
Robert Hannigan

story goes, seeking experts in cryptograms, a class of plant that includes seaweed, and soon was hired for Bletchley Park. Tandy spent the war mostly compiling and cross-referencing German and Japanese terms that could not be found in standard dictionaries but also—and here is where an expert in saltwater algae is good to have around—salvaging and preserving codebooks retrieved from sunken German ships and U-boats.

Hannigan pays attention to the administrative side as well. Brilliant people often turn out to be difficult employees or terrible managers (you probably don't need a book to tell you this). In dealing with unusual and creative people, Hannigan says that the British experience shows that a flexible and informal system works best, though it requires managers to know their people well enough to see who works best alone or in a team, whom to flatter, and how to channel disparate energies toward a common goal.

Knox again is a good example. At the start of World War II, he was made part of the joint UK-French-Polish team working on Enigma, but he was a disaster—undiplomatic and determined to control all that he worked on, and his boss at one point had to send a written apology to the French for Knox's behavior. Ultimately, the team was reorganized so that Knox could concentrate on his own research, which provided methods that others could use to exploit the intercepts. Despite his repeated threats to resign, Knox stayed on and, working with a small, all-female staff of his own—"Dilly's Girls," a tag that would not be tolerated in today's corporate cultures—made the breakthrough that led to the British naval victory over the Italians at Cape Matapan.

GCHQ's Cold War work remains hidden, but Hannigan leaves the impression of significant successes against Soviet targets, and for much the same reason as in World War II. Here, he adds some interesting comments on neurodiversity and the challenges—and rewards—of hiring people with "problems." In retrospect, of course he sees that such individuals have long been overlooked resources, with specific talents

that enable them to make valuable contributions. The Israelis, he notes, have found that autistic individuals make very good imagery analysts, better at interpreting blurred images than any software, because of their "relentless focus on the detail of what can or cannot actually be seen, resisting our normal tendency to extrapolate or make assumptions and guesses." (248)

Hannigan brings the story to the present with a discussion of cybersecurity. The problem of how to adapt intelligence work to changing threats and circumstances is not new, and neither is Hannigan's recommended solution—to continue the tradition of innovation and openness to unconventional people and approaches. He points to NCSC, whose founding he oversaw, as an example of rethinking whether the traditional extreme secrecy of the SIGINT world is appropriate for cybersecurity. "Calling out Russian, Chinese, Iranian, or North Korean cyber actions and describing some of their details goes against most of the instincts of the secret world," he says, but has the advantage of spreading the information that enables parties outside the formal intelligence world to help combat these threats. (284)

Hannigan tells his story and makes his case in clear, delightful prose, with the dry wit for which the English are famous. It helps to have a background in intelligence history—he assumes basic knowledge of codebreaking in the wars as well as such back stories as why Charles Dodgson (aka Lewis Carroll) is not held in much esteem these days—but avoids technical jargon or discussions, so the book is accessible to the lay reader. Indeed, if you are at all interested in intelligence work and the people who do it, you won't want to put it down.

That said, however, some US readers may find that *Counter-Intelligence* has a subversive side. Hannigan views diversity through the lens of individuality. He takes his talent where he finds it, regardless of race, gender, and so on; he seems unconcerned about building a GCHQ that looks like Britain. In the United States, by contrast, diversity, equity, and

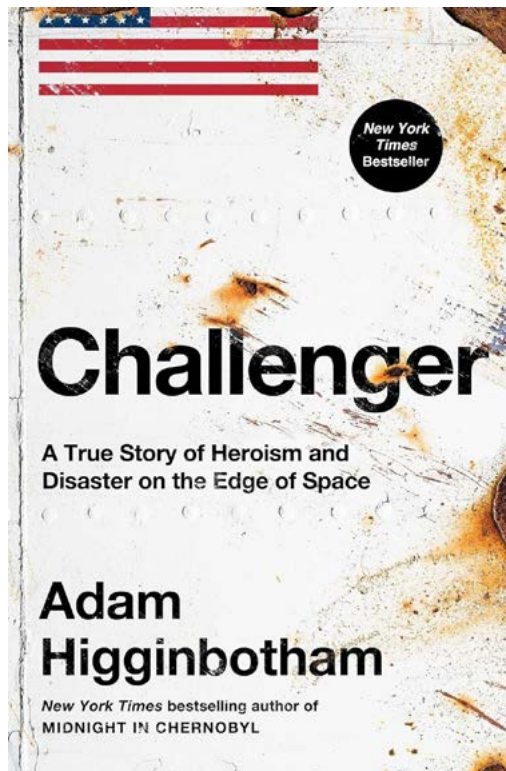
inclusion (DEI) emphasizes groups and group identity. This is not surprising, as such an emphasis lends itself to the needs of large organizations—the US Intelligence Community comes to mind—by making metrics easier to collect. What this approach does not do, however, is guarantee the hiring of the talented individuals a given organization truly needs. This is what Hannigan is telling us when he says that so many of the greatest contributors at Bletchley Park could not make it through today’s hiring processes. It also is

what he is saying when he cites Conway’s Law, that “large organizations are constrained to build systems that mirror their own structures” and will “arrange staff according to existing processes ... reflecting the way that work has been done in the past” rather than consider radical change in their processes. (77) The IC today is far more diverse than it was 40 years ago, but many of its day-to-day procedures are unchanged, albeit computerized. Whether the IC has become any better at its core tasks is an open question.

Heroism and Disaster

If figuring out how to build a successful organizational culture isn’t enough of a task for you, then Adam Higginbotham’s *Challenger* will give you plenty more management issues to consider. This will be especially so if, like many of us, you’ve asked why we keep making the same mistakes over and over.

Challenger is a history of the space shuttle program, from its origins in the late years of the Apollo program, when NASA was trying to figure out what to do after the moon landings ended, through the *Challenger* disaster in January 1986. Higginbotham, a journalist and author of the extraordinary *Midnight in Chernobyl* (2019), tells the story in riveting detail. As with his recounting of the Chernobyl nuclear catastrophe, Higginbotham brings his characters to life, makes complicated technology easy to understand, and builds the suspense even though you know what is going to happen.



Why, then, should an intelligence audience be interested in the well-known tale of NASA’s failure? The answer is that, as a government agency, NASA’s problems are the same as those found in the IC. Looking to build on the glory of the moon landings, as well as to preserve its prestige and budgets, NASA set itself the ambitious goal of building a reusable space plane. The shuttle would be more technologically advanced and complex than any previous space vehicle, and NASA would use it, in essence, to build a cargo airline in orbit.

Unfortunately, such ambitions do not come cheap and as the program advanced through the 1970s, NASA found itself operating in an unfriendly political and public relations environment in which its budgets were subject to repeated cuts. Nonetheless, the space agency maintained its goals. This meant that, as costs rose and pressure to show results and placate an increasingly critical Congress and public increased,

NASA began cutting corners. Risks that should have been considered unacceptable—most notably the design flaw in the solid rocket boosters that made a catastrophic failure all but inevitable—were wished away, under the designation of “acceptable.” After all, the reasoning went, as the shuttles flew mission after mission and nothing bad happened, the chances the boosters would explode must be minimal. Even as the engineers at Morton Thiokol, the booster’s manufacturer, repeatedly warned of the dangers, “NASA managers prioritized magical thinking over technical realities.” (422)

Matters came to a head in January 1986, when NASA, frustrated by bad publicity from repeated delays, pressed Thiokol to agree that it was safe to launch *Challenger*, even though the cold weather made the boosters especially likely to fail. Thiokol’s higher managers, for their part, were worried about losing the lucrative contract to build the rockets and overruled their engineers’ objections. The launch went ahead, and *Challenger* and its crew were lost, exactly as predicted.

Following the loss of *Challenger*, former Secretary of State William Rogers led the formal inquiry, which led to extensive changes in NASA’s procedures. But organizational culture is a powerful force and, once the glare of publicity eventually dimmed, “slowly, insidiously, some of the old ways and attitudes became reestablished,” writes Higginbotham, describing Conway’s Law in action. In January 2003, during the launch of *Columbia*, a piece of insulating foam on the giant external fuel tank fell off and hit the leading

edge of the shuttle’s left wing, damaging the tiles that protected against the heat of reentry. Like the boosters, this wasn’t a new problem—it had been known since the first launch in 1981—but, as it had never led to trouble before, the risk was assumed away. This time, however, the hit on the tile left a hole that let in superhot gas during reentry, in effect melting the wing from within as the shuttle returned to earth.

The management and leadership lesson of Higginbotham’s account is simple: wishing does not make things so, and not listening to the people who know what they are talking about leads to terrible outcomes. Just as important, having a glorious past is fine, but trying to relive it without sufficient resources is folly; when budgets are cut, ambitions must be adjusted as well. Pretending otherwise—telling employees to “do less, better” or “work smarter, not harder”—leads only to sloppy, substandard work.

These books offer the reader two different experiences. *Counter-Intelligence* is a story of intelligence triumphs as well as a guide to shrewd personnel management; it’s an upbeat book that, while it may leave you frustrated with your organization, tells you that improvement is possible. *Challenger*, by contrast, is more complex and relentlessly grim. But you’ll see more of your own experiences in Higginbotham’s book, and gain an understanding of why true change in government is so difficult. You won’t go wrong reading either one, and reading them in tandem is truly enlightening. ■

intelligence in public media

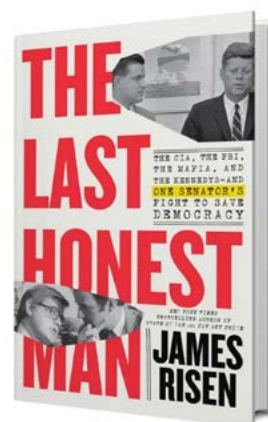
The Last Honest Man *The CIA, the FBI, the Mafia, and* *the Kennedys—and One Senator's* *Fight to Save Democracy*

Authors James Risen with Thomas Risen

Published By Little, Brown, 2023

Print Pages 468

Reviewer David Robarge
The reviewer is the chief of CIA's History Staff.



Frank Church arguably is the most significant figure in the history of congressional oversight of intelligence. The Idaho Democrat's leadership of the Senate Select Committee to Investigate Government Operations with Respect to Intelligence Activities, familiarly the Church Committee, cast unprecedented scrutiny on the Intelligence Community—specifically programs and operations of questionable morality and legality. Along with those of the White House's Rockefeller Commission and the House of Representative's Pike Committee, the Church Committee's efforts in 1975–76 brought about a permanent change in public accountability for the US government's most prominent secret agencies. Never again would CIA, FBI, and NSA be able to operate with the clandestinity they had enjoyed in preceding decades.

No biography of Church has been written since 1994, and, notwithstanding its overlong and overblown title, *The Last Honest Man* by longtime intelligence writer James Risen and his son, journalist Thomas Risen, is a solid and generally fair profile that does justice to Church's lasting influence on US intelligence. They thoroughly recount his upbringing, education, local influences, and early interest in politics and displays of oratorical skill. Church got intelligence training in the US Army and served as an order-of-battle analyst in China in 1945. He married the well-connected daughter of a prominent Idaho family, survived a serious bout of cancer by way of an experimental treatment, and at age 32 won a long-shot bid for a US Senate seat in 1956, refusing along the way to use scandalous material against his incumbent opponent.

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

The Last Honest Man

One of the book's main themes is the dual nature of Church's character: "the ambitious, publicity-seeking politician yearning for acceptance in Washington ... and the radicalized outsider who hated the Washington establishment, the Frank Church who despised the American imperialism represented by a spy agency prepared to kill foreign leaders." (5) This twofold quality made good sense in Idaho politics. Church survived and prospered as a "blue" internationalist in an isolationist "red" state by endorsing his constituents' strongly held views on gun control and environmentalism—he was against the former and for the latter. But his own psychology came with a cost—a public image of him as a moralistic showboater. "He suffered from political ambition that was sometimes blinding. He was a publicity hound with a careful, studied speaking style that could make him seem pretentious and arrogant; he earned the nickname 'Senator Cathedral.'" (8)

While in the Senate, Church underwent a gradual political and ideological transformation. He started out as a conventional Cold War Democrat with vague domestic policy views but moved leftward in both areas. Fights over civil rights legislation and the Vietnam War turned him into an ardent liberal. He regretted voting for the Tonkin Gulf Resolution authorizing a US military buildup in Vietnam and pushed the chairman of the Senate Foreign Relations Committee, William Fulbright, to hold public hearings that intensified opposition to the war. The Cooper-Church Amendment, which banned funding for US military forces in Laos and Thailand, made him a national figure, and he reveled in the attention he got for rebelling against a president of his own party. Contrarily, his disaffection toward the Washington establishment grew; Church wanted to be part of it by raising his official prominence, but he eschewed its social trappings and gained few friends among his legislative colleagues.

Although Church tried, his new-found fame did not translate into roles with the congressional Watergate inquiries because of his outsider status. Opportunely timed leaks of information about the International Telephone and Telegraph Corporation's influence in

foreign countries gave him a public stage from which to investigate the hidden power of US corporations in world affairs. His inquiries into US multinational corporations' involvement with CIA's election intervention in Chile in 1970 and Lockheed's pervasive use of bribery to win overseas contracts drew backlash from senior senators who thought he was going too far, but he resisted their pressure to let up.

Church's relatively close re-election win in 1974 goaded him to consider a presidential run in 1976—complicated by his leadership of the select committee investigating the IC that began work in early 1975 after the Family Jewels disclosures.^a His quandary highlighted his two sides—the reformer and the politician. "At the most important moment in his career, Church couldn't choose between the two, between his genuine moral outrage over the CIA's abuses and the growth of an American empire, and his own political ambitions. And so, in the most fateful decision of his career, he would try to do both: run what would become known to history as the Church Committee, and run for president." (167)

The 16 chapters covering the committee's work constitute the heart of the book. Not much new is revealed on the major topics the senators and the staffers examined—assassinations, Mafia plots to kill Fidel Castro, a very limited set of covert actions, the MKULTRA drug-testing program, the FBI's COINTELPRO attack against Martin Luther King, CIA and NSA domestic surveillance—but the Risens' treatment of them is useful for consolidating information about them in one place and providing well sketched portraits of some of the principals, especially Mafiosi Johnny Roselli and Sam Giancana (both mysteriously murdered during the committee's investigation). Church, who admired John F. Kennedy, had to tread carefully when Kennedy's relationship with Giancana lover Judith Exner emerged in the course of the Castro assassination plots investigation. Church's delicate treatment of the matter caused Republicans on the committee to complain that he was covering up for the Kennedy family.

a. David Robarge, "Evolution of Surveillance Policy: US Intelligence, Domestic Surveillance, and the Time of Troubles," *Studies in Intelligence* 68, no. 2 (June 2024).

Interesting details appear about the inner workings of the committee's staff, notably the different personalities and agendas of staff director William Miller and committee counsel F.A.O. "Fritz" Schwarz and how they affected the Committee's work. Miller was "a genial, straitlaced former U.S. Foreign Service officer"; Schwarz was "a long-haired, aggressive New York lawyer." They "represented the two sides of Church's personality. Miller reflected the Frank Church who was a politician yearning for status and acceptance from the establishment. Schwarz represented the post-Vietnam Frank Church who was a radical eager to overturn the militaristic, imperialistic status quo." (182, 184) The two clashed almost immediately. Church sided with Schwarz. According to one staffer partial to Miller, the staff director "wanted to reform the [intelligence] community, point out some mistakes, and get to the bottom of the problems, but do it in a way that the intelligence community cooperated with. And Schwarz wanted to do it in a more adversarial way.... Schwarz managed to put on a good show, and that's exactly what Church wanted." (189)

Church's decision to focus initially on the CIA assassination plots antagonized the pro-Miller faction, but he ignored the critics, assigned a small unit with three committee members (John Tower, Gary Hart, and himself) and 15 staffers, led by Schwarz, to delve into them.^a The result: "Schwarz's work with Church... ultimately solidified his control over the committee's staff, while Miller faded further into the background." (202) Church fended off White House resistance to publishing the assassination report and, without full Senate approval—he said none was needed—went ahead and released it.

The committee held no public hearings on the assassination plots or covert action operations. That put Church in a double bind: "When he held open hearings, the press said he was showboating to hype his possible run for the presidency. When he held closed hearings, pundits said he was engaged in a cover-up.... Unable to go public with the lurid tales uncovered in the assassination investigation, Frank Church and his staff scrambled to find another story that would capture the public's imagination and grab headlines

in the committee's first public hearing" scheduled for September 1975. (328) When they found out that the CIA had illegally kept a supply of shellfish toxin after President Nixon had ordered its destruction, they had their story. The result was the oft-depicted scene of some of the committee members handling the notorious dart gun—labeled an CIA assassination pistol although it was a US Army weapon used to disable sentry dogs, which the Risens do not mention.

Several other errors or unnuanced statements appear in these chapters about the committee. Counterintelligence chief James Angleton, whose testimony (later withdrawn) that "It is inconceivable that a secret intelligence arm of the government has to comply with all of the overt orders of the government" appalled Church, receives the usual stereotyped treatment as a paranoid alcoholic. Kim Philby was a penetration, not a double agent. CIA was not involved in coup plots against South Vietnamese President Ngo Dinh Diem. DCI Richard Helms's notes about the White House meeting on September 15, 1970, with Richard Nixon and Henry Kissinger about keeping Salvadore Allende from winning the October election in Chile—"One in 10 chance perhaps, but save Chile!...not concerned risks involved...make the economy scream"—are not mentioned even though they contradict the self-exonerating statements that Kissinger, Nixon, and Kissinger aide Alexander Haig made later. The 1973 coup in Chile was not "CIA-backed." Lastly, in its covert-action inquiry, the committee examined only a small set of regime-change operations, leaving the enduring impression that CIA's covert actions were all anti-democratic exercises in eliminating troublesome left-wing nationalists and protecting compliant pro-US dictators. A thorough review of CIA covert programs reveals exactly the opposite to be true: the overwhelming majority (upward of 90 percent) were intended to protect democratic governments or popular sovereignty where it was threatened and to promote anti-authoritarian movements in autocratic or totalitarian states.

In the end, Church had to recant his characterization of CIA as a "rogue elephant" and accept that it acted under presidential authorization, even if often vaguely

a. See David Robarge, "Interview with Former US Senator Gary Hart," *Studies in Intelligence* 65, no. 4 (December 2021).

The Last Honest Man

conveyed. As the committee wound down its work, Church spent less time with it and more on his presidential campaign. His late start irreparably hobbled it, however, and he never built sufficient momentum to win enough primaries to stymie Jimmy Carter. His pursuit of the White House “seemed like little more than a Church family vanity project.” (371) An effort to become Carter’s running mate failed awkwardly.

During Carter’s presidency, some of the reforms Church had worked for came to fruition: the standing oversight committees in the Senate and House, the Foreign Intelligence Surveillance Court to oversee domestic surveillance, Carter’s executive order banning US involvement in foreign assassinations, and the Foreign Corrupt Practices Act outlawing bribery of foreign officials. Church also took the politically risky step of supporting the Panama Canal Treaty, much disliked in Idaho, but he believed it was vital to repairing the regional image of the United States as an imperialistic interloper. That upset the careful balance he had struck in the state’s politics. “We get just a little bit tired of hearing about your conscience,” said one letter to the editor in a local paper.” (393) Up for reelection in 1980, Church suffered from Idahoans’ disapproval of Carter, whereas Ronald Reagan’s popularity there helped Church’s opponent Steve Symms narrowly prevail. According to Symms, fellow Idahoan James Angleton encouraged him to run as

a way to get back at Church for damaging his own reputation and harming CIA.

Church left politics quietly, working for a Washington law firm and traveling with his wife, who had been his longtime political confidante. However, in early 1984 he was diagnosed with pancreatic cancer and died that April. He was buried in Morris Hill Cemetery in Boise. Three years later when Angleton died, he also was buried there, about one hundred feet from Church.

The Last Honest Man is a valuable and very readable addition to the literature on congressional oversight of US intelligence. For further reading on the Church Committee, see:

- Loch K. Johnson, *A Season of Inquiry: Congress and Intelligence* (Dorsey Press, 1988)
- Kathryn S. Olmsted, *Challenging the Secret Government: The Post-Watergate Investigations of the CIA and FBI* (University of North Carolina Press, 1999)
- Frank J. Smist, Jr., *Congress Oversees the United States Intelligence Community, Second Edition, 1947–1994* (University of Tennessee Press, 1994)
- L. Britt Snider, *The Agency and the Hill: CIA’s Relationship with Congress, 1946–2004* (CIA Center for the Study of Intelligence, 2008) ■

intelligence in public media

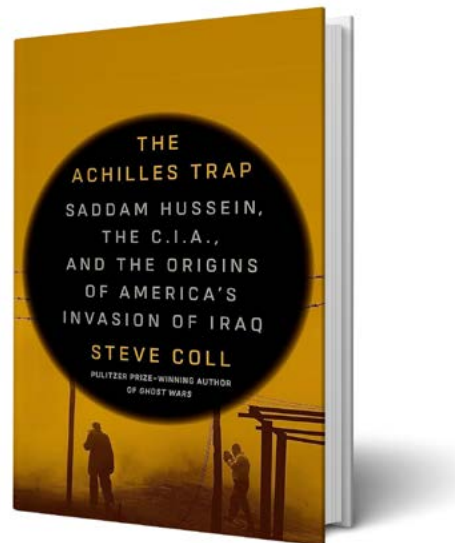
The Achilles Trap *Saddam Hussein, the CIA,* *and the Origins of America's* *Invasion of Iraq*

Author Steve Coll

Published By Penguin Press, 2024

Print Pages 556

Reviewer Brent Geary
The reviewer is a member of CIA's History Staff and a member of the *Studies* Editorial Board.



For a quarter century, two-time Pulitzer Prize winning journalist and academic Steve Coll has been among the most astute observers and chroniclers of US foreign policy and intelligence history. He is the author of several excellent works, including books on the influence of oil giant ExxonMobil, US relations with South Asia, and the bin Ladin family. *Ghost Wars* (2004), in particular, is among the finest studies of a discrete US foreign policy issue written this century, if not the very best. Ostensibly about CIA and its role in Afghanistan in 1980–2001 and the early hunt for Usama bin Ladin—CIA provided Coll with access to serving officers for oral histories—*Ghost Wars* captured far more than that. In richly detailed and riveting vignettes as varied as the evolution of US relations with Saudi Arabia to the

background of former CIA Director George Tenet's rise to prominence, Coll's research and nuanced writing were exemplary. For these reasons, it remains a must-read for students of US national security and intelligence history.

In 2018, Coll published *Directorate S*, chronicling the CIA's conflict with al-Qa'ida in Afghanistan and Pakistan and US relations with both countries from 9/11 to 2016. While sweeping in scope and impressive in its own right, *Directorate S* lacked some of the punch of its predecessor. *Ghost Wars* explained, years later, how 9/11 came about and benefited greatly from the passage of time; *Directorate S* told a story that was, at the time of publication, still very much unfolding and about which, after nearly two decades of war, we had all grown weary.

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



With his latest offering, *The Achilles Trap: Saddam Hussein, the CIA, and the Origins of America's Invasion of Iraq*, Coll again is working with the benefit of years of hindsight and moderated emotions and writing about a subject that very much needs a comprehensive accounting. And, once again, he has risen to the occasion. *The Achilles Trap*—an allusion to the mythical Achilles' vulnerability despite his seeming invincibility—is another tour de force and might be the definitive work on the matter for years to come.

While careful to examine factors at play in both Washington and Baghdad, at the center of this new book is Coll's extensive research and trenchant analysis of Iraqi leader Saddam Hussein. Many others have analyzed the inner workings and motivations of the George W. Bush administration during this time, but only Coll has done so in combination with those of the Iraqi leader. Drawing from interviews with US officials, former intelligence analysts, and regional experts as well as some 2,000 hours of recordings of Saddam's sensitive government meetings made available after his fall, the author meticulously retells the dictator's story from his earliest days to his execution. As one reviewer put it so well, "People love to imagine that world affairs are a game of chess" whereby leaders make decisions based on a solid understanding of the other players and both sides' national self-interests.^a Coll reminds us, however, that decisionmakers are people, too, with sometimes fatal flaws that lead them to make horrendous choices.

To sum up, Coll argues convincingly that delusions across several US administrations and from Baghdad made all but inevitable the ensuing clash. In his telling, after initially agreeing to accept intelligence support from the Reagan administration during the early years of the Iran-Iraq War (1980–88), Saddam felt betrayed when he learned—along with the rest of the world, in 1986—of the secret US sale of arms to his enemy Iran during the Iran-Contra scandal. Already inclined to view the world through anti-Zionist conspiracy theories, Saddam decided after that episode that the United States could not be trusted and began entertaining delusions of leading the Arab world against

a. Noreen Malone, "Is America All-Knowing and All-Powerful? Yes, Thought Saddam Hussein," *New York Times*, March 28, 2024.

both Israel and the United States. In addition, Reagan's failure to hold Saddam to account for his genocidal gassing of Iraqi Kurds in 1988 led the Iraqi leader to believe the US government would not take strong action against him and possibly empower revolutionary Iran in the process. Those delusions contributed to his decisions to invade neighboring Kuwait in 1990, to attempt to assassinate former President Bush in 1993, and start down the path of his eventual destruction.

As for the United States, Coll lays blame across four presidencies, starting with Reagan, whose embrace of Saddam as a counter to Iran followed by his secret dealings with Tehran thoroughly confused and confounded the Iraqi leader. George H.W. Bush, for his part, is described as trying to reassure Saddam of US support right up to the latter's invasion of Kuwait, only to wage war on him, enact crippling sanctions, and impose an international weapons-inspection regime after Saddam's defeat. The Clinton administration—with public acknowledgment by members of Congress—continued a “covert” action program begun by Bush designed to foment a coup against Saddam, but provided sparse resources for the effort and ignored those who argued that it had virtually no chance of success. Additionally, Coll illustrates effectively that Clinton understood that he should hold direct dialogue with Saddam's regime to better understand its intentions regarding its WMD programs, but that Clinton demurred for fear of being accused of weakness by his political opponents. (475) Most significantly, by running a covert action against Saddam at the same time that the US government and international inspectors were pressing him to be transparent about his WMD program, Coll argues that Clinton—and his successor—deluded themselves that Saddam could ever convince them that he was genuinely dismantling his programs.

Unintended consequences abound in Coll's telling of the Iraq covert action, with one highly unfortunate result being the empowerment of an individual he described as “talented, ambitious, and ruthlessly deceptive,” Iraqi opposition leader Ahmad Chalabi, for a time a favorite of certain senior US officials who was “destined to alter the courses of Iraqi and American history.” (268) Over several pages, Coll provides a detailed case for the prosecution against the

duplicious Chalabi, one which future national security decisionmakers would be wise to read and remember. With the US government so openly seeking to oust Saddam, as well, the Iraqi leader and his inner circle viewed international weapons inspectors as being part of a larger effort to remove him from power, resulting in varying degrees of cooperation and behaviors by Saddam's henchmen that inspectors and analysts interpreted as part of a WMD cover-up. Coll provides cautionary words about not just this covert action, but covert action itself as a tool of policy, citing no less an authority than former CIA Deputy Director for Operations Tom Twetten. “If you can execute foreign policy without it, that's preferable,” Twetten said, because of such unintended consequences. (267) Another former CIA operations officer, Dave Manners, made a similar point in more colorful language, stating “A half-assed covert action was worse than none at all.” (303)

Addressing the US intelligence failure regarding Iraq WMDs, Coll argues convincingly that while the US Intelligence Community clearly got it wrong, because of the unique circumstances in Iraq there was probably no way for it to have done otherwise. For example, he illustrates that even members of Saddam's inner circle did not know or believe that he had destroyed the WMD programs just months before the US invasion. Likewise, because the US IC had dramatically underestimated facets of the WMD program before learning their true size and scope following the 1991 Gulf War, US intelligence analysts and collectors alike were determined not to undersell those programs a second time. Lastly, Coll reminds readers that basically no experienced outside observers of Iraqi politics believed in 2003 that Saddam had destroyed his programs and that to have argued otherwise would have required evidence that was simply not available absent deep penetration of every aspect of Saddam's highly compartmented regime.

While many mistakes of analysis and collection were made during this episode, Coll demonstrates that Saddam had complied with the expectations of the international community but that he was unable or unwilling to convince us—or even his own lieutenants—of that fact because of his history of hiding his programs, the excessive secrecy of his regime, and his

The Achilles Trap

misguided belief that the US government knew he had destroyed the weapons and sought his destruction anyway.

The Achilles Trap is not without flaws, but they are mostly minor. Writing about contemporary events—years before most relevant documentation will be released to the public—Coll once again relies heavily on oral histories. While understandable, it is also fraught with the possibility of bad memories, score-settling, personal bias, and limited scope, issues which may have informed some of the storylines Coll pursues. However, he rarely if ever makes claims based on one or two sources, and having conducted more than 100 interviews, he usually had sufficient material to draw from. Also, in an effort to describe the repressive and violent Iraqi regime and provide context for how its operation contributed to its failure to convince weapons inspectors that it had destroyed WMDs, Coll probably spends too much time describing the lives and circumstances of a handful of individual Iraqi scientists. Again, this is a small criticism, as their stories are important but probably did not require the number of pages dedicated to them.

Coll's book—as in Melvyn Leffler's *Confronting Saddam Hussein* (see Michael J. Ard's review in *Studies in Intelligence* 67, No. 3, September 2023)—concludes the George W. Bush administration did not inten-

tionally mislead the American public but rather exaggerated available evidence about Iraqi WMD and Baghdad's ties to al-Qa'ida and engaged in "unabashed fearmongering." (449) In seconding his point, another reviewer argued that had Coll written *The Achilles Trap* in 2002, "his career might have ended," because Coll would have been labeled an apologist for Saddam for depicting the dictator as an onerous and deeply flawed human being, but not a caricature.^a I find no fault with that analysis and it speaks volumes that the book's reviews—across media outlets of vastly different political bents—have been universally positive. If you do not remember those days, trust me, people did not or could not think straight about the relative threat that Saddam represented.

At a time when journalists are regularly criticized as lacking impartiality or accused of partisanship, it is important to give credit where it is due. With *The Achilles Trap*, Steve Coll proves once again that it is possible to be both critical and fair, even when writing about the murky, ethically challenging worlds of intelligence and national security. Intelligence professionals—especially analysts, operations officers, and their managers—diplomats, warfighters, policymakers, and all others who seek to understand the ways in which our country became embroiled in a war in Iraq should give *The Achilles Trap* permanent space on their bookshelves. ■

a. Spencer Ackerman, "Steve Coll's Latest Shows Saddam Hussein's Practical Side," *Washington Post*, February 27, 2024.

intelligence in public media

Zhou Enlai: A Life

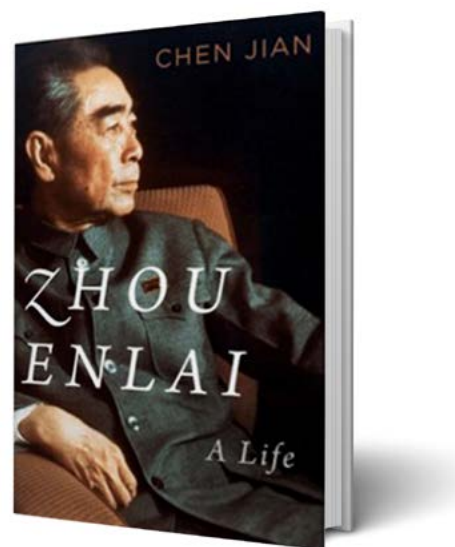
Author: *Chen Jian*

Published By: Harvard University Press, 2024

Print Pages 840

Reviewer: *Matthew J.*

The reviewer is a CIA analyst. He previously taught and researched East and Southeast Asian politics and PRC foreign policy.



In seeking to fulfill his ambition to remake the global order, People's Republic of China (PRC) President Xi Jinping often looks to Foreign Minister Wang Yi to help implement that grand vision. In his role, Wang is one of the most front-facing individuals of the Chinese Communist Party (CCP) outside of Xi. Early in his tenure, Wang said that Zhou Enlai, the creator and first head of the Ministry of Foreign Affairs (1949–58), would “always be a model for diplomats”^a and recounted Zhou’s view that PRC emissaries must tackle their duties in the same way the People’s Liberation Army did. Another PRC diplomat recounted that within the Foreign Ministry one

“can criticize Mao Zedong, but you cannot criticize Zhou Enlai.”^b These comments should come as no surprise, as Wang’s father-in-law served as an aide to Zhou, but today’s consistent mentions of the late premier reflect the reality that Zhou’s shadow continues to loom large over Beijing’s rise as a global power.

In *Zhou Enlai: A Life*, Cornell University historian Chen Jian traces Zhou’s life from humble beginnings in Jiangsu Province to a top CCP leader and China’s point figure in international relations. Chen, who was born in China and earned his first college degree in a Chinese university and still teaches in Chinese institutions, is well

a. Peter Martin, *China’s Civilian Army: The Making of Wolf Warrior Diplomacy* (Oxford University Press, 2021), 199.

b. *Ibid.*, 16.

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

Zhou Enlai: A Life

placed to tell this story, having previously published well-received books on Beijing's decision to enter the Korean War and PRC foreign policy under Mao.^a Chen is extraordinarily adept in utilizing Chinese sources, a skill on ample display in this, the most deeply researched and comprehensive English-language biography ever written on Zhou. His sources included material found in the Chinese Central Archive, the Foreign Ministry Archive, several provincial archives, numerous diplomatic papers of key CCP leaders, as well as selected Chinese-language works on Zhou, even including a compendium of his poetry.^b

Zhou Enlai, A Life is told chronologically in four parts: Zhou's early life; the Chinese Communist revolution; the early PRC; and the years, including the Cultural Revolution, leading up to Zhou's death in 1976. In judging Zhou's legacy, Chen finds a middle ground, somewhere between the CCP's official record that hails him as an exalted individual and scholarship that holds Zhou responsible for supporting the worst excesses of the Mao era. (5–7) In sum, Chen provides a nuanced treatment of Zhou.

Beginning with Zhou's early life in Huai'an, Chen positions Zhou in a traditional Chinese class in which classical education was expected of male children who would compete for official government positions. Zhou's mother and aunt instilled in him an appreciation for knowledge and Chinese traditions, and Chen writes that there was "always a place reserved in his mind for the teachings of the ancient Chinese sages that he learned in his childhood, even once he seemed to have wholeheartedly embraced Communist ideologies and revolutionary philosophies." (17)

In 1910, at the age of 13, and one year before the fall of the Qing Dynasty, Zhou went to live with an uncle in Northeast China. He never returned to Huai'an, spending the next decade studying and working in different parts of China before traveling to Japan and Europe. Living in Paris in the immediate aftermath of the 1917 Bolshevik Revolution made an impact on

Zhou, and it was there in 1922 that he wrote: "We should believe in the theory of Communism as well as the principles of class revolution and proletarian dictatorship." (59) Chen notes that Zhou's commitment to communism stemmed from his genuine feeling of shame over "China's backwardness" and his belief that national liberation was only achievable through revolution. Chen also notes that Zhou thought the "country's salvation should be associated with greater meanings and purposes," than those of capitalist and imperialist states. (60)

Zhou returned to China in 1924, meeting Mao for the first time and subsequently leading the CCP's clandestine operations in Shanghai from 1927 to 1931. There he earned the respect of party leaders as an individual who could run day-to-day intelligence operations. Of Zhou's time in Shanghai, Chen writes that "Zhou's control over the administrative power and intelligence network of the party, and then the party-state, would endure," and "although Zhou never became the paramount leader of the party, he consistently stood at the center of the party's operational network." (110) By 1943, Zhou made clear where he stood on Mao's leadership, publicly proclaiming that "Comrade Mao Zedong's direction is the direction of the Chinese Communist Party." (217) For Chen, Zhou's sincerity was unclear, but his statement supporting Mao "formed the basis on which Zhou was to work with Mao in the decades to come."

Following the CCP's victory in 1949 over Chiang Kai-shek's Guomindang forces, Zhou became both the PRC's premier and foreign minister, occupying a key role in Mao's inner-circle in leading the government and China's diplomacy—Zhou was central in negotiations with the Soviet Union in 1950 which secured \$300 million in loans for Beijing along with territorial concessions in Northeast China. (298). He and his wife, Deng Yingchao, moved into the Zhongnanhai leadership complex in Beijing along with Mao and other CCP leaders.

a. *China's Road to the Korean War: The Making of the Sino-American Confrontation* (Columbia University Press, 1995) and *Mao's China and the Cold War* (University of North Carolina Press, 2001).

b. Others who have used Chinese archival material as well include Rush Doshi, *The Long Game: China's Grand Strategy to Displace American Order*; Julian Gewirtz, *Never Turn Back: China and the Forbidden History of the 1980s*; Jeremy Friedman, *Shadow Cold War: The Sino-Soviet Competition for the Third World*. Gregg Brazinsky, *Winning the Third World: Sino-American Rivalry During the Cold War*.



Richard Nixon Library, February 21, 1972

In chapter 16, one of the book's most insightful, Chen meticulously recounts PRC diplomacy and strategy during the Korean War. Zhou oversaw China's involvement in Korea, meeting several times with Kim Il Sung and engaging with Moscow and Pyongyang as the conflict unfolded. Zhou also handled PRC diplomacy toward Vietnamese communists and their leader, Ho Chi Minh. After attending the Geneva Conference in 1954, it fell on Zhou's shoulders to convince Vietnamese communists to accept a negotiated settlement to end their war against the French. At a key meeting in Liuzhou, China, not far from the Vietnam border, Zhou delivered a detailed assessment of why it

was critical the Vietminh accept the deal, noting that an expanded conflict, like the one just stopped in Korea, served no one's purpose. Ho ultimately accepted Zhou's reasoning. (372) Zhou became a staunch advocate of supporting revolutions in Africa and Latin America. (492) With respect to Taiwan, Chen argues that Zhou played a role in softening Beijing's tone following a series of clashes in the mid-1950s. (418) However, a crisis in 1958, instigated by Mao, demonstrated just how much salience the issue had for CCP leaders.

Regarding domestic issues, which also fell into Zhou's sprawling portfolio, Chen paints Zhou as having a pragmatic side, while recognizing his need to stay in Mao's good graces. When Mao decided to rush Chinese economic development during the mid-1950s, Zhou initially cautioned against a "rash advance," drawing the chairman's ire. At a CCP National Congress in 1958, Mao chastised Zhou for "failing to get the bigger picture" and accused him of stoking divisions within the party. Sensing his political standing was faltering, Zhou took responsibility for his mistake of opposing a "rash advance," stating publicly that "as proven by China's revolution and reconstruction, Chairman Mao has represented the truth." (414) Within a year of this speech, Mao launched the disastrous Great Leap Forward. Chen credits Zhou's political sense for helping him navigate the tumultuous years of the Cultural Revolution (1966–76), when Mao sought to reinvigorate his control over the CCP by turning loose mobs of young party members (Red Guards) to attack individuals who had putatively lost their way and slipped back into capitalist and counterrevolutionary behavior. In Chen's view, Zhou understood the chaos Mao had unleashed and did what he could, at times, to protect colleagues and maintain "administrative and executive power" in the country. (574)

The last chapters of the book detail one of the most important periods of Zhou's career—managing détente with the United States in the 1970s. Zhou held secret meetings with Secretary of State Henry Kissinger in Beijing to lay the groundwork for President Richard Nixon's visit in February 1972 and succinctly set out the PRC's position on the most vexing question in the bilateral relationship: the status of Taiwan. In Chen's view, Zhou was shrewd and adept at taking

Zhou Enlai: A Life

on Mao's directives for what the PRC wanted to accomplish in any new relationship and articulating that vision to Kissinger. He could be pragmatic in one meeting with Kissinger and fiercely ideological in the next. Ultimately, Zhou and Mao were pleased with Washington's willingness to recognize "only one China and that Taiwan was part of China." (635) When President Nixon arrived in Beijing, Zhou's hand was the first he shook after disembarking Air Force One.

Zhou Enlai's approach to global affairs was based on a view that post-1949 China needed to act assertively to remedy a "century of humiliation" at the hands of Western powers. For those familiar with Beijing's

current thinking, that should sound familiar. While Zhou could be a shrewd and pragmatic diplomat, he was also a committed revolutionary whose ideology and sense of historical determinism influenced his foreign policymaking. For intelligence professionals, recognition of the CCP's complicated past and historical trajectory, from victors in the Chinese Civil War to rising power, is essential to understanding how Beijing approaches its place in the world today. Ultimately, Chen's book is as much a story of the CCP's rise and its influence on the Cold War and beyond as it is a profound biography of one of the PRC's founding leaders and most important diplomat. ■

intelligence in public media

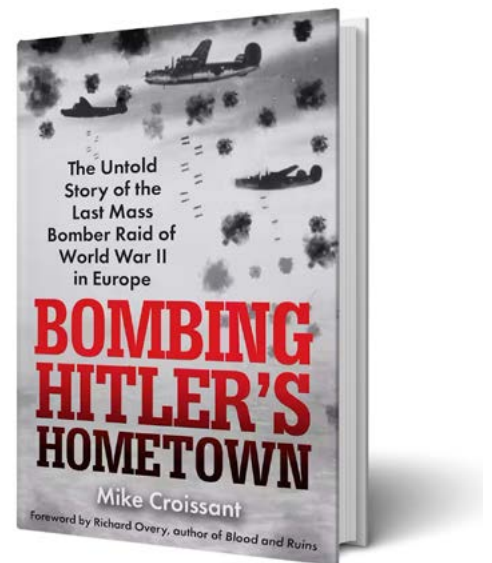
Bombing Hitler's Hometown The Untold Story of the Last Mass Bomber Raid of World War Two in Europe

Author *Mike Croissant*

Published By Citadel Press, 2024

Print Pages 352

Reviewer *David A. Welker*
is a member of CIA's History Staff.



Former CIA officer Mike Croissant has produced a highly readable account of the last massed US bombing raid over World War II's German Reich, which targeted Linz, Austria, on April 25, 1945—just two weeks before Germany would surrender. In some respects, this is a labor of love and remembrance of the author's uncle, who survived the raid only to perish with six other war veterans in an aircraft accident in Wisconsin just weeks after returning home. Yet it is much more than that, telling in considerable, page-turning detail how the Linz raid was prepared and executed, as well as its impact on the men who flew it, on Austrian civilians on the ground, and on the war's course. In doing so, Croissant has recorded a microhistory of a bombing raid that will be of enduring interest to readers of military history for years to come.

The author opens with the raid's origin and initial planning before backtracking to explain Adolph Hitler's youthful connection to Linz. In doing so, Croissant demonstrates that Linz and its inhabitants had no wider role in creating the dictator than did Austria or Germany during the early 1900s. Yet, protected for years from bombing raids by extensive air defenses, emplaced as a result of its connection to the fuhrer, by 1945 Linz's luck had run out.

Croissant's detailed telling of the experiences of the American fliers involved in the raid is some of the best prose of the widely explored air war genre. Numerous personal stories unfold rapidly but in a way that allows readers to easily juggle a considerable number of personalities and accounts. Giving background and details

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

Bombing Hitler's Hometown

derived from Croissant's own interviews—which offer a priceless record as the Greatest Generation fades into eternity—enables readers to quickly feel as if they know these men and in a small way come to share their suffering and sacrifice as they endure danger, fighting, and too often death. Another value of the book is in revealing the wartime experiences of several men who would later go on to fame, such as future senator and presidential candidate George McGovern and television producer Norman Lear.

Croissant's book also rightly highlights contributions of the under-appreciated B-24 Liberator heavy bomber, which is long overdue. Despite making major contributions to the US bombing campaign over Nazi Germany, the Liberator has too long flown in the shadow of the better known and much-heralded B-17.

Attention too is paid to Austrian civilians on the ground affected by the raid, another often-overlooked part of such bombing campaigns. The author nicely balances these depictions as neither wholly deserving Nazi targets nor as innocent victims, instead depicting both, as their individual actions suggest and caught amidst a global struggle.

One unusual note in the book is its detailed treatment of US fliers who fell into Soviet hands. Although most reached Soviet lines intentionally, because combat damage prevented their planes from returning to Italian bases, as Croissant shows in considerable, often-painful detail despite being allies, the Soviets were hardly friends of these desperate Americans. In fact, reaching Soviet lines was often as dangerous for them as falling into German hands. Accounts of Soviet wartime brutality are hardly new, but these stories should serve as a wakeup call for those few who remain blinded to Russia's painful reality.

Other unique post-raid personal accounts include those of fliers sent not to German Air Force-run POW stalags, but rather to infamously brutal SS-controlled

concentration camps. Like the accounts of Soviet treatment, these gripping, horrifying experiences will have readers blanching at their depiction of just how far our fellow humans can devolve into savagery. Yet these are stories we need to remember.

Because this is a military history, intelligence plays a background, supporting role throughout the book. However, late in the volume an officer of CIA's predecessor, the wartime Office of Strategic Services (OSS), makes an interesting starring turn, introduced as an unknown man whistling a few bars of Yankee Doodle while walking past the cell of crashed Linz raid flyers who had been sent to the Mauthausen concentration camp. The whistler was OSS officer Jack Taylor, whose presence in the hellish camp had come in a far more roundabout way than the captured airmen he was quietly reaching out to that day. The 33-year-old California orthodontist joined the Navy at the war's outbreak, but his prewar sailing experience quickly attracted the attention of the maritime component of the new OSS, and he was soon teaching small boat tactics and underwater demolition. Eventually he had logged 15 covert missions behind Axis lines on the Mediterranean coast. This experience led to his command of Operation DUPONT, a covert mission to gather intelligence about German defenses in southern Austria. The operation was a disaster from the start, and Taylor was captured and sent to Mauthausen for execution. He was spared that fate but suffered multiple beatings. His whimsical musical greeting lifted the spirits of prisoners and offered all the hope any of them would have until the US Army liberated them.

Bombing Hitler's Hometown in a broader sense tells the 15th Air Force's story, which has too long been eclipsed by the better-known, England-based 8th Air Force, as notably told in Donald L. Miller's recent *Masters of the Air* and the accompanying television series. Croissant's welcome work makes an excellent companion to that volume and reminds readers of the great sacrifices our forebears made during the war. ■

intelligence in public media

The Suicide Museum: A Novel

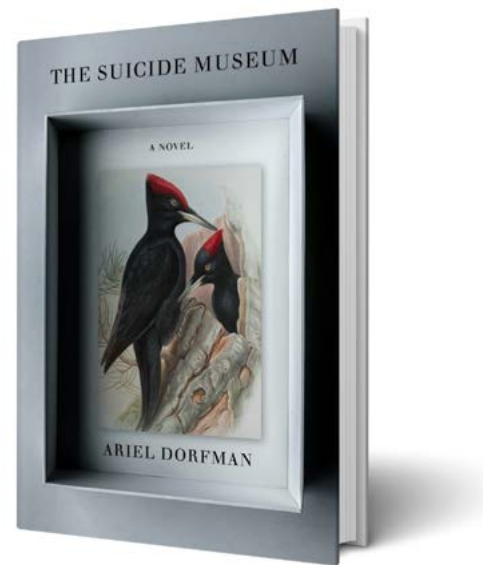
Author Ariel Dorfman

Published By Other Press, 2024

Print Pages 688

Reviewed By *Graham Alexander*

The reviewer is a CIA operations officer, writing in penname.



Chilean-American author Ariel Dorfman's semi-autobiographical novel, *The Suicide Museum*, is a curious work—one in which the boundaries between fiction and reality are not always apparent. Dorfman presents a seemingly first-person account of his investigation into the death of Chilean President Salvador Allende in September 1973 after a military-led coup (see box, next page). The book is difficult to categorize in other ways, too. *The Suicide Museum* is part political treatise, detective thriller, and biography with elements of espionage and historical fiction baked alongside for variety. Dorfman's habit of dwelling on certain themes and indulging in long digressions will occasionally test the patience of even committed readers. Still, his ability to craft highly readable prose in a story that is nothing if not original

makes *The Suicide Museum* worthwhile for connoisseurs of the Cold War and the circumstances surrounding Allende's ouster and death.

The Suicide Museum traces Dorfman's quest, commissioned by a fictional Dutch billionaire, to learn authoritatively how Allende died at the La Moneda Palace in Santiago, Chile, after military forces led by Augusto Pinochet staged a US-approved coup against him on September 11, 1973. This quest, however, does not follow a traditional arc in which the main characters enter stage right and the suspense builds toward climax and reveal. Dorfman dwells instead on meetings with his financial sponsor Joseph Hortha, Dorfman's wife and children, and even famous rock stars.

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

The Suicide Museum: A Novel

The reader is also treated to long passages regarding Dorfman's and Hortha's views on religion, death, the environment, and especially Salvador Allende. Dorfman frames Allende throughout *The Suicide Museum* as a kind of demigod who was destined to lead Chile into a vaguely defined state of political paradise if only malicious plotters had not foiled him. Dorfman does not mention that Allende won the presidency with roughly 36 percent of the vote in 1970, that he was hardly the paragon of morality in his private life, that he was working in cooperation with Cuban and Soviet intelligence to install a socialist system, and that Chile's economy collapsed under his administration. This is understandable, at least in an artistic and literary sense, because Allende is less a character than a symbol of the unrealized, still-beckoning left-wing political program toward which Dorfman, Hortha, and every other major character aspire. Unquestionably, however, those interested in a more evenhanded examination of Allende and Chile's history will be better served by other sources.

Dorfman's winding, nearly unpredictable plot development is made intelligible, even entertaining, by the clarity of his writing. *The Suicide Museum* stretches for nearly 700 pages but is easily digestible because of the novelist's talent for crafting sharp, memorable images with admirable economy. Only after 400 pages does the reader learn the meaning of the book's title but the description is both memorable and haunting – one that ties neatly with Dorfman's ongoing investigation into Allende's mysterious death.

Dorfman's habit of finding and then losing the plot is likely to test the patience of many but one that ultimately forces readers to read attentively through his random peregrinations. *The Suicide Museum* defies convention defiantly; near its conclusion Dorfman seems to solve the Allende mystery, only to change his verdict, and then change it again for reasons that are hard to fathom or follow. This is, as noted, not a traditional detective or espionage thriller. Alas, that may have been the point all along as both Dorfman and Hortha argue that the destination is the journey itself. Allende the saint, and not the man, serves at the conclusion of *The Suicide Mission* as the lodestar for Dorfman's political agenda: one with which readers

will have become familiar and can therefore assess on its own potential and merits. ■

**Excerpt from CIA Chief Historian
David Robarge's review of *Hostile
Intent: US Covert Operations in
Chile, 1964–1974*,
by Kristian Gustafson
(*Studies Vol. 52, No. 3, 2008*)**

Pinochet's death in December 2006 brought no closure to the long debate over CIA intervention in Chile and its legacy. The discussion essentially remains polarized between left and right, and for some time an objective narrative of the facts and a fair-minded analysis of the critical and apologetic perspectives have been sorely missed. Such is the landmark contribution of Kristian Gustafson's *Hostile Intent: U.S. Covert Operations in Chile, 1964–1974*, which must be considered the indispensable study in the large bibliography on that seemingly intractable subject. A former student of Professor Christopher Andrew's at Cambridge University and now a lecturer at Brunel University in England, Gustafson previewed some of his findings in this journal in 2003 [Vol. 47, No. 3]. In *Hostile Intent*, he demonstrates in an orderly and comprehensive way, with a good grasp of Chilean politics and full facility with the now substantial documentary record, how US administrations carried out their Chilean policy founded on the concern stated as early as 1958 by the senior State Department official responsible for Latin America that "were Allende to win we would be faced with a pro-Soviet, anti-U.S. administration in one of the most important countries in the hemisphere."

intelligence officer's bookshelf

Compiled and reviewed by Hayden Peake and other contributors

Memoirs

In True Face: A Woman's Life in the CIA Unmasked

by Jonna Mendez with Wyndham Wood
(Basic Books, 2024) 306 pages, index.

Jonna Mendez first came to public attention in 1999 when she was mentioned in her husband Tony's book *Master of Disguise*.^a Although she was a 27-year CIA veteran, readers gained only a glimpse of her career in that book. *In True Face* reveals an inspiring, atypical story of professional achievement in the world of espionage and a government that was "biased against women" in the workforce. (21)

Born Jonna Hiestand in 1945, in Wichita, Kansas, Jonna left Wichita State University to attend a friend's wedding in West Germany. After some European adventures, she married CIA officer John Goeser and joined CIA as a secretary, "the storied beginning of most CIA women." (45) She quickly encountered unexpected restrictions on her freedom. There was little she "could do without John's written permission or physical presence, including purchasing a movie ticket at the American theater." (20)

While adjusting to these restrictions, she became adept at CIA administrative procedures and was appointed a secretary in CIA's Technical Services Division (TSD) in Europe—the provider of espionage gear, or Q in James Bond's world—as a staff employee. Intrigued by the TSD mission, on returning to the States Mendez requested assignment to TSD headquarters, then located in the old OSS headquarters in Foggy Bottom, Washington. Still a secretary, Mendez sought advice about assignments in a professional track. She was informed that "the only way of moving up in that office was by getting an advanced degree in engineering, physics, chemistry, optics, or some other esoteric technical specialty." (50) Ability was not enough.

a. Anthony J. Mendez, *Master of Disguise: My Secret Life in the CIA* (William Morrow, 1999).

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

A defiant Mendez rejected this option, and *In True Face* she tells how the path she chose allowed her, after training at the Farm, to become an expert photo-operations officer. She would go on to acquire proficiency with secret writing, microdots, low-light-level video, and the use of sophisticated bugs, miniature cameras, covert communications systems, fake passports, and unusual undetectable disguises. (107) The latter ability led to her becoming aide to Tony Mendez, who ran CIA's Graphics and Identity Transformation Group. She would eventually rise to become chief of Disguise. (225) In that capacity, she was taken by then CIA Director Webster to the Oval Office, where she demonstrated how facial masks could conceal true identity to a surprised president.

In addition to the ever challenging operational assignments at home and overseas, Mendez dealt with several unanticipated milestones in the coming years. The first was the amicable end to her 23-year marriage to John. (239) The second, sometime later, was her marriage to Tony. And most unexpected of all, pregnancy at 47 and early retirement at 48. (255)

In True Face reveals an active retirement life that brought good and shockingly bad news. Among the good news was the excitement around *Argo*, the movie version of the CIA's role in helping several US Embassy personnel escape from Iran at the outset of the hostage crisis in 1979. The movie won the Academy Award for best picture in 2012. The bad news was the discovery that Tony had Parkinson's disease. Because the symptoms progress slowly, they maintained considerable activity, including making a presentation at a conference in Venice.

Since Tony's death in 2019, Jonna has pursued her love for photography and been involved with the International Spy Museum, in addition to writing her memoir in which she emphasizes two debatable points: the CIA is "still steeped in misogyny" (249) and "women make better operations officers than most men." (290)

An awe-inspiring contribution to the intelligence literature. ■

No Cloak, No Dagger: A Professor's Secret Life Inside the CIA

by Lester Paldy

(Rowman and Littlefield, 2024) 283 pages, index.

In 1984 Lester Paldy was one of a group of university professors that spent a day at CIA Headquarters learning about the agency so they could help, where appropriate, in "recruiting talented students for a variety of specialties." (6) The experience favorably impressed Paldy.

Still, four years later Paldy was surprised when CIA officer Arthur Hulnick contacted him to suggest he spend a year as a scholar in residence at CIA. (8) From CIA's perspective, Paldy was a good choice. He had been a Marine officer and a full professor (physics) at Stony Brook University, where he taught arms control and national security issues. He was also a member of the university's Arms Control and Peace Studies Center, editor of a college science teaching journal, and, most important, he enjoyed teaching physics to liberal arts majors.

No Cloak, No Dagger tells how Paldy persuaded Stony Brook to grant him a leave of absence and how, after completing standard new employee entry processing, he stretched his leave out to 25 years with CIA.

Expecting to work on arms control issues, Paldy was "disappointed when I realized my first assignment was going to be with the Center for the Study of Intelligence [CSI]." (11) After discussions with his superiors, he

was reassigned to the Arms Control Intelligence Staff (ACIS). Later he notes that "the Agency's journal, *Studies in Intelligence*, which anyone can access online ... represents an Agency effort to offer the public some measure of accountability." (82–83). The journal is produced in CSI.

Paldy mentions the types of work in which he was involved but never any specifics. For example, he was "part of a CIA team seeking ways to prevent the Soviets from cheating on their nuclear treaty commitments," and he later briefed senior officials and national laboratory directors on the outcome of the last negotiating round in Geneva. In neither case does he offer any details. (4) Likewise, he recounts frequent travels, commenting mostly on his accommodations but little about the reasons for his trips. During the latter part of his intelligence career, Paldy began lecturing on counterintelligence at the FBI Academy in Quantico, Virginia, but, again he offers no details on how the assignment came about or what his course looked like. (153) The pattern is repeated when he mentions teaching tradecraft to CIA scientists. (177)

Although Paldy describes his overall favorable impression of the agency and his work, he comments candidly on problems he observed. Examples include "weak diversity—women and minorities—too much bureaucracy, the use of torture and occasional weak leadership." (178) He comments that he "never attended a meeting where managers sought new ideas, welcomed departures from operational orthodoxy, or encouraged junior officers to take risks" are not detailed or documented. (251)

No Cloak, No Dagger presents an interesting view of CIA by an officer who worked hard to help his colleagues. He retired suspecting that "only a small percentage of my training efforts enabled case officers to recruit agents." (269) He doesn't explain how he reached that conclusion. ■

Biographies

Agent Link: The Spy Erased from History

by Raymond J. Batvinis

(Roman & Littlefield, 2024), 325 pages.

Sometime in 1934, William Weisband, a clerk working for the Waldorf Astoria Hotel in New York was recruited by the KGB and given the codename LINK. Fifteen

years later another KGB agent he turned him in to the FBI. Although his codename appeared in the VENONA traffic, he never spent a day in jail for his spying. Espionage historian and retired FBI special agent Raymond Batvinis tells this unusual counterintelligence story in *Agent Link*.

That Weisband was a KGB agent during World War II is not a revelation, but many details of his life and espionage operations have not been reported because his FBI, NSA, US Army, and KGB files were unavailable until recently. Some remain classified, but Batvinis acquired enough new material to provide a more thorough, although still incomplete, account of Weisman's life.

The files say he was born Wolfe Weisband in Alexandria, Egypt, on August 28, 1908, although later in life he would say he was born in Russia. His parents had emigrated to the United States to escape persecution there. In 1925, the family moved to New York City, where Wolfe soon became William. He would quickly become enamored of a libertine lifestyle in the city. Trying to support what became expensive habits, he took a series of clerical jobs in hotels. Batvinis estimates that during his six-year stint at the Waldorf Astoria, he began to work for the KGB, but exactly when and under what circumstances remains classified (or lost) in Russian files. Although Moscow's new agent had no technical expertise, Batvinis suggests he was just right for service as a courier. In any case, his immediate financial problems were solved.

Agent Link follows Weisband's courier and later agent-handling career in the 1930s and early 1940s, when he moved to California and began running agents, including Jones Orin York, who would betray him to the FBI after the war. Batvinis also describes Weisband's military career, which began when he was drafted into the US Army on September 1, 1942. Mainly because of his linguistic skills, he was eventually commissioned, sent to signal school at Ft. Monmouth, New Jersey, and then served overseas, all the while still serving as a KGB agent. Returning to the States in late 1944, he was assigned to Arlington Hall Station, where Army Signal Corps code-breaking was headquartered. It was there that he would do the most damage, translating what came to be called the VENONA messages and, of course, informing the KGB that its messages were being decoded. Batvinis stresses that Weisband didn't know to whom the traffic referred, since codenames were used. That revelation was provided by Kim Philby. Thus, Batvinis concludes, by 1949, "there was nothing that American code breakers were doing that Moscow didn't know." (253)

On February 2, 1948, after Meredith Gardner, the VENONA codebreaker, discovered that a KGB spy codenamed NEEDLE was Jones Orin York, Weisband's days were numbered. Batvinis describes what happened

after York identified LINK and why Weisband eventually served a year in jail for contempt of court. Once free, he had periodic, troubled contacts with the FBI and NSA as he tried to support his family. He died on May 14, 1967, with his wife Mabel and their children at his side.

Agent Link features an unusual literary style that gives the reader a broad view, not only of Weisband, but of the many intelligence officers and agents with whom he had direct and indirect contact. For example, in addressing the defection of GRU code clerk Igor Gouzenko, Batvinis provides a short biography of Gouzenko before addressing his impact on LINK. Likewise with Philby, Eliza-beth Bentley, Anatoli Golitsyn, Alexander Feklisov, and many FBI special agents.

Batvinis has provided a more comprehensive account of the William Weisband case. A welcome and valuable contribution. ■

Beverly Hills Spy: The Double-Agent War Hero Who Helped Japan Attack Pearl Harbor

by Ronald Drabkin

(William Morrow, 2024), 256 pages.

When author Ronald Drabkin was searching FBI files for material on his father, who had connections with US Army counterintelligence during World War II, he came upon references to Frederick Rutland, a former British pilot also known as Agent Shinkawa of the Imperial Japanese Navy. Shinkawa had lived well in exclusive Beverly Hills, California, and entertained celebrities of the day like Charlie Chaplin, Boris Karloff, Nigel Bruce, Amelia Earhart, Douglas Fairbanks, and the father of Yoko Ono. (4) His reporting as a Japanese agent had led to redesign of the aircraft carriers that carried out the Pearl Harbor attack and improvement of the famous Japanese fighter plane, the Zero.

Rutland's story takes an unexpected turn when he becomes a double agent for US Naval Intelligence. Anticipating the attack on Pearl Harbor, he informed the FBI, but he wasn't believed and, according to Drabkin, the FBI on Hoover's orders covered up his report. Returning to Britain after nine years in the United States, he reported to UK Naval Intelligence and was debriefed by its director and Ian Fleming. His request to return and spy on the Japanese in the United States and Mexico was denied.

Rutland is not the only spy featured in Drabkin's book. Cdr. Itaru Tachibana of the Imperial Japanese Navy was

very active in southern California and Mexico, and he had contacts with Rutland in Beverly Hills. Tachibana became controller of Toraichi Kono, formerly Charlie Chaplin's valet—whom Kono tried unsuccessfully to blackmail—and who in turn recruited an actor friend, Al Blake, to collect intelligence at Pearl Harbor for Japan. But Blake only pretended to cooperate, and he reported Kono and Tachibana to the Office of Naval Intelligence, which recruited Blake to report on his putative colleagues.

Drabkin's account of how these spies worked and interacted with US and British intelligence services is based on recently released FBI and MI5 files—none of which is cited! He does provide an interesting bibliography, but sorting out sources is a task left to the reader.

Although *Beverly Hills Spy* is well written and tells us about interesting pre-war operations, intelligence scholars will be disappointed. ■

The Eagle In The Mirror: In Search of War Hero, Master Spy and Alleged Traitor Charles Howard 'Dick' Ellis

by Jesse Fink

(Citadel Press, 2024) 319 pages, index.

A casual query from his father led Australian biographer Jesse Fink to examine the career of Charles Howard 'Dick' Ellis. He quickly discovered that Ellis was well known to some retired World War II intelligence officers and intelligence historians, though their assessments of his career differed in important ways.

There was agreement that Ellis was born in Australia on February 13, 1895, and died on July 5, 1975, in Eastbourne, England. He had enlisted in the British Army, was wounded in France, then was sent to officers' school before returning to the continent, where he was wounded again. After recuperating in England, he was assigned duties that involved Russia and soon learned the language. Eager to return to action, he joined the intelligence corps in Persia and Transcaspia where he learned Farsi and Urdu. He later added German, Turkish, Mandarin, and some Italian and Spanish to his linguistic skills. It is not surprising that after the war Britain's Secret Intelligence Service (MI6) recruited him.

In the interwar period, Ellis studied at Oxford—and briefly at the Sorbonne—then served MI6 in Geneva, where he wrote an impressive scholarly account of the origins of the League of Nations,^a while working undercover as a journalist.

In mid-1941, Ellis was sent to the United States. After Pearl Harbor, he joined the MI6 element in New York City, the British Security Coordination office headed by William Stephenson, as liaison to OSS. He returned to London in 1944 and began a series of important assignments in Western and Asian countries, including Australia, where he was involved with establishing their intelligence services. Although Fink provides no source, he notes that “Ellis personally sent George Blake, later exposed as a Soviet mole, to Seoul, Korea” as head of station (121) before retiring in 1953.

Then in 1979, Prime Minister Margaret Thatcher exposed Sir Anthony Blunt as a Soviet agent and left the impression that he was the only example of MI5 being involved in a case in which British secrets were provided to Britain's enemies. Retired MI5 officer Peter Wright disagreed and told his story in three books, one with journalist Chapman Pincher, a second with intelligence historian Nigel West, and a third his own, *SpyCatcher*, with Paul Greengrass.^b In short, Wright charged that Ellis, in need of money, had sold secrets to the Germans before the war and that he had confessed to MI5. Later, suspicions arose that he had also been working for the Soviets, allegations Ellis denied.

Fink challenges the assertions of espionage and those made by other publications and intelligence historians. He even suggest the possibility that Ellis was acting under MI6 orders. This approach is technically conceivable because no written confession has been produced; the charges were based on Wright's memory and “corroborated” to West by unnamed MI5 sources. Fink goes on to assert that Ellis's record of working “behind the scenes in some of the biggest conflicts and events of the 20th century,” including “the Japanese bombing of Pearl Harbor ... the creation of the Central Intelligence Agency and Kim Philby's defection,” (xvii) supports his innocence. But he cites no evidence Ellis was involved in these events.

Three other sources are worth remembering. *The Eagle In The Mirror* relies heavily on the questionable reasoning

a. C. Howard-Ellis, *The Origin, Structure and Working of the League of Nations* (George Allen & Unwin, 1928).

b. Chapman Pincher, *Their Trade Is Treachery* (Sidgwick & Jackson, 1981).

of William Stevenson, the discredited biographer of Sir William Stevenson. (198) CIA historian, Thomas Troy, who knew Ellis well, concluded that Ellis “was widely believed to have been both a Nazi and a Soviet agent.” (xvii) This author is also quoted as considering it likely but unproven that Ellis served both the Nazis and Soviets. (200)

Ellis was never charged with any offense. He died in 1975 at his home in England. Of necessity, Fink leaves readers uncertain of where Ellis placed loyalty, but he has provided a fine summary of a controversial case. ■

Ian Fleming: The Complete Man

by Nicholas Shakespeare
(Harper, 2023) 831 pages, index.

James Bond, or secret agent 007, is the avatar of the modern fictional spy hero. He may also be more widely known than his creator, Ian Fleming, even though many details of Bond's life were never reduced to paper. Not so with Fleming, who has been the subject of considerable literary scrutiny, including the 1966 biography by John Pearson and the more recent study focusing on his James Bond books, *Ian Fleming's Inspiration: The Truth Behind the Books*, by Edward Abel Smith.^b

Given this history, British biographer Nicholas Shakespeare's initial reluctance to accept an offer to write another biography of Fleming is understandable. But his doubt was based on a different reason: He didn't much like his subject. In fact he thought Fleming a “moody, harsh and withdrawn person, habitually rude and often cruel.” (xiv) And some of Fleming's friends felt similarly; “You're the epitome of the English cad” said one, and Fleming agreed. (xv)

But since he had not known the man himself, Shakespeare did his homework and, with the incentive of access to family papers not seen before, changed his mind. *Ian Fleming: The Complete Man* is the stunning result.

The story is presented in two parts. The first tells of Fleming's birth in London on May 28, 1908, his influential wealthy Scottish family and friends, his hobbies and troubled education, and failure to complete Eton and Sandhurst. He also started a lifelong rare-book collection and worked at journalism, publishing, and finance before his military service. The second part deals with his

postwar life including his marriage and the history of the James Bond books and movies. Several other topics are dealt with in both parts because they reflect his persistent personal idiosyncrasies, such as his dalliances, the real-life model for Bond, his friends and adversaries—many names came from friends—and some behavioral myths.

An example of the latter occurred when author Edward Abel Smith suggested Fleming left Eton—where he overlapped for a year with Guy Burgess—early because of a sexual encounter. Shakespeare cites a letter from Eton authorities stating that it is “entirely false to say that Ian was sent away from Eton for spending the night with a girl.” (77) That he did leave prematurely is clear and several reasons are discussed. Like Burgess, “[he] sported an Old Etonian tie all his life.” (56) Transferring to the military academy at Sandhurst, Fleming soon acquired a case of gonorrhoea and left on “his own accord.” (84) His older brother Peter graduated and served in the Special Operations Executive.

That Fleming joined the Office of Naval Intelligence is well known and Shakespeare explains how that happened. But he never makes clear why Fleming, with his lack of experience, achieved the position as the chief's principal assistant. That he performed well is not, however, in dispute, though sometimes surprising. For example, although a staff officer with no command authority, he managed to establish an operational “intelligence-gathering commando unit, 30AU.” (58)

Shakespeare also discusses the lingering controversy around Fleming's contributions to the formation of US intelligence organizations. He concludes: “The magnitude of his assistance to Donovan has been rated high by British authors” and historians who exaggerate [his] contribution. American historians view his efforts as minimal since Fleming had so little experience. Shakespeare concludes “the truth lies in between.” (279) Perhaps so, but no COI/OSS documents are cited that attribute key formative decisions to Fleming or other British officials.

After the war, Fleming moved to Jamaica where, according to Shakespeare, “the idea for Bond came to him as he swam in his bay.” (445) However, the writing of his Bond novels would not begin until he had married and spent several years at the *Sunday Times*, where he established a network of correspondent agents. He would

a. John Pearson, *The Life of Ian Fleming* (McGraw Hill, 1966).

b. See Hayden Peake's review in *Studies in Intelligence* 65, No. 4 (December 2021).

later write his only children's book, *Chitty Chitty Bang Bang*, for his son Casper. (617)

Then in 1952, Fleming began his first Bond novel, *Casino Royale*, and Shakespeare adds interesting background to its creation. For example, in the original typed version of the book, the main character was James Secretan. (115)

Fleming would write his 14 Bond novels during the next 12 years. None of the first five sold well in the UK or US in hardback, and Fleming came close to killing off Bond. Friends persuaded him to continue, and sales increased after Fleming's dinner with Senator John F. Kennedy, in which Fleming gave Kennedy "the benefit of his wartime experience in suggesting how to deal with Fidel Castro." (xxvi)

Interspersed with his literary efforts, Shakespeare writes, Fleming continued a colorful lifestyle that involved frequent travel, dealing with movie rights to his books, his encounter with the real Dr. James Bond, the author of bird books, and the influence of many famous people. The latter category includes Prime Minister Anthony Eden, Sean Connery, and the traitors, Guy Burgess and Donald Maclean, whom Shakespeare suggests provided "strong motivation when Ian created James Bond ... to repair the damage they had done." (403)

Ian Fleming: The Complete Man is the story of two men, one real, one fictional. The former became so well known before he died on August 12, 1964, at Canterbury, that "Question 12 of 24 in the 2020 test for British citizenship" is "Who first introduced James Bond?" Shakespeare has revealed much of his life story with all its complicated relationships. And he has shown how the iconic Bond has had a continuing impact on the world's culture and the image of secret espionage agents. A superb book by any measure. ■

The Spy Who Came In From The Circus: The Secret Life of Cyril Bertram Mills

by Christopher Andrew

(Biteback Publishing Ltd., 2024) 322 pages, index.

He is not mentioned in J. C. Masterman's precedent-setting 1972 book, *The Double Cross System*, although he was part of the operation. In 1982, intelligence historian Nigel West noted only that he was the MI5 representative in Canada in 1945.^b Then in Juan Pujol's 1985 wartime memoir, *GARBO*,^c came the startling news that Cyril Mills had been GARBO's first case officer. Little new appeared in print about Mills until the publication of *Stars & Spies* in 2021 by Christopher Andrew and Julius Green.^d But Professor Andrew wasn't stopping there. *The Spy Who Came In From The Circus* completes the story.

Cyril Mills, the son of Betram Mills—founder of the popular Bertram Mills Circus—was educated at Harrow and Cambridge (Corpus Christi), which he entered in 1920. Andrew proudly notes that Mills followed the footsteps of Corpus Christi's first spy, Christopher Marlowe.

After graduating Cambridge with honors in engineering, Mills studied oil refining in the United States and Burma, where he also acquired acts for the circus he would take over on the death of his father. The circus was a hit in Europe and the United States, and Mills used it to develop friendships with notables such as Winston Churchill.

Andrew explains how his circus work in Europe led to Mills' work for both MI6 and MI5. Mills found it easier to fly and soon earned his license and bought a plane. Flying over Germany in the late 1930s, he noticed airfield construction that exceeded civilian requirements. Using his university connections, he reported his observations to MI6; MI5 was alert to the chance that Mills was a German provocateur. Eventually convinced Mills was loyal, they continued to accept his reporting until the phony war ended. Too old to be a bomber pilot, Mills went to work for MI5 and joined the Double Cross operation.

After working with several double agents, Mills was posted to Canada in December 1942 and put in charge of

a. J. C. Masterman, *The Double Cross System in the War from 1939-1945* (New Haven CT: Yale University Press, 1972).

b. Nigel West, *A Matter of Trust: MI5 1945-1972* (Weidenfeld & Nicolson, 1982), 26.

c. Juan Pujol with Nigel West, *GARBO: The Personal Story of the Most Successful Double Agent Ever* (Weidenfeld & Nicolson, 1985).

d. Christopher Andrew and Julius Green, *Stars & Spies: Intelligence Operations and the Entertainment Business* (The Bodley Head, 2021), 268-69.

the Double-Cross System there. He had frequent contact with William Stephenson and his British Security Coordination operation in New York, and Andrew makes it very clear that Mills's view of Stephenson and his friend William Donovan of OSS was "uncharacteristically, ungenerous." (152)

Mills was also very critical of how the RCMP handled espionage cases and early in the Cold War considered MI6 "a ghastly mess as a result of the stupidity and incompetence of Menzies," its chief at the time. (220) He did allow that things improved after his close friend Dick White took over.

Mills' career as MI5 representative in North America ended at the end of August 1945, and he returned to London. While resuming his circus business, he continued working parttime for both MI5 and M6 during much of the Cold War. For 15 years he maintained a home across from the Soviet Embassy that allowed the British to monitor KGB/GRU comings and goings. The value of the operation is in question as the Soviets were aware of his role.

The Spy Who Came In From The Circus presents much that is new about Cyril Mills' intelligence career and in several instances raises doubts. One concerns Mills' claim to have recruited GARBO. (274) Andrew writes on page 131 that "they recruited him as a double agent codenamed BOVRIL" in Europe. (131) Mills did not go to Europe. GARBO met him as "Mr. Grey" after he arrived in England. (132) And the statement that the Abwehr codenamed Pujol ARABEL (131) is incorrect; that was the name of the network. More generally, Andrew refers to B "Branch" throughout, as he did in his official history of MI5, but according to the Liddell diaries the correct term was "Division" until Dick White became director.

Mills kept his intelligence work secret even from his family for most of his career. But late in his life circumstances changed, and MI5's existence was publicly acknowledged, allowing Mills to meet with former colleagues for reunions. Cyril Mills died, aged 89, on July 20, 1991. Chris Andrew has made sure his contributions will be remembered. ■

Histories

The British and American Intelligence Divisions in Occupied Germany, 1945–1955: A Secret System of Rule

by Luke Daly-Groves

(Palgrave Macmillan, 2023) 398 pages, index.

This review contains a substantial contribution from US Army Intelligence Historian Thomas Boghardt.

When Luke Daly-Groves began his PhD program at the University of Leeds, his thesis topic concerned Anglo-American intelligence rivalry surrounding the employment of ex-Nazis in postwar West Germany. As his research progressed, he encountered occasional references to an "Intelligence Division" (ID) accompanied by little or no further comment. Intrigued, he turned to US and British national archives and discovered extensive ID files that filled a large historiographical gap. He then changed his thesis topic, and this book is the result.

The IDs, as he calls them, refer to the British and US Intelligence Divisions of their respective military headquarters in West Germany. Their primary mission, Daly-Groves contends, was Anglo-American intelligence liaison in occupied Germany. He writes that

despite at times being larger than more well-known and studied intelligence organisations such as MI5, MI6 and the CIA, the IDs have hitherto remained one of the most secret and misunderstood elements of even the secret histories of America, Britain and Germany. (4)

The IDs were staff organizations, not operational elements, and this distinction largely accounts for historians having paid them little attention. Daly-Groves does not seem to recognize the difference. He implies the IDs had operational or command (318) functions as he discusses their liaison work in five key areas: military, scientific, security, political, and state-building intelligence. In fact, much of the operational work in these areas was carried out by subordinate field agencies, such as the US Army's Counter Intelligence Corps. Daly-Groves references CIC operations and records throughout the book but does so without clarifying the CIC's relationship to the ID.

Although Daly-Groves affirmatively and repeatedly asserts the IDs played a "crucially important role" in the occupation of Germany, (13) he provides few specifics. He does show they produced influential finished intelligence based on input from various national operational

organizations such as the CIC and then CIA, MI6, and MI5. But his evidence indicates they analyzed and often shared their results, which others used.

A key feature of the IDs relationship, according to Daly-Groves, was the “junior” status of the Americans and their “dependence” on the British (86, 103, 120, 256, 260). The notion of “British brain” vs. “American brawn” goes back to the pioneering work of British codebreakers in World War II. It gained traction and came to encompass intelligence at large during in the early Cold War, as Britain sought to compensate for imperial decline by hewing closely to the United States and emphasizing a “special relationship” between the two nations. But if anything, a careful reading of the evidence in postwar Germany suggests a rather different dynamic.

For example, Daly-Groves maintains that the British stole a march on the Americans by selecting the pro-British Otto John as the first director of the West German security service, the Bundesamt für Verfassungsschutz (BfV). That John, an anti-Nazi who had fled to Britain in 1944, was London’s man rather than Washington’s, is true as far as it goes. Left unsaid is that the Americans had already installed their own candidate, Reinhard Gehlen, as head of the far more powerful West German foreign intelligence service—the Gehlen Organization or Bundesnachrichtendienst—and ceded the directorship of the minuscule BfV to the British as a sop. Only in passing does Daly-Groves mention John’s defection to East Berlin in 1953, leaving the BfV in shambles. What this says about the British wisdom of choosing John in the first place is not discussed.^a

A similar pattern emerges in the career of Konrad Adenauer, the first chancellor of West Germany. Identified by US intelligence as a potentially valuable postwar ally, the US military government appointed him mayor of liberated Cologne in 1945. The British promptly deposed him when they assumed control of the city as part of their occupation zone. Adenauer never forgot this slight. For the duration of his chancellorship from 1949 to 1963, he aligned West Germany with the United States and kept London at arm’s length.

This “unparalleled example of Occupational buffoonery,” as a British official quoted by Daly-Groves aptly called it, (294) casts British decisionmaking—and the intelligence that informed it—in a dim light. In view of these and

other blunders, it is hard to disagree with the assessment of British intelligence historian Stephen Dorril that the “British were often out-gunned and outclassed by the Americans” in postwar Germany.

The insignificance of Berlin, as compared to West Germany, as an intelligence center constitutes another central theme of the book. But here too the evidence is shaky. While the IDs were headquartered in West Germany and operated a sprawling apparatus in their respective zones, Berlin occupied a unique position, located as it was deep inside the Soviet Zone. The Berlin blockade of 1948–49; the closure of the intra-German border in 1952; the 1953 uprising in East Berlin; espionage, counterespionage, and signals intelligence operations across the sectoral borders; and the work of the US and British military liaison missions in Potsdam constitute key features of early Cold War intelligence. Notably, Daly-Groves references them only in passing. The fact that fewer British intelligence officers operated in Berlin than in West Germany *as a whole*, can hardly be taken as evidence of the city’s irrelevance to intelligence, as the author argues. (324)

Daly-Groves’ treatment of the IDs discusses their many sub-elements, which often had confusing designations. He tends to overwhelm the reader with acronyms, at times cramming over a dozen into a single paragraph, (198) and he does not always seem to grasp their meaning: For example, he frequently refers to the “DAD,” an initialism spelled out in a list of abbreviations as “Department of the Army Detachment.” But the list fails to add that this designation served as a cover name for CIA, leaving the reader with the impression that the DAD was simply another Army field agency. (xvii) The organizational charts may or may not be helpful in sorting out individual agencies and their relationships to each other. (45–47)

The author conducted extensive archival research, but his sources are sometimes hard to trace. For example, on page 219, footnote 329, he lists: “NARA II, RG 319, UD1075, Box 28, 26861603, Typed Notes, ‘Germany, 1948-1949,’ Undated.” But the listed NARA reference refers to a file unit (folder ‘agents’) and not a series. Surely, the cited document exists somewhere, but it could not be found in the place indicated.

Daly-Groves somewhat selectively covers the works of other scholars. Thomas Boghardt’s book on Army Intel-

a. Daly-Groves does not cite the standard works by Michael Wala on the early years of the BfV and John’s defection: *Keine neue Gestapo* (2015) and *Otto John: Patriot oder Verräter* (2019).

ligence in postwar Germany, *Covert Legions*, is cited for the most part only in support of the author's own theses. Paul Maddrell's work on Allied intelligence exploitation in postwar Germany comes in for harsh criticism for supposedly overemphasizing this aspect of Allied intelligence over other areas. (122, 255, 315–320) Publications that directly contradict the author's findings are sometimes ignored altogether, as is the case with Sarah Douglas's masterful deconstruction of the self-aggrandizing account of the British intelligence officer and later historian Hugh Trevor-Roper, one of the "heroes" of Daly-Groves's narrative.

Overall, *The British and American Intelligence Divisions in Occupied Germany* is a mixed bag. Daly-Groves has indeed written a comprehensive history of the Intelligence Divisions, but he has not shown that they operated "a secret system of rule that was the real backbone of the occupation of Germany." (2) That credit must be shared with their headquarters, the field agencies, and military government. ■

Eyes On The Enemy: U.S. Military Intelligence in World War II

by Chris McNab
(Casement, 2023) 198 pages.

In *Eyes On The Enemy*, military historian Chris McNab, author of many books on weapon systems and military campaigns, has turned his attention to US military intelligence prior to and during World War II.

McNab's approach to this rather imposing task is straight forward and inadequate. He first reviews the circumstances facing the Army, Navy, and OSS intelligence organizations before the war, resulting in the Pearly Harbor surprise. Unfortunately this includes a description of the MAGIC codebreaking machine that confuses it with the PURPLE decoded traffic it produced. While his primary "focus is on combat intelligence," he does comment on intelligence support to special intelligence missions in Europe and the Pacific. (x)

The balance of *Eyes On The Enemy* is presented in five chapters that discuss (1) organizations, objectives and training; (2) combat and human intelligence; (3) signals and cryptography; (4) aerial and naval reconnaissance; and (5) intelligence and counterintelligence. McNab introduces each chapter with explanatory comments, but most of the text consists of extracts from Army field manuals published during the war. These manuals present the military way of accomplishing missions and, as any former intelligence officer knows, are of little direct use in the field, where each command has its own way of accomplishing its mission. Thus *Eyes On The Enemy* comments on what needs to be done, but gives no examples of how the problems are solved in practice. This omission and the absence of source notes and an index seriously weaken the value of the book, although it may be of use to someone unfamiliar with the subject. ■

Non-US Intelligence

Lifting The Fog: The Secret History of the Dutch Defense Intelligence and Security Service (1912–2022)

by Bob de Graaff
(Rowman & Littlefield, 2024) 637 pages.

The Dutch Military Intelligence and Security Service (*Militaire Inlichtingen-en Veiligheidsdienst* (MIVD)), created in 2002, is the new name for the Military Intelligence Service (MID that consolidated the intelligence services of the Army, Navy and Air Force. In 2019, the Utrecht University professor of intelligence and security studies, Bob de Graaff, was asked by the Netherlands Institute for Military History (*Nederlands Instituut voor Militaire Historie*, NIMH) to write the history of the MIVD and its predecessor organizations. The book would cover the institutional development of the military intelligence

services since the establishment of their foundational organization, the Studiebureau Vreemde Legers ("foreign armies research office") in 1912. De Graaff was granted "unfettered access to the service's archives," although not everything he discovered could be published. *Lifting The Fog* presents his results in chronological form, supplemented by case studies and suggestions for MIVD's future.

Because the Netherlands remained neutral during World War I, military intelligence focused on the security needs of the individual services and progressed little from its 1912 origins. This created a significant gap between the other European nations, and de Graaff recounts how the Dutch corrected the imbalance as the interwar world situation worsened.

A detailed case study of the Venlo Incident^a from the Dutch point of view, illustrates how in 1939 the Dutch had developed a flawed intelligence liaison relationship with MI6. (49) De Graaff's account includes some names not previously associated with the case and adds documentary support to the view that the Abwehr, not the SS/SD under Walter Schellenberg, was the originator of the plot to kidnap the two MI6 officers, as often reported. (33)

De Graaff tells how during the war the Dutch government, then in exile in London, formed a resistance organization to conduct operations in the Netherlands. A Bureau of Intelligence (*Bureau Inlichtingen*, BI) was created under the Minister of War in the government-in-exile that coordinated all Dutch intelligence contacts with MI6—but not SOE, to which, despite Dutch reticence, agents were seconded for training and dispatched to the Netherlands. In what came to be known as Operation Englandspiel, the Germans compromised the operation for two years and nearly 50 men were lost. Lesson learned: always control your own agents. (56)

After the war, the Dutch reevaluated their intelligence threat. In de Graaff's discussion of the issue he notes—without explanation—that “CIA had largely overlooked the threat of a nuclear war.” (129) He does admit the nuclear threat was not of great concern to Dutch intelligence until 1983, but he never clarifies what is an obvious error.

During the Cold War the Dutch military intelligence agencies gained considerable experience in counterintelligence operations involving the Soviets and Warsaw Pact nations, and de Graaff deals with them in some detail. (385) Of particular interest is the assistance the Dutch rendered when the Polish CIA agent Ryszard Kuklinski made contact with Dutch Army intelligence. (136)

De Graaff describes Dutch efforts after the Cold War to refine their intelligence program. He devotes a chapter to the role the services played in the fall of Srebrenica, emphasizing its long-term impact on the military intelligence process in the Netherlands. (263) Although MIVD was never intended as a major source of intelligence for NATO ground forces, de Graaff makes a strong case for its international successes—especially in the areas of

HUMINT, SIGINT, and cyber, where *Lifting the Fog* demonstrates MIVD punches above its weight.

MIVD's vision for the future assumes a situation of “fundamental uncertainty,” in which early warning is an important mission, particularly in the cyber domain. (419) More generally, de Graaff suggests the need “for an overarching philosophy of military intelligence that not only can be a starting point” but adapts well to political and security demands while shifting from “need to know ... to the “need to share, and from early warning to early action.”

Lifting The Fog is a thoroughly documented account of an impressive intelligence service—though the lack of an index is annoying—and a major contribution to the intelligence literature. ■

In the Labyrinth of the KGB: Ukraine's Intelligentsia in the 1960s–1970s

by Olga Bertelsen

(Lexington Books, 2022) 370 pages.

After practicing medicine and dental surgery in Ukraine, Dr. Olga Bertelsen earned a PhD at the University of Nottingham—where she focused on Soviet/Russian history and intelligence. She went on to teach and study at several US universities. She is currently an associate professor of global security and intelligence at Tiffin University in Ohio.

In the Labyrinth of the KGB is the story of the Kharkiv intelligentsia, multiethnic writers who after Khrushchev's 1956 secret speech revealing the true Stalin, explored the limits of free expression. Bertelsen uses the “labyrinth” to refer to the many paths of expression writers attempted to pursue only to be blocked by the KGB in the 1960s and 1970s.

This opposition to free expression was not new. As Bertelsen shows, attempts to eradicate Ukrainian nationalism and Zionism, its two major targets, had a long history under Stalin. Ukrainians took what came to be called the “Khrushchev Thaw” after de-Stalinization as an opportunity to revive their national culture and consciousness, but the Soviets viewed this as a threat to national identity. By the second half of 1958, the crippling reality of re-Stalinization had set in.

a. Two British Secret Intelligence Service (SIS) agents were abducted on the outskirts of Venlo, the Netherlands, on November 9, 1939. The incident was later used by the German Nazi government to link Britain to an attempted assassination of Hitler on November 8, 1939, and to help justify Germany's invasion of the Netherlands, while a neutral country, on May 10, 1940.

Bertelsen gives examples, as told by the Kharkiv writers themselves, about how they were forced to comply with KGB rules that left no space for artistic or creative expression on particular matters. The topic of the *Holodomor*, the Stalin enforced famine in Ukraine during 1932–33, is a good illustration. Official opposition to treatment of this topic was well known and yet the authors found ways of mentioning it. Among other responses, the KGB resorted to what Bertelsen calls “memorycide” and “burning approximately 600,000 volumes of ancient prints, rare books, and manuscripts.” (204)

Most of the time, Bertelsen uses the term “local” KGB or just KGB to identify those trying to enforce policies, but she notes that in July 1967,

The KGB created special counterintelligence departments to combat the ideological sabotage.... The Fifth Directorate and its subordinate departments were charged with the mission to conduct surveillance of the most active dissidents or individuals who attracted the KGB's attention by their nonconformist behavior. Each Fifth Chief Directorate operative used seven to 10 informers who methodically listened to the writers' conversations in cultural institutions, the Writers' Union, and its literary sections, conveying their content to their handlers. (30)

In the Labyrinth of the KGB is based largely on interviews with surviving authors and KGB operational documents found in the central (Kyiv) Security Services archives (former KGB archives) in Ukraine. They document the story of Kharkiv writers who endured the policies and penalties implemented by an authoritarian regime and forecast what is likely to occur if the current Russian government is successful in Ukraine. ■

The Russian FSB: A Concise History of the Federal Security Service

by Kevin Riehle

(Georgetown Univ. Press, 2024), 197 pages.

The acronym “KGB” was consigned to history with the demise of the Soviet Union on December 26, 1991. The security and intelligence functions it performed were not. Retired US intelligence analyst Kevin Riehle, a lecturer in intelligence and security studies at Brunel University in London, has written an excellent account of the struggles of the Russian Federation to create intelligence successor organizations.

The Russian FSB begins with a capsule history of Russian security elements and their frequently changed

names from tsarist times to the present. Some missions changed over time, but one did not: protect the “tsar.” (7)

In the early 1990s, a number of new security organizations were created, each quickly succeeded by variants until the reorganization in 1995 when the Federal Security Service (FSB) officially founded. At first glance, it resembled the old KGB because it absorbed three of the KGB's four main directorates. Only the KGB's First Chief Directorate, responsible for foreign intelligence remained independent of the FSB; that was the Foreign Intelligence Service (SVR).

In practice much had changed. The FSB was given expanded responsibilities in law enforcement, intelligence collection—including HUMINT—covert action, and border security in Russia, along with the authority to operate in the former Soviet republics, especially for counterterrorism liaison purposes. Riehle concludes that this makes the FSB Russia's “primary clandestine service within the former Soviet space.” (2) FSB authority increased further in 2003 and 2004, when the SIGINT elements and border guards directorate were subordinated to the FSB. Since then, the FSB has been Russia's foremost security and intelligence service.

Riehle describes the new organization, its functions and leadership, especially its dependence on President Putin. He suggests the FSB was at least partially responsible for an erroneous assessment that a quick victory could be achieved in Ukraine—a conclusion that took a toll on the leadership and trust. (157) Although less is known about personnel issues, training, assassinations, and digital warfare elements, Riehle mentions them while acknowledging source limitations. His main Russian sources—Agentura.ru and the Dossier Center—are posted by Russians living in the West. He does rely on Russian media for information on FSB corruption, which has gotten ample attention.

The FSB has made many enemies within the Russian ruling elite and society. The former from current practices discussed in the book, the latter from the fearful burden of the KGB's second chief directorate, whose legacy of domestic counterintelligence and the gulag is not forgotten. *The Russian FSB* sees little hope for improvement in the Putin era. A valuable contribution to the intelligence literature. ■

