Revisiting a Question Asked in 2009

What Are We Talking About *Now*, When We Talk About Counterintelligence?

John Ehrman

> *No better lesson than the Dreyfus Affair will ever be shown to the people; they have to make the effort to distinguish between liars and truthful men. They have to read, question, compare, verify, think.—Georges Clemenceau*[1]

"This essay is only a start for the work of developing a robust theory of counterintelligence," I wrote at the end of "What Are We Talking About When We Talk About Counterintelligence?" in the June 2009 issue (Vol. 53, No. 2) of this journal. Almost as soon as the article appeared, however, I began to have doubts about it. Was it a weaker starting point to understanding counterintelligence (CI) than I had hoped? What might I have gotten wrong or ought to have said differently? But, I decided, what's done is done. I went on with other projects and didn't think about the article again for years.

What were we talking about when we talked about counterintelligence in 2009?

My goal in "What Are We Talking About When We Talk About Counterintelligence?" was to help plug a gap—the absence of a common understanding of what CI is—that I viewed as greatly reducing the effectiveness of US counterintelligence efforts. I started with a definition of CI, calling it the study of the organization and behavior of intelligence services. I went on to describe the different types of intelligence services we considered at the time. I emphasized that counterintelligence is almost always an analytical task that requires a deep understanding of the culture, operations, and structure of a target service. I further described these elements in four main points.

- To understand a service means knowing its history and the political and legal frameworks in which it operates, as those define its missions.
- Intelligence services are subject to political forces in their nations, but they are not passive. While acted upon, they also work to protect and advance their interests and are thus involved in complex political maneuvering.
- Services are insular and conservative, and they are often badly managed. They generally do not learn from their mistakes, leading to predictable behaviors.
- CI operations are more than just spy hunting. They can become exceptionally complex, and when they do, CI analysts especially need know the histories and behavioral patterns of the subject service or services.

What is Different in CI Today?

The CI world is not static, however, and around 2020 I began to wonder how it might have changed since 2009. Much remains the same, but the social, technological, and political contexts in which CI is situated—the understanding of which I argued is critical to the work—was by then going through a series of changes as great as any in the past. Simultaneously, legal and geostrategic shifts, the spread of collection methods hitherto available only to the services of major powers, the rise of social media, introduction of ubiquitous private and public surveillance systems, privatization of intelligence work, and the dependence of state services on new generations of employees with outlooks vastly different than those of their predecessors were driving profound shifts in counterintelligence.

It is with these developments in mind that I believe the time has come to look at the original article and ask, 15 years on, what are we talking about *now*, when we talk about counterintelligence?

The Original Article and Its Impact

"What Are We Talking About" began to take shape around 2007 as a few handwritten notes I had

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.

penned to myself. Essentially, these were observations on the work my colleagues and I in Central Eurasia Division and the Counterintelligence Center of CIA carried out daily at the time. After a while I copied them to a whiteboard and discussed them with people who came by my office. Some months went by, and I started to think of turning them into a *Studies* article. After several more months of research and writing, I sent the draft to the managing editor at the time, who presented it to the *Studies* Editorial Board for approval, which it granted. Some members, however, were reluctant to approve it. “It might be too much of a primer,” “not sophisticated enough” were the concerns.

Primer or not, “What Are We Talking About” seems to have filled a niche. Soon after publication, it began to find its way into the syllabi of intelligence courses, first internally at CIA and then into university classes. It also found its way into anthologies; I was once told the article soon became the most reproduced *Studies* article ever. More important, it seems to have succeeded in its goal of stimulating further academic and theoretical discussions of CI, especially in the context of nonstate actors, cybersecurity, and comparative studies. (See text box.)

Some of these works can be long and abstract—what, exactly, is a “syncretic spy” or a “counterintelligence threat ontology”?[2]—but they have done much to expand CI studies beyond the traditional focus on the United States, Britain, Russia, and China. I certainly can’t claim credit for this surge in CI research, but I like to think that “What Are We Talking About” had something to do with it.

An Extended and Elevated Discussion

Academic writings on aspects of counterintelligence theory, both general and specific, seem to have taken off around 2010. Below is a small sample of articles and longer works, broken down by category.

General

- Miron Varouhakis, “An Institution-Level Theoretical Approach for Counterintelligence,” *International Journal of Intelligence and Counter-Intelligence* (*IJIC*) 24, no. 3 (2011);
- Henry Prunckun, “Extending the Theoretical Structure of Intelligence to Counterintelligence,” *Salus Journal* 2, no. 2 (2014).

CI and nonstate actors

- Gaetano Joe Ilardi, “Irish Republican Army Counterintelligence,” *IJIC* 23, no. 1 (2010);
- Carl Wege, “Hizbollah’s Counterintelligence Apparatus,” *IJIC* 25, no. 4 (2012);
- John Gentry, “Toward a Theory of Non–State Actors’ Intelligence,” *Intelligence and National Security* 34, no. 4 (2019);
- Blake Mobley and Carl Wege, “Counterintelligence Vetting Techniques Compared Across Multiple Domains,” *IJIC* 34, no. 4 (2021).

CI and Cybersecurity

- Daniel Boawn, “Cyber Counterintelligence, Defending the United States’ Information Technology and Communications Critical Infrastructure from Chinese Threats,” Utica College, Master’s Thesis, 2014;
- John Gaitan, “Strategic Counterintelligence: An Approach to Engaging Security Threats to American Security,” Johns Hopkins University, Master’s Thesis, 2017;
- Neil Ashdown, “How Commercial cyber threat intelligence practitioners talk about intelligence and counterintelligence,” https://pure.royalholloway.ac.uk/ws/portalfiles/portal/40090891/CTI_and_Counterintelligence_Ashdown_Aug20.pdf (2020).
- John Gentry, “Cyber Intelligence: Strategic Warning is Possible,” *IJIC* 36, no. 3 (2023);

Comparative Studies

- Philip Davies and Kristian Gustafson, eds., *Intelligence Elsewhere* (Georgetown University Press, 2013);
- Ryan Shaffer, ed., *The Handbook of Asian Intelligence Cultures* (Rowman & Littlefield, 2022);
- Shaffer, ed., *The Handbook of African Intelligence Cultures* (Rowman & Littlefield, 2022).

What I might Have Said Differently

Reading the article today, I am more than satisfied with how it has held up. The definition of CI that I offered—“the study of the organization and behavior of the intelligence services of foreign states and entities and the application of the resulting knowledge”—may be a little awkward, but it captures the need for a broad view of CI, one that includes asset vetting, spy-hunting, penetration of hostile services, reporting, and likely a dozen or more additional functions. It also makes clear the centrality of analysis in CI work—operations, to be sure, are vital, but analysis is critical.

Preparation for a CI position.

Consistent with this, I focused on a point that, in retrospect, I ought to have emphasized even more. Generalized CI training for new CIA operational and analytical officers, I argued, is useful but inadequate for people expected to staff CI positions effectively. In the long run, CI officers will require a great deal more depth and breadth of expertise to be successful.

An officer's expertise needs to start with an understanding of his target country's CI history—that is, the record of its services' operations and methods as well as where they fit in the country's or entity's political and social history. After all, can anyone do effective CI work on Russia without knowing of Moscow's long record—from the Okhrana in the 1880s to the Foreign Intelligence Service (SVR) today—of deception and misinformation, illegals and provocations, or how Dzerzhinskiy set up the Cheka and ran its operations against anti-Bolshevik exiles? Can an analyst understand the behavior of German intelligence in 2023 without knowing the histories of the Gestapo and Stasi? Whether it is Russia, Germany, Israel, Hizbollah, or any other entity, only with an understanding of such backgrounds is an analyst or collector in a position to work on a given CI account.

Challenges of Filling CI Positions

Stemming from this is another point I made and to which I ought to have paid more attention, the difficulty of finding people to do counterintelligence work. Staffing, in fact may be the most difficult problem in CI. When intelligence services need to hire area experts, economists, engineers, or any number of other specialists, they can turn to universities or other government departments to find pools of candidates. But few schools, especially among the prominent universities where intelligence services focus their hiring efforts, teach intelligence as a discipline and, even within these programs, CI is usually but one or two class sessions in a general course on intelligence. Services are left to look for CI candidates within the general hiring pool or among current staff officers, and then teach them the specialized skills they will need.

Learning the craft of counterintelligence takes a long time, however. I believe aspiring CI officers must first learn the practical work of intelligence, which takes several years of job experience, before starting in counterintelligence. In my observation, new hires assigned directly to CI tend to become overwhelmed and soon transfer to work in the areas of their academic training. Once in a CI position, it takes anywhere from one to five years, depending on the specialty, to achieve a working knowledge. Even then, CI officers must be conscious of how much they still do not know and the need to continue learning.

The difficulty of staffing CI units often forces services, including CIA, to assign nonspecialists to CI positions. This practice has some benefits, including giving officers experience in CI work while providing much–needed manpower to CI components; these officers then can apply their newly learned skills in future assignments. Unfortunately, however, we depend too much on short-term assignees, thus leaving a lot of the day-to-day CI work in the hands of inexperienced people who will not be in their CI jobs long enough to develop depth on their accounts.

Staffing, in fact may be the most difficult problem in CI.

This practice has had serious real-world consequences. I have been involved in dozens of cases during the past two decades, reviewed many more, and have seen the operational failure—some of which have made it into in the press—that result from this system. Indeed, the losses of the past decade have been serious enough that both CIA Director Burns and the Deputy Director for Operations have acknowledged the compromises and the need to rebuild human operations.[3] The damage could have been prevented or, at the least lessened, had experienced CI officers been integrated into case management.

If this point does not sound convincing, consider the contrary example of Ghost Stories, the operation against Russian illegals in the United States. This operation spanned more than a decade and ended with a stunning success—the arrests of all the SVR illegals in the United States and their subsequent swap for US and British assets imprisoned in Russia. British author Gordon Corera has described how, over a period of years, US intelligence officers managed a Russian asset, acquired details of the illegals, and then eventually exfiltrated him from Russia.[4] From the start, moreover, CI analysts with years or, in some cases, decades of experience on Russia were completely integrated into the operation. These

Counterintelligence may not change, but the landscape on which it is situated certainly does.

analysts processed incoming information, generated reports and follow–on requirements, and participated in operational planning meetings where they informed the debates on the way forward. Toward the end, their deep knowledge of Russian intelligence and the case enabled them to write memos for senior leaders and policymakers that accurately predicted Moscow's reaction to the arrests and helped guide the swap negotiations.[5] It was a textbook example of the contribution CI analysis can make to operational success.

Anyone who sees this call for deep expertise as a US- or CIA-centric view of the role of CI analysis, or simply reflecting my own experiences, might consider the view from the other side. Each of the services that have outfoxed us was able to do so in large part because they had a core group of long-serving officers dedicated to the US target. You can be sure that these officers knew the history of our operations against their countries, had carefully studied our methods and the results of their own operations against us, and then drew appropriate lessons. They won their rounds not because they were naturally superior to us, but because they did the painstaking work of basic counterintelligence.

If I understated the importance of some points, there was one that I got totally wrong. "Double agents and dangles usually do not provide enough information about the target service to justify the effort" required for such an operation, I wrote. I was told early in my career that CIA's job is to collect information, not give it away, and therefore double-agent operations were a waste and to be avoided. For 30 years I failed to question this bit of received wisdom. Since 2009, however, I've looked at enough double–agent cases, many with CIA as the victim, to know that a well–conceived and executed double or dangle operation can be devastating to the target service. The best I can say on this is that you're never too old to learn.[6]

Other than these points, I would not make any changes to "What Are We Talking About." The descriptions of service types remain accurate, the principles and tasks I outlined are timeless, and I believe that what I said about the nature of intelligence politics and the nuts and bolts of the work still stands.[7]

That said, the world moves on. Counterintelligence may not change, but the landscape on which it is situated certainly does. This means that the way we do CI—and the way we talk about it—needs to keep up with the times, and it is to that challenge that I now turn.

The Changed Landscape

New CI focus after the Cold War

In retrospect, we can see that the landscape began to change in the mid-1990s, with the passage of the Economic Espionage Act of 1996. The law, which for the first time criminalized industrial espionage, has had an unhappy life. From the start it was criticized as too vague, which left the legislation vulnerable to the charge that it was passed more to give spies something to do after the Cold War than to protect US industry from nebulous threats.[8] No one was tried for violating the Act until 2009, suggesting that the law, which was passed during a period of unquestioned US technological and economic dominance, reflected anxieties more than real threats. Indeed, the economic espionage threats of 1996 were seen to stem from France and Japan, which hardly turned out to be the case. Moreover, the law was written at the very dawn of the internet age and so has been ineffective against the cyber threats that have emerged since; nor, for that matter, does it seem to have done much to stop China's industrial spying and technology theft.[9]

Toward the end of the Clinton administration, the US took another, more consequential, step to expand the scope and reach of US counterintelligence programs. President Clinton's last Decision Directive, PDD–75, in January 2001 established the National Counterintelligence Executive (NCIX, now the National Counterintelligence and Security Center [NCSC]), and mandated that it produce annual threat assessments and counterintelligence strategies. Subsequently, the Counterintelligence Enhancement Act of 2002 codified the Executive as the "head of national counterintelligence for the United States Government."[10]

NCSC has found no end of CI threats, many of them shifting to reflect the worries of the times. The first National Counterintelligence Strategy (2005) emphasized terrorist and economic threats, along with such ambitious goals as ensuring that "counterintelligence analytic products are available to the President…to inform decisions."[11] By the time the 2020–22 strategy was published, terrorism had largely fallen off the list of CI threats, replaced by "increasingly aggressive and complex threats" from a large and growing variety of state, nonstate, and private threat actors targeting critical infrastructure, technology, supply chains, and the US political system. "It is essential that we engage and mobilize all elements of United States society" to combat the foreign threats, wrote NCSC Director William Evanina.[12]

I believe such a strategy is doomed to a well-deserved failure. It places more and more issues under CI protection but makes no effort to prioritize threats or what is to be protected. In effect, China, Cuba, and Hizbollah are equally threatening, while university, military, technological, and industrial targets all must be protected. The strategy gives no indication of how all this is to be accomplished or where the people to do it will be found. Indeed, Evanina and one of his predecessors, Michelle Van Cleave, acknowledged in a Senate hearing in 2022 that NCIX is an ineffective entity and that US counterintelligence remains fragmented and disorganized, addressing threats in a "Whack-A-Mole through different organizations."[13] Even worse, in scoping threats so broadly and demanding the mobilization of our entire society, the strategy moves in the direction of creating a counterintelligence state, one in which even the most mundane information is deemed sensitive and surveillance and informing become pervasive. This was how the Soviet Union operated and how China defines espionage threats today.[14] It is hardly where we want to go.

Rise of Private Intelligence Entities

NCSC is right about one thing: the proliferation of new intelligence actors is real. "What Are We Talking About" described three types of intelligence services—external, internal, and unitary—and discussed the differences among them. I included in this typology both state and nonstate services, thinking of the latter as mostly belonging to terrorist groups, criminal gangs, and other nefarious actors who, at the time, generally lacked the high-end technical capabilities of government services. During the past 15 years, however, a fourth type of service has emerged, one that is controlled by private parties and has a range of capabilities that formerly were found only in traditional state services.

NCSC is right about one thing: the proliferation of new intelligence actors is real.

Private intelligence outfits are not new, of course. Retired intelligence officers and academics for decades have offered political risk analysis and risk management services to international corporations or entities with specialized interests. Their products, however, relied on publicly available information or narrow source bases, such as old contacts of the former officers. Consequently, the results were hit-or-miss and vulnerable to manipulation—one need only look to the role of Fusion GPS, a relic of that system, in the 2016 US presidential election for an unfortunate example.

Starting in the 1990s, however, the types of information available to private services began to broaden and improve. Round-the-clock cable television news enabled private parties to monitor events at the same time as government services. Soon after, high-resolution commercial satellite imagery became available and enabled entities outside of governments to carry out analysis that hitherto had required resources available only to the largest, best-funded services. As the *New York Times* reported in 1997, the first commercial satellite photos were "expected to be used for civilian spying on military targets, which could include battlefields, bases, arms factories and missile fields … to monitor arms control treaties and to police the world's intelligence services."[15] The *Times'* prediction was spot on. Today constellations of privately launched mini-satellites provide continuous imagery coverage, which appears in the media within hours of events, be they wars or earthquakes, to help inform the public.[16]

Private capabilities in the 1990s, however, could not yet go beyond the immediately visible. The explosive growth of social media in the 2010s eliminated that limitation, making it possible for private entities to start replicating even more capabilities of major governments. The pathfinder was Bellingcat, founded not by an intelligence veteran or academic specialist but by Eliot Higgins, an amateur whose skill and passion was the exploitation of open-source, internet-based resources to monitor current events and provide accurate, independent analysis to the public.[17] Working at first as an informal network of like-minded internet sleuths, Bellingcat collected video, blog, and social media posts to produce near real-time analysis and, as its methods became more sophisticated, added the targeting and recruiting of human sources to enable longer-term investigations. Following the 2020 poisoning of Russian oppositionist Aleksey Navalny, Bellingcat, "by exploiting Russia's corruption," the *Financial Times* reported, "got hold of flight manifests, intelligence agency-issued fake passports, and open-source data

It is hardly a bold prediction to say that continuing advances in technology will enable private intelligence entities to duplicate more and more state-level capabilities.

to prove that Navalny had been poisoned with Novichok."[18]

Others have followed Bellingcat's lead. *Politico* has used internet searches of corporate and customs records to document Chinese military shipments to Russia, for example, and a company in France that supplies data to institutional investors has begun using satellite monitoring of atmospheric pollutants to estimate the impact of sanctions on Russian industrial output. Most recently, the *New York Times* has used intercepted Russian phone calls for stories on the war in Ukraine, and commercial radar tracking data to create a graphic illustrating how the US was using drones over Gaza to look for hostages held by Hamas. These methods, I suspect, are little different from those used by the US Intelligence Community.[19]

While the US lead in advanced collection technologies has eroded, the work of Bellingcat and similar organizations to date has been a net positive for the United States. Traditional media outlets—notably the *New York Times*, *Wall Street Journal*, and *Washington Post*—several years ago adopted its methods for their web-based stories. Since early 2022 they have integrated these into their coverage of the Ukraine war, providing readers with the types of detailed interactive coverage and background explanations until then reserved for government intelligence consumers.[20] Their work plays an important role in providing independent corroboration of official statements, exposing disinformation, and giving readers deeper insights and analysis of events.[21]

It is hardly a bold prediction to say that continuing advances in technology will enable private intelligence entities to duplicate more and more state–level capabilities. In particular, I expect Bellingcat or a similar organization will soon start sophisticated cyber operations, perhaps tunneling into what its targets believe are their secure computer and communications networks. Whoever does this will then have developed capabilities almost indistinguishable from those of traditional state intelligence services, though without the expenditure of tens of billions of dollars per year. With the coming of artificial intelligence (AI), of course, we likely will see developments as yet undreamed of.

The Downsides of Private Capabilities

Even if the Bellingcat ethos is compatible with US interests, the future likely belongs to outfits with far fewer scruples. Two intelligence firms, Israel's NSO Group Technologies and the United Arab Emirate's quasi–governmental Dark Matter (the latter staffed largely by former US intelligence officers), have been happy to sell their advanced collection capabilities to anyone, no matter how unsavory, with money to pay.[22]

The problem of unsavory actors is only going to become worse. In the United States, the demand for contractor support at the intelligence agencies has led to the creation of numerous small companies providing various services, and it is only a matter of time until private equity firms start to buy contractors with the goal of combining them to create full-service outfits. If—when—this happens, I believe it will be an exceptionally dangerous development. Higgins and his associates operate from an ideological commitment to uncovering objective truth, as generally do traditional media outlets. In contrast, private equity firms are committed to profit and probably will have few reservations about who they take on as customers and what their clients' purposes may be.

The end of government monopolies on imagery, signals, and human collection already is raising another significant question for the traditional intelligence world. If such information now is easily obtained from commercial sources or social media analysis, then what is secret anymore? Information from well-placed agents and exotic technical systems that amateurs and the private sector cannot yet match, certainly, but this likely is only a declining fraction of overall intelligence gathering.

In the future, perhaps the only truly secret intelligence will be that which focuses on a small number of the most critical problems, such as decisionmaking at the very top of the tightest authoritarian states. Another question will be what advantages state services such as CIA will be able to claim in covering other issues; it may be that, in a world where advanced intelligence analysis is easily obtained, the IC's competitive advantage will be a reputation for objective, policy-neutral analysis. This, to say the least, will be difficult to maintain.

As the sphere of true secrecy continues to contract, governments are likely to feel they can be much more liberal in releasing information that until now has been tightly held. This, in fact, has already started to happen. In late 2021 and early 2022, as part of their effort to dissuade Russia from invading Ukraine, the US and UK governments released such detailed information on Moscow's preparations as to make it clear that their collection reached deep inside the Russian state, an action previously unthinkable.[23]

While the disclosures failed to deter Putin's invasion, as a political strategy the intelligence releases were a success—the accuracy of the predictions boosted the credibility of US and UK intelligence which, in turn, made it much easier for Washington and London to rally and maintain their own and other nations' popular support for Ukraine.[24] It also provides a template for future crises. Setting aside Chinese skill in deception, should the United States detect Chinese preparations for hostilities with Taiwan, Washington no doubt will be quick to release detailed intelligence and assessments.[25]

Changing Character of the IC Workforce

Another type of change, reflecting broader social trends, is creating additional problems for traditional state intelligence services. In "What Are We Talking About," I pointed out the importance of understanding not only the social contexts of services but also the socio–economic backgrounds of their employees, as both have great influence on service behavior.[26] Simply put, services reflect the societies in which they are situated—spend any time at all with the UK's SIS and you will quickly see it is a microcosm of the British class system, just as Moscow's services exemplify Russia's endemic corruption.

The United States is no different. The IC's new hires have come of age in an era of rapid technological change and increasing political turmoil.

The United States is no different. The IC's newest employees have come of age in an era of rapid technological change and increasing political turmoil. To make a sweeping generalization, they are the products of a society in which education standards have slipped badly during the past several decades, especially in the liberal arts, and that places much less emphasis on the traditional ideas of truth and national loyalty that lie at the heart of intelligence work.[27] At the same time, many in this cohort—stereotypically male, somewhat immature and socially awkward—are attracted to the atomized, nihilistic world of the internet, where they are vulnerable to misinformation, recruitment by traditional state services, and the appeal of violent political movements.[28]

These changes do much to explain the past decade's shift in the nature of insider threats. The vast increase in cyber operations and the drive to use the data in real time for counterterrorism and targeting operations has required services to hire large numbers of young, computer–savvy people, with all the risks that come with them. Those who already tend toward pathological behavior, notes counterintelligence psychologist Ursula Wilder, "will find on the internet remarkably easy ways to reach outlets for their addictions or compulsions" and the more such an individual's "online life becomes the center of his or her consciousness and motivation, the more real–life stabilizing commitments … will weaken and attenuate," creating a heightened risk of falling into espionage or other behaviors damaging to national security.[29]

Wilder's point is not just theoretical. Starting with Edward Snowden and Bradley Manning, and now through Joshua Schulte (Vault 7) and the accused Discord leaker, a wave of young people have used their accesses to disclose enormous amounts of data to the media or directly to hostile governments. Unlike the spies we are used to dealing with—if not ideologically committed, like Ana Montes, then usually middle-aged men unhappy with their lives and careers, disillusioned, or simply broke, like Aldrich Ames—these individuals seem to act for reasons that even they do not always seem to understand.[30] As the continuing expansion of cyber operations increases services' dependence on young computer specialists, it is virtually certain that this problem too will only get worse.

Compounding this problem is that the frequency of disclosures, both official and unauthorized, is turning them into nonevents. With so much having been revealed in the past decade, it is hardly news when yet another collection program, sensitive capability, or batch of highly classified documents becomes public.[31] It would not be surprising if, in the years to come, prosecutors have to settle for lesser charges or lighter sentences than in the past, as leakers argue to indifferent juries that, given the shrinking sphere of secret information and the accumulation of prior disclosures, their acts have done little or no additional harm.

The US IC understands these issues and has taken steps to address them. Under the umbrella term of "insider threat," it has instituted such defensive measures as continuous vetting, zero-trust architecture, and beefed-up internal monitoring. But the scale of the problem—tens of thousands of clearance holders working in multiple agencies and spread around the world—means that implementation of the rules will be, at best, uneven. Because of the inevitable wide variations in local conditions, staff training, leadership, and adherence to procedures, rules are bent or unevenly enforced, leaving numerous gaps for bad actors to exploit.

That laxity, according to the Air Force Inspector General's report, is precisely what happened in the case of the accused Discord leaker. People in his chain of command were aware of his problematic behaviors but did not report them, his commanders were "not vigilant in inspecting the conduct" of their subordinates, and his unit had a "culture of complacency" regarding security.[32]

Taken together, all these changes —the loss of government monopolies on collection, the rise of private services, changing views of what information is sensitive and who may disclose it, and the relentless growth of cyber operations—indicate that CI will become an even more complicated endeavor than it is already. But complicated does not mean hopeless. Some of the problems confronting counterintelligence can also help it—AI, for example, may become a vital tool for analyzing enormous data sets. Nonetheless, AI will by no means be a silver bullet as growing CI challenges will create a requirement for more CI people, who will not become any easier to recruit and train. US and allied intelligence services would be well advised to start working on this now.

The Good News: A Growing Body of Quality Literature

Given all of this, is there any good news in the world of counterintelligence? The answer, perhaps surprisingly, is yes. At the end of "What Are We Talking About," I noted the need for research into the politics, sociology, and economics of intelligence services, as well as for comparative studies. Each of these, as the examples in the textbox on page 26 and other citations throughout this article indicate, have become fruitful areas for academic study. Reading these papers may at times be hard going, but we know a lot more about the behavior of intelligence services than we did 15 years ago, let alone during the Cold War period, and many more people are addressing the issues than ever before.

Most useful for those tasked to work on specific services is the unprecedented quantity of publications produced by intelligence historians during the past two decades. Indeed, we are in a golden age of intelligence history. A generation ago, an interested reader could digest most serious books on counterintelligence in a few months. For CI students, there were:

- J.C. Masterman's *The Double-Cross System in the War of 1939–1945* (1972);
- David Martin's *Wilderness of Mirrors* (1980);
- Christopher Andrew and Oleg Gordievskiy's *KGB* (1990);
- Thomas Mangold's biography of James Jesus Angleton, *Cold Warrior* (1992); and
- not many more.[a]

Since the mid-1990s, the declassification of the Venona documents, opening of Cold War archives, additional releases (whether authorized or not), and memoirs have led to an explosion of histories that have greatly improved public understanding of intelligence and counterintelligence. (The number of book reviews in each issue of *Studies* has roughly doubled in the past 15 years.) This does not include, moreover, the contributions of articles in *Studies* and prominent academic journals on intelligence including, *International Journal of Intelligence and CounterIntelligence, Intelligence and National Security*, and the *Journal of Intelligence History*.

Many intelligence books are aimed at popular audiences, but nonetheless provide valuable insights into the eternal questions of counterintelligence. To start with two obvious examples, The Venona operation and the materials brought out by the Soviet defector Vasiliy Mitrokhin provided an enormous body of primary source information on Soviet intelligence operations that, supplemented by additional research

[a] For an overview of the literature at the end of the Cold War period, see Cleveland Cram, *Of Moles and Molehunters: A Review of Counterintelligence Literature, 1977–92* (Center for the Study of Intelligence, 1993).

by other authors, has helped rewrite the history of Moscow's services and their Cold War competition with the West. (See textbox.)

Historians have written valuable accounts of the Warsaw Pact services, filling gaps in a literature that has traditionally focused on the US, British, and Soviet services. When it comes to writing on deception and betrayal, moreover, it is hard to name a writer who has contributed more than Ben Macintyre, with his updated histories of Britain's World War II deception operations, and the Philby and Gordievskiy cases. Dozens of additional examples are easy to find.

Where to Start?

With so much now available, where does a new CI practitioner start to read? Before diving into specific readings for a particular country or issue, I suggest any new US counterintelligence officer become familiar with the following three topics.

Dreyfus Affair

I wrote in these pages in 2011 that the Alfred Dreyfus Affair was the first modern CI case and also the first modern CI disaster, as it exploded from an apparently straightforward investigation into a political and cultural whirlwind that still affects French public life.[a] Jean-Denis Bredin's account, *The Affair: The Case of Alfred Dreyfus* (George Braziller, Inc., 1986), is still the best English-language history of the case and is essential to understanding what can happen when counterintelligence goes wrong.

Suggested Readings for the New CI Analyst

Though aimed at popular audiences, below is a sampling of the work that nevertheless provides valuable historical insights into adversary intelligence services..

Archival Material

- Robert Louis Benson and Michael Warner (eds.) *Venona: Soviet Espionage and The American Response, 1939–1957—Selected Documents and Messages* (NSA-CIA, August 1996) at https://www.cia.gov/resources/csi/books-monographs/venona/
- Woodrow Wilson Center Digital Archive at https://digitalarchive.wilsoncenter.org/topics/mitrokhin-archive

Cold War Histories

- John Earl Haynes, Harvey Klehr, and Alexander Vassiliev, *Spies: The Rise and Fall of the KGB in America* (Yale University Press, 2009)
- Catherine Belton, *Putin's People: How the KGB Took Back Russia and Then Took on the West* (William Collins, 2020)
- Gordon Corera, *Russians Among Us: Sleeper Cells, Ghost Stories, and the Hunt for Putin's Spies* (William Collins, 2020)
- Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare* (Farrar, Straus and Giroux, 2020)
- David Shimer, *Rigged: America and Russia and One Hundred Years of Covert Electoral Interference* (Alfred A. Knopf, 2020)
- Calder Walton, *Spies: The Epic Intelligence War Between East and West* (Simon & Schuster, 2023)

Warsaw Pact Services

- Kristie Macrakis, *Seduced by Secrets: Inside the Stasi's Spy-Tech World* (Cambridge University Press, 2008)
- Katherine Verdery, *My Life as a Spy: Investigations in a Secret Police File* (Duke University Press, 2018)

Deception and Betrayal: Ben Macintyre's Work

- *Agent Zigzag: A True Story of Nazi Espionage and Betrayal* (Harmony, 2007)
- *Operation Mincemeat: How a Dead Man and a Bizarre Plan Fooled the Nazis and Assured an Allied Victory* (Harmony, 2010)
- *A Spy Among Friends: Kim Philby and the Great Betrayal* (Crown, 2014)
- *The Spy and the Traitor: The Greatest Espionage Story of the Cold War* (Crown, 2018)

Hiss and Rosenberg

Similar to Dreyfus, the Alger Hiss and Julius and Ethel Rosenberg cases affected US society and political culture for decades. They are critically important examples of how the Soviets penetrated the US government at the highest levels and did much to shape how Americans view espionage as well as how the FBI and CIA carry out their counterintelligence work today. Allan Weinstein,

[a] Alfred Dreyfus was a French artillery office of Jewish ancestry tried and convicted of treason in 1894 and exonerated in 1906. See "The Dreyfus Affair: Enduring CI Lessons," *Studies in Intelligence* 55, no. 1 (March 2011).

Perjury: The Hiss Chambers Case (Knopf, 1978, and Hoover Press, 2013), and Ronald Radosh and Joyce Milton, *The Rosenberg File: A Search for the Truth* (Henry Holt and Co., 1983, and *The Rosenberg File, Second Edition*, Yale University Press, 1997) are the standard accounts.

2008 Financial Crisis

What does an economic meltdown have to do with counterintelligence? Plenty, is the answer. Analytic rigor and skepticism of conventional wisdom are vital for CI and, in this vein, Michael Lewis, *The Big Short: Inside the Doomsday Machine* (Norton, 2010 or, if you are pressed for time, the 2015 movie), and Gregory Zuckerman, *The Greatest Trade Ever*: *How One Man Bet Against the Markets and Made $20 Billion* (Penguin Books, 2010), recount how outsiders asked uncomfortable questions, went out of their way to check the facts, and endured ridicule from counterparts. They turned out to be right in their forecasts of a catastrophic failure and their experiences are valuable reading for officers whose job it is to make unpopular judgments.

Spy Fiction

Thoughtful spy novels too, are important reading for counterintelligence officers. They explore human frailties, motives, and loyalties and weaknesses, as well as how intelligence officers view their profession, and they give readers much to ponder. The Cold War era gave us many great espionage tales and the best of Graham Greene, John le Carré, Len Deighton, and W. T. Tyler remain well worth reading.[a] Occasionally, too, bad espionage fiction is worth reading: Julian Semyonov's *Tass is Authorized to Announce* (Riverrun Press, 1979) gives the Soviet view of the spy world, albeit in almost unreadable prose.

The spy novel fell on hard times after the Soviet Union collapsed and authors lost their standard plots, but in the past decade the genre has recovered. Russian villains are back, along with Chinese, but more interesting has been the emergence of a new generation of authors and how they are changing the genre. Women, in particular, are changing a form that has been almost entirely dominated by male authors. Their novels not only feature women protagonists, but also offer new perspectives on identity, sexuality, and family, and how these topics intersect with intelligence work. Notably, two of these authors, Karen Cleveland and Alma Katsu, bring CIA experience to their stories.[b]

The spy novel's renaissance, moreover, has not been limited to the United States and the United Kingdom. Sergei Lebedev's *Untraceable* (Apollo, 2021) shows what Russian authors can do when freed from ideological conformity, and Leonardo Padura's *The Man Who Loved Dogs* (Farrar, Straus, and Giroux, 2015) is extraordinary not only for its literary quality but for how it pushes the limits of the permissible in Cuba.

Final Thoughts

I will close with a final, personal observation. I spent the first half of my intelligence career, almost 20 years, as a political-military analyst. During that time, I often heard CI officers say how different their work was from other intelligence disciplines. I always dismissed this as the puffery of people trying to use the mystery of counterintelligence to make themselves seem important. But now, having worked since 2000 at home and abroad in CI analysis, operations, counterespionage, and management, I have to say that they were right. CI is a different world, one of unending doubt and ambiguity, where questions may not be answered for decades, if ever. It certainly is not for everyone but, for the right people, it is an endlessly fascinating and rewarding occupation.

I am grateful to Ean Forsythe and his students, Tim Ray, and Diane Parsont for their comments on earlier drafts of this article.

❖ ❖ ❖

The author: John Ehrman is a retired CIA analyst.

[a] For example, Greene, *The Confidential Agent* (1939) and *The Human Factor* (1978); le Carré, *The Spy Who Came in From the Cold* (1964) and *Tinker, Tailor, Soldier, Spy* (1974); Deighton, *Berlin Game*, *Mexico Set*, and *London Match* (1984–85); and Tyler, *The Spy Who Lost the War* (1980).

[b] See Kate Atkinson, *Transcription* (2018); Karen Cleveland, *Need to Know* (2019); Lara Prescott, *The Secrets We Kept* (2019); and Alma Katsu, *Red Widow* (2021).

Endnotes

1. Quoted in Deborah Bauer, *Marianne is Watching* (University of Nebraska Press, 2021), 93.
2. The "syncretic spy" appears in the concluding essay of Davies and Gustafson, *Intelligence Elsewhere*, 294, and "counterintelligence threat ontology" is in Dries Putter and Sascha-Dominik Dov Bachmann, "Scoping the Future Counterintelligence Focus," *International Journal of Intelligence and CounterIntelligence* [hereafter *IJIC*] 36, no. 2 (2023).
3. "US Struggles to Spy on China, Its Leading Espionage Priority," *Wall Street Journal*, December 27, 2023; DCIA Fireside Chat with William Burns: Aspen Security Forum 2023, July 20, 2023, https://www.cia.gov/static/598a62b34629a8120fb16d68e440aa15/Director_Burns_Aspen_Security_Forum_Transcript_07202023.
4. The best publicly available account of the operation is Gordon Corera, *Russians Among Us: Sleeper Cells, Ghost Stories, and the Hunt for Putin's Spies* (William Collins, 2020).
5. On the role of CI analysis in the negotiations, see Leon Panetta, *Worthy Fights* (Penguin, 2014), 281–84.
6. See Eleni Braat and Ben de Jong, "Between a Rock and a Hard Place: The Precarious State of a Double Agent during the Cold War," *IJIC* 36, no. 1 (2023).
7. See Chris Whipple, *The Spy Masters* (Simon & Schuster, 2020), and John McLaughlin, "Four Phases of Former President Trump's Relations with the Intelligence Community," *IJIC* 34, no. 4 (2021).
8. See Richard Maxwell, "What is a Spy to Do?" *Social Text* 56 (Autumn 1998): 125–41.
9. See Brenda Rowe, "Transnational State-Sponsored Cyber Economic Espionage: A Legal Quagmire," *Security Journal* 33 (2020): 63–82, and William Edelman, the 'Benefit' of Spying: Defining the Boundaries of Economic Espionage Under the Economic Espionage Act of 1996," *Stanford Law Review* 63 (January 2011): 447–74.
10. 50 USC 401.
11. Office of the National Counterintelligence Executive, *The National Counterintelligence Strategy of the United States*, March 2005, 7.
12. National Counterintelligence and Security Center, *National Counterintelligence Strategy of the United States of America, 2020–2022*, January 2020, iii.
13. "On Protecting American Innovation: Industry, Academia, and the National Counterintelligence and Security Center," Hearing before the Select Committee on Intelligence of the United States Senate, September 21, 2022, 12–74.
14. On the Soviet counterintelligence state, see John Dziak, *Chekisty* (Lexington Books, 1987). For China's current CI campaign, see "China to its People: Spies are Everywhere. Help us Catch Them," *New York Times*, September 3, 2023, and "No Laughing Matter," *Economist*, January 13, 2024.
15. "First Civilian Spy Satellite Soars Into Space, Launched in Russia by a U.S. Company," *New York Times*, Dec. 25, 1997. For an extended discussion of the development of these capabilities, see Amy Zegart, *Spies, Lies, and Algorithms*, (Princeton University Press, 2022), chap. 9.
16. See "Satellite Photos Show Cleansing of Syrian Site," *New York Times*, Oct. 26, 2007. For private satellite constellations, see David Zikusoka, "Spying from Space," *Foreign Affairs*, digital version, February 2, 2024. Recently, the media has used imagery in its daily coverage of events; for example the *Wall Street Journal* published before and after images of Yemeni targets struck by the United States and the UK in January 2024. See "US Strikes Give Yemen's Houthis the Enemy They Long Sought," *Wall Street Journal*, January 13, 2024.
17. Eliot Higgins, *We are Bellingcat* (Bloomsbury, 2021), reviewed in *Studies* 65, no. 1 (March 2021). For an analysis of the impact of combined open technical and social media sources Sean Larkin, "The Age of Transparency: International Relations Without Secrets," *Foreign Affairs*, May/June 2016.
18. "Lunch with the FT: Christo Grozev," *Financial Times*, August 12, 2023. For Bellingcat's report, see https://www.bellingcat.com/news/uk–and–europe/2020/12/14/fsb-team-of-chemical-weapon-experts-implicated-in-alexey-navalny-novichok-poisoning/.
19. "China Secretly Sends Enough Gear to Russia to Equip an Army," *Politico*, July 24, 2023; "Pollution Reveals what Russian Statistics Obscure: Industrial Decline," *Wall Street Journal*, May 5, 2023; "US Drones are Flying over Gaza to aid in Hostage Recovery, Officials Say," *New York Times*, November 3, 2023.
20. See "Caught on Camera, Traced by Phone: The Russian Military Unit That Killed Dozens in Bucha," *New York Times*, December 22, 2022; "'Putin is a Fool': Intercepted Calls Reveal Russian Army in Disarray," *New York Times*, September 28, 2022; "US Drones are Flying Over Gaza to Aid in Hostage Recovery, Officials Say," *New York Times*, November 2, 2023. For examples of similar coverage, see "How We Know Russia is Using Iranian Drones in Ukraine," *Wall Street Journal*, November 11, 2022; and "A Web of Trenches Shows Russia Fears Losing Crimea," *Washington Post*, April 3, 2023.
21. See https://www.bellingcat.com/news/2023/03/29/how-online-investigators-proved-video-of-ukrainian-soldiers-harassing-woman-was-staged/.
22. See "Ex-US Intelligence Officers Admit to Hacking Crimes in Work for Emiratis," *New York Times*, September 14, 2021; "Pegasus Spyware Used to Hack US diplomats Working Abroad," *Washington Post*, December 3, 2021; "In a First, Spyware is Found on Phone of Prominent Russian Journalist," *Washington Post*, September 13, 2023. See also Ronald Deibert, "Subversion Inc: The Age of Private Espionage," *Journal of Democracy* 33, no. 2 (2022).

23. See “U.S. Intelligence Document on Russian Plan for Possible Ukraine Invasion,” *New York Times*, December 3, 2021; “U.S. Says Russia Sent Saboteurs Into Ukraine to Create Pretext for Invasion,” *New York Times*, January 14, 2022; “Biden does a Victory Lap on Russia–Ukraine Intelligence,” *Washington Post*, February 24, 2022; “Xi Doesn’t Want to See Putin Humiliated,” Financial Times, May 27, 2023. See also “To counter Russia in Africa, Biden deploys a favored strategy,” *Politico*, May 7, 2023, https://www.politico.com/news/2023/05/07/wagner-russia-africa-00095572.
24. See Serge Schmemann, “Why Secrets Lost Their Sizzle,” *New York Times*, June 11, 2023.
25. See “Data on air bases suggest a Chinese invasion of Taiwan may not be imminent,” *Economist*, July 29, 2023.
26. See Hager Ben Jaffel and Sebastian Larsson, “Why do We Need a New Research Agenda for the Study of Intelligence?” *IJIC*, Posted July 6, 2023, and John Gentry, “Demographic Diversity in U.S. Intelligence Personnel: Is It Functionally Useful?” *IJIC* 36, no. 2 (2023).
27. See Margaret Marangione, “Millennials: Truthtellers or Threats?” *IJIC* 32, no. 2 (2019).
28. For vulnerability and the internet, see Ursula Wilder, “The Psychology of Espionage and Leaking in the Digital Age,” *Studies in Intelligence* 61, no. 2 (June 2017): 5.
29. Ibid., 5–6.
30. For examples, see Patrick Radden Keefe, “The Surreal Case of a CIA Hacker’s Revenge,” *New Yorker*, June 6, 2002, and “Alleged Leaker Fixated on Guns and Envisioned ‘Race War’,” *Washington Post*, May 13, 2023. For additional perspectives on insider threats, see Eric Shaw and Laura Sellers, “Application of the Critical-Path Method to Evaluate Insider Risks,” *Studies in Intelligence* 59, no. 2 (June 2015), and Chloe Wilson, “Exposing the Cracks: Impact of the COVID-19 Pandemic on Organizational Justice in the Intelligence Community,” *Studies in Intelligence* 66, no. 4 (December 2022).
31. See Schmemann, *New York Times*, June 11, 2023.
32. Inspector General of the Department of the Air Force, “Report of Investigation (S9691),” August 2023. For additional details, see “Jack Teixeira got Security Clearance Despite History of Violent Threats,” *Washington Post*, December 11, 2023.

❖ ❖ ❖