Studies in Intelligence Vol. 53 No. 2 (2009)

Toward a Theory of CI

What are We Talking About When We Talk about Counterintelligence?

John Ehrman

A consistent theme in public discussions of the performance of US intelligence is how poorly Americans conduct counterintelligence (CI). Whether it is the former chief of the CIA's Counterintelligence Center (CIC), Paul Redmond, famously observing that Americans are "too nice" to carry out CI properly or former National Counterintelligence Executive Michelle Van Cleave lamenting that the US government is failing at strategic CI or the legions of books and articles by scholars and journalists criticizing intelligence agencies for failing to catch spies and protect secrets, the conclusion is almost always the same. "Our national CI program has failed to carry out its mission," wrote George Kalaris and Leonard McCoy in Studies in Intelligence in 1988. In 2005, the WMD Commission echoed their conclusion when it reported that "US counterintelligence efforts have remained fractured, myopic, and only marginally effective." While these criticisms often are unfair or exaggerated—the United States has had many CI successes—they do contain elements of truth. US counterintelligence efforts often are poorly organized, conceptualized, and executed, and CI remains a relatively neglected area of study in the Intelligence Community.[1]

A large reason for this neglect is the absence of a theory for counterintelligence. This problem is not unique to CI, and students of intelligence have noted that the field as a whole suffers from a lack of strong theoretical work. Counterintelligence, however, seems to be worse off than the rest of the intelligence disciplines. Recent intelligence scholarship, for example, has discussed theoretical issues relating to the definition of intelligence, the overall state of intelligence theory, obstacles to success in intelligence, and the politics of the CIA. These works, however, largely focus on intelligence in policymaking and barely mention CI, no doubt reflecting the interests and experiences of academic specialists and also the practical obstacles to research created by the secrecy and mystery inherent in CI. Indeed, only two articles specifically on counterintelligence theory seem to have been published in the past few decades, and neither is a thorough treatment of the subject.[a2]

What follows is an effort to begin developing a theory of counterintelligence. My purpose is not to present a fully formed theory but, rather, to take the first steps toward building one by considering what a theory would need to cover. Viewed that way, this article may be thought of as an answer to the question, "What are we talking about when we talk about CI?" I begin with an explanation of the benefits a theory would bring to CI work, then define counterintelligence, break down its various aspects, and finish with suggestions for further research for building a theory. This structure reflects my belief that counterintelligence is primarily an analytic discipline, which in turn centers on the study of intelligence services. Much of what I will put forward is based on my observations during a decade of work as a CI analyst and manager at the CIA, discussions with intelligence officers from the United States and other countries, as well as my classified and unclassified reading in the field.

* * * * *

Footnotes

a) Vincent Bridgemen, "Defense Counterintelligence, Reconceptualized," in Jennifer Sims and Burton Gerber, eds., *Vaults, Mirrors, and Masks* (Washington: Georgetown University Press, 2008) and Stan Taylor, "Definitions and Theories of Counterintelligence," in Loch Johnson, ed., *Strategic Intelligence, Volume 4: Counterintelligence and Counterterrorism* (Westport, CT: Praeger Security International, 2007).

Why Theory?

Intelligence officers generally are practical people, concerned with achieving concrete results for their customers. They usually are uninterested in theories which, in their view, do not offer immediate help with their

Theory is an important building block for intellectual disciplines, whether in intelligence or any other field.

work. Nonetheless, theory is an important building block for intellectual disciplines, whether in intelligence or any other field. Specifically, a well-developed theory will offer:

- *A framework for understanding and explaining a subject.* This includes not only an overall definition that bounds the field of study, but also a way to break it down into smaller, manageable parts that, in turn, can be clearly defined and understood. The definitions also provide a common vocabulary for those working in the field, thereby ensuring that they can understand each other.
- *A way to model expected behavior.* As economic and political models demonstrate, theory enables the building of models of how people or institutions can be expected to behave in given situations. Even though they simplify and generalize, models can be tested against real-world data and their predictive values further refined.
- *A way to identify gaps in knowledge.* By systematically describing a topic, we not only can catalogue what we know about it but, just as important, find out what we do not know. These gaps can then become objectives for data collection, as well as new areas of study for analysis.

Definition

Generations of undergraduates opened their economics textbooks on the first day of class and learned from Paul Samuelson that economics is "the study of how societies use scarce resources to produce valuable commodities and distribute them among different people." This is almost ideal as a definition—it is short and precise, but also flexible enough to cover almost anything that someone interested in the subject might want to study. Although many definitions of counterintelligence exist, to date no one has defined it in such succinct terms. (For a sample of definitions, see box on facing page.) With a goal in mind similar to Samuelson's, I propose the following definition of counterintelligence:

> *Counterintelligence is the study of the organization and behavior of the intelligence services of foreign states and entities, and the application of the resulting knowledge.*[3]

This definition has several advantages. Foremost, it acknowledges that counterintelligence is an analytic discipline. The definition also is broad enough to include any national-level intelligence service, whether foreign, domestic, technical, or military. It can also include lower-level intelligence services, such as those belonging to provinces or police departments. While this article will concentrate on the discussion of national-level services, the definition includes nongovernmental organizations (NGOs), and thus brings the intelligence activities of terrorists, criminal gangs, as well as traditional NGOs, into the field of study. (While counterintelligence traditionally has been a state-sponsored activity, the definition allows nonstate actors—or even academics—to carry out CI.) Finally, the definition avoids making the study of intelligence services purely a research exercise. Indeed, applied counterintelligence has an important role to play in policy decisions, as well as intelligence operations.

What is Counterintelligence? Competing Definitions

The term "counterintelligence" means information gathered, and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons or international terrorist activities.–National Security Act of 1947, as amended (50 USC 401a)

Counterintelligence means information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage or assassinations conducted for or on behalf of foreign powers, organizations or persons, or international terrorist activities, but not including personnel, physical, document or communications security programs.–Executive Order 12333

Counterintelligence is the business of identifying and dealing with foreign intelligence threats to the United States. Its core concern is the intelligence services of foreign states and similar organizations of non-state actors, such as trans-national terrorist groups. Counterintelligence has both a defensive mission —protecting the nation's secrets and assets against foreign intelligence penetration—and an offensive mission—finding out what foreign intelligence organizations are planning to better defeat their aims.–Office of the National Counterintelligence Executive

CI can be defined as the identification and neutralization of the threat posed by

foreign intelligence services, and the manipulation of those services for the manipulator's benefit.–Roy Godson

Counterintelligence is the broad subset of intelligence focused on the intelligence efforts of a competitor. The core of the mission is about understanding and exploiting a competitor's reliance on intelligence.–Vincent Bridgeman

Counterintelligence Activity. Activity conducted by special state agencies against foreign intelligence services and organizations and individuals being used by them.–KGB, via Mitrokhin

Counterintelligence is detective work, but of a highly specialized kind, focusing on operational detail in a secret world where meetings are arranged and held, and messages and intelligence information are exchanged, in a way meant to conceal the fact that they have ever occurred.–Frederick Hitz

Counterintelligence is to intelligence as epistemology is to philosophy. Both go back to the fundamental question of how we know things, both challenge what we are inclined to take most for granted.–Thomas Powers

---

The Study of Intelligence Services

The foundation of all counterintelligence work is the study of individual intelligence services. This is an analytical process, whose goal is to understand service behavior—that is, how services define and carry out their missions. Every service has its own distinctive behavior, as even a cursory comparison of services will show. Studying their behavior has the potential to provide a range of useful insights: such research may shed light on the roles a service may play in a country's foreign policy decision making, its internal politics, or how its components and officers may be expected to act operationally. These findings would be useful to both policy and operational consumers. Conducting such analysis, in turn, requires examining the major factors that govern service behavior, a process that starts with identifying the type of service under examination and then proceeds to look at how the service's mission is defined, the external and internal political environment, its history, and the people who staff it.

Types of Intelligence Services

The first step in studying any intelligence service is to categorize it. There are three types of intelligence services—external, internal, and unitary.

Differences in the conceptions of their missions, as well as the political, social, and historical contexts of services have led to widely varying behavior.

- External, or foreign, intelligence services focus on targets and operations outside their country's borders (or sponsoring organization), with the primary goal of collecting secret information about the capabilities of foreign states and entities. External services may be civilian, military, or technical. Their operations at home almost always are limited to targeting foreigners who are either residents or in transit. Examples of civilian external services include the CIA, Britain's Secret Intelligence Service (SIS), and the Russian SVR. Well-known military intelligence services include the US Defense Intelligence Agency (DIA) and Russia's GRU. The US National Security Agency (NSA) and the UK's Government Communications Headquarters (GCHQ) are leading technical intelligence services that concentrate on foreign targets.
- Internal, or domestic, intelligence services operate against targets within their borders or sponsoring organization, with the primary mission of identifying and countering threats to the security of the host state or entity. These threats include the intelligence operations of other states or organizations, domestic political subversion, and terrorism. Internal services are almost always civilian, and their operations abroad are limited and often dominated by liaison work. Some of the best-known internal services are the FBI, the British Security Service (BSS), the French DCRI, Russia's FSB, and the Israeli Shin Bet.
- Unitary services combine internal and external intelligence functions in one organization. Historically, most unitary services have existed in totalitarian states, where their far-reaching capabilities made them effective instruments of repression. One of the most important functions of the Soviet KGB and the intelligence services of the Warsaw Pact states was to crush political dissent; when the communist bloc regimes collapsed, the successor governments

quickly split their services and abolished the internal service's political role. Today, unitary services, such as China's Ministry of State Security (MSS), mostly are found in the few remaining communist states. The Canadian Security Intelligence Service (CSIS) and New Zealand Security Intelligence Service (NZSIS), however, are examples of how limited resources and a relatively benign external security environment sometimes make a unitary service a sensible option for a democratic state.

Factors Determining the Behavior of Intelligence Services

It is tempting to assume that similar intelligence agencies will behave in the same ways. After all, if external services all have the same basic function, it stands to reason that there will be little difference in how they organize themselves, prioritize their tasks, and conduct operations. This view is not entirely inaccurate. Because of the similarity of their work, services tend to have similar internal structures and use many of the same operational methods. But this disguises important distinctions among services, as a quick comparison of the BSS and Shin Bet or the CIA and SVR will reveal. Differences in the conceptions of their missions, as well as the political, social, and historical contexts of the services have led to widely varying behavior among them and are important to understand in any analytic effort.[4]

Definition of the mission. At the broadest level, an intelligence service's mission is defined through political and legal processes that set the goals of the service and the limits of its powers. Until the 1970s, services commonly were free to set their goals with minimal government supervision and had few legal limits on how they carried out their work. Since the mid-1970s, however, the trend has been for governments to institutionalize and limit the powers of their services by writing laws that define their missions and authorities, especially with regard to areas involving civil liberties, such as the use of electronic surveillance.

This movement began in the United States, where the post-Watergate revelations of CIA and FBI wrongdoing led to the establishment of congressional oversight, and the need to clarify the rules for electronic surveillance led to the passage of the Foreign Intelligence Surveillance Act (FISA) in 1978. Later in the 1970s and 1980s, revelations of political interference and civil liberties violations by domestic services in Australia

and Canada, and the Spycatcher affair in the United Kingdom, led these countries to pass legislation placing their services on firm legal foundations (MI-5, the forerunner of BSS, had been operating since 1909 without any statutory authority) and setting rules for their operations.

- The CSIS Act of 1984 was typical of such laws. It defined the service's mission—"the Service shall collect, by investigation or otherwise, to the extent that it is strictly necessary, and analyse and retain information and intelligence respecting activities that may on reasonable grounds be suspected of constituting threats to the security of Canada"—and specified procedures for obtaining warrants, protecting civil liberties, and establishing public accountability and oversight.
- The process accelerated during the 1990s, when states as varied as the newly democratizing countries in Eastern Europe, Russia, South Africa, and Israel all passed similar legislation to define their services' missions, powers, and oversight.[5]

Counterintelligence analysts should carefully study the legal contexts of services, for these have the potential to affect service performance significantly. In fact, intelligence scholars have found that effective oversight and enforcement of the laws and regulations governing a service can help it meet high standards for conduct and performance, while poorly structured oversight harms service performance. The laws and regulations developed during the past three decades have focused most on domestic services, whose activities naturally raise more civil liberties concerns for democratic government than those of external services operating abroad.

> A service that works within a clear set of laws can expect to build public confidence in its performance—and receive public support— as well as to improve its self-confidence.

As much as domestic services may complain about constraints on their powers or the time lost obtaining warrants, having clear and well-enforced rules reduces uncertainty for both the service and the general population. As long as they act in accordance with the laws, for example, domestic services know that the evidence they gather will hold up in court and cases will not be lost because of procedural mistakes, while civilians will have less fear that a service is acting beyond its authorities. Service

leaders, for their parts, know that if they follow the rules, their own liabilities are minimized; in the event of a flap, they may be fired but they will not go to prison. Over the long term, therefore, a service that works within a clear set of laws can expect to build public confidence in its performance—and receive public support—as well as to improve its self-confidence.[6]

Because their governing laws provide only broad guidance, services are left to decide for themselves what they will try to accomplish on a day-to-day basis. These decisions, in turn, depend on their understanding of their governments' strategic positions, threat perceptions, and policies, as well as the services' own goals and available resources. For most services, internal and external, the result is that they focus their efforts on just a few critical capabilities and issues.

- Internal services today often make counterterrorism their highest priority, leaving comparatively few resources to monitor other security threats. In these cases, they often ignore foreign intelligence activities that do not pose immediate threats to their government's interests. I know of one major service, for example, that devotes almost all of its efforts to counterterrorism and monitoring local Russian intelligence activity, leaving almost no resources for other CI work.
- Only a handful of external services—the CIA, SVR, and, to a lesser extent, SIS, French DGSE, and Mossad—attempt to cover the world. Almost all other services concentrate on their immediate neighbors or regions. These services usually are dependent on liaison relationships for information on areas beyond their immediate neighborhoods, and often trade their regional expertise for what they require from globally capable services.[7]

Internal services, however, generally can adopt new missions faster than external services. With the advantages that come from legal and political support, while operating on territory that they know well and where they can openly appeal for (or compel) public assistance, domestic services can quickly shift resources and begin new operations, as many Western services did in the months after 11 September. In contrast,

> Anyone seeking to understand or predict the behavior of a service needs to have at least a basic understanding of the political system in which the service is located.

because they operate clandestinely on foreign territory and must hire and train officers who can work in alien environments, external services need much more preparation time for undertaking new missions. While external services can shorten this time, as the CIA did in September 2001, this tends only to happen in emergencies. In general, experience suggests that building effective capabilities for new overseas missions is a process that takes several years.

External and Internal Politics. Intelligence services are government bureaucracies, subject to the same political forces and tendencies as any others. Thus, anyone seeking to understand or predict the behavior of a service needs to have at least a basic understanding of the political system in which the service is located. In a democratic state, as numerous cases from the past few decades attest, political or other external events can have enormous consequences for services, even when the services are not directly involved or responsible. The end of the Cold War, to cite an exceptional case, led to drastic cuts in the size and capabilities of US and European services; the Asian and Russian financial crises of the late 1990s led to budget cuts that devastated the capabilities of several major services; and recent intelligence failures, such as the 11 September attacks and the Iraqi WMD fiasco (which involved the services of several countries), brought not only public investigations and large-scale restructurings but also internal changes in how individual services collect and evaluate information.[8]

The political situations of intelligence services in authoritarian or totalitarian states are more difficult to determine. The absence of effective legal frameworks and the importance of personal networks over institutional relationships for government decision making make it difficult for outside observers to see what is going on. Examples from the history of communist bloc services, however, suggest that in authoritarian and totalitarian states the positions of their services may be paradoxical. The dependence of such regimes on their services for repression, the integration of the services into the governing apparatus, and the absence of any outside check, provide the services with immunity from external inquiries and pressure for reform. At the same time, however, should the leadership perceive a serious failure or disloyalty within its services, the punishments are likely to be far more harsh than in democracies—jail terms and even executions are not unknown.

Even as they are acted upon, however, intelligence services work diligently to protect and advance their interests. The result is that services are

almost always engaged in complex, multifront political struggles. The most basic of these is the constant effort to gather more resources—people, funds, and influence over decision making—from their political superiors, and to resist externally imposed changes.

Inevitably, a country's services are forced to compete with one another, and each seeks to gain an advantage by claiming credit for successes, denigrating rivals, or taking away cases. The conflicts between the CIA and FBI, CIA and DIA, MI-5 and SIS, the KGB and the GRU (and now the FSB and SVR) are well-known examples of this phenomenon and suggest that bureaucratic conflict between intelligence services is the norm, even as political leaders try to force them to cooperate.

- The conflicts do not appear to extend to eliminating competitors, however. Internal, external, and military services are specialized enough and have enough separate consumers so that they do not try to take over each other's roles. (Governments sometimes merge services, as the French did with their internal and police services to form the DCRI in 2008, but the fear of unitary services limits this to combinations of similar services.) Their attacks tend to be on the margins, especially as they try to claim primacy on a case or specific issue, and this behavior seems opportunistic rather than systematic.[9]

In addition to interservice rivalries, services are prone to internal bureaucratic fighting. The complexity of intelligence organizations and their work provides many potential flashpoints, such as turf battles and disputes regarding primacy for specific operations, arguments about tradecraft, analytical disagreements, or straightforward budget fights. These battles can be as bitter as any with another service, if only because the participants know each other well and, because they see each other every day, can easily keep score. As with interservice rivalries, this behavior is normal and to be expected.

History and myths. Every service celebrates its past, and its views of these times can have important effects on its contemporary behavior. Services often have achieved the most in times of national crisis, and tales of their feats of daring, undertaken without

The complexity of intelligence organizations ... provides many potential flashpoints, such as turf battles and disputes regarding primacy for specific operations, etc.

regard for bureaucratic formalities, can serve to inspire and socialize new recruits into their cultures. History is also accompanied by myths, which can enhance the glories of past deeds and also be used to bury the less heroic episodes. Thus, the CIA still takes great pride in the exploits of the OSS, but makes little mention of the Soviet agents who penetrated it. For the Mossad, the kidnapping of Adolf Eichmann, Eli Cohen's operations in Syria, and its post-Munich assassinations of terrorists have achieved mythic status, but the service probably says little about its botched operations, such as when it has killed the wrong person. Mossad's case also is a good example of how history influences current behavior. Its heritage has given Mossad an operational outlook that encourages risk taking to the point of recklessness—the Pollard and Franklin cases demonstrate that it is willing to undertake operations that have the potential to create political disasters that far outweigh the intelligence benefits.[10]

Studying a service's old cases and methods also provides windows into current operations. The best example of this comes from the Russian services, as their operational history, beginning with the Czarist Okhrana and continuing through the Soviet and post-Soviet periods, is one of remarkable continuity. The Okhrana, for example, pioneered the use of penetrations and agents provocateurs in opposition groups, a practice picked up by the Cheka and used throughout the Soviet period.

- Today, the SVR continues to use illegals, officers who receive years of training and resource-intensive preparation to live overseas under false, non-Russian identities. This practice is another holdover from the early days of Soviet intelligence, when the USSR had few legal intelligence establishments overseas, but in today's world probably produces no better results than any other clandestine methods. Nonetheless, the SVR proudly carries on this tradition.
- The FSB continues the practice, again begun by the Okhrana, of attempting pervasive internal surveillance. Like the Soviet internal security services, moreover, the FSB continues to be an obedient and ruthless tool the political leadership can use against its opponents, as the murder of Aleksandr Litvinenko in 2006 indicates.[11]

People. Finally, services are not robotic institutions but, rather, are staffed by hundreds or thousands of people who

Internal and external services are remarkably inward looking.

make and execute decisions.
To my knowledge, there are no
open-source sociological or comparative studies of intelligence officers, and I have found only one classified study, dating from 1983. Nonetheless, intelligence history, as well as personal observations, point to some hypotheses about the populations of services.

- External service officers tend to be from higher socioeconomic classes. The nature of their work—living and operating in other countries, posing as diplomats or businessmen, and interacting with political leaders at home and abroad—requires a university education, knowledge of foreign languages and culture, and confidence interacting with senior diplomatic and political officials. People with these characteristics likely will come from the upper middle class or higher; if of working class origin, they will have adopted such mannerisms and outlooks in school or during their training. The stereotypes of Ivy League CIA officers and Oxford- or Cambridge-educated SIS officers are rooted in fact, and the KGB (and SVR today) recruited many of its officers from Moscow's elite universities.
- Internal service officers tend to be from the working and lower middle classes. Their work is similar to police work and, as they carry out their duties on their home turf, street smarts are more important than a veneer of sophistication. Tellingly, according to Jeffrey Richelson, when Canada was preparing to move its internal security service out of the Royal Canadian Mounted Police and into CSIS, the government worried that the transferees from the Mounties, with only high school diplomas, would lack the education and broad backgrounds desired for CSIS officers. Nor is it surprising that the FBI's Robert Hanssen, while he had a university degree, was the son of a policeman and started his career as a police officer in Chicago.[12]

One trait that internal and external services have in common is that they are remarkably inward looking. A look at almost any service reveals that except for the chief, no outside appointee holds a position of authority; the ambitious politicians, lawyers, think tank analysts, and academics who move in and out of almost all government ministries do not exist in the intelligence world. As a result, services are staffed and run (again, except at the very top) by career employees. While this gives services solid foundations of experience and expertise, as well as officers who identify strongly with their organizations, it also isolates them.

In contrast to militaries, which prepare promising officers for high-level

responsibilities by sending them to staff schools and civilian university programs, intelligence services have no schools or systems to provide advanced or mid-career training to their officers other than language classes or short technical courses. Intelligence officers often rise to senior levels with little exposure to outside ideas, which has consequences for the behavior of services.

- The management of services tends to be mediocre. In general, strong-performing case officers and street agents rise through the ranks and assume management positions. They usually receive no formal management training before taking these positions, however, and little systematic training afterward. As a result, services' mid- and senior-level managers often have little interest in overseeing critical administrative and planning details, or taking initiatives to change or modernize their services before a failure or crisis forces them to do so.
- Services are slow to innovate or learn from their errors. Examinations of the US Intelligence Community, for example, have found that longstanding organizational cultures created strong incentives against innovation, especially at the FBI, and that these contributed to the disaster on 11 September. Similarly, I am aware of at least one major foreign service that has been unable to address its chronic problems in vetting sources and reporting, despite years of effort.[13]

Applied Counterintelligence

Analyses of the behavior of other countries' intelligence services can be applied in many ways. On the policy side, CI analyses can help fill gaps in analysts' understanding of the political processes in other countries. For intelligence operations in general, understanding the workings of other services can be the difference between success and failure. This knowledge also is critically important for CI operations in particular, as well as for counterespionage investigations. Unfortunately, while a large amount of this information is available, potential consumers of counterintelligence information often either do not understand its utility or view it in such narrow terms that they fail to take full advantage of it.

Policy Support

Counterintelligence analysis can provide valuable information for use in policy deliberations, especially in issues involving authoritarian or totalitarian states. Because those regimes, unlike democratic governments, do not debate their policies in public, understanding the intelligence services and their practices can help analysts infer how their political leaders view the outside world. For example, collecting samples of raw reporting and finished reports enables counterintelligence analysts to judge the quality of the information a service gathers, its rigor in vetting reports, and whether it provides its customers with an accurate picture of the world, or distorted and politicized reports that serve only to support the leadership's preconceptions.

Counterintelligence analysis can provide valuable information for use in policy deliberations, especially in issues involving authoritarian or totalitarian states.

Such information can help political analysts, in turn, refine their judgments of how likely a regime is to make a potentially disastrous move because of its own misperceptions—certainly an important question in dealing with states such as North Korea or Iran. In other cases, the careful study of the history, operations, and personnel of a service can be critical in understanding how it may constrain or undercut its government's policies. The best recent example of this is Pakistan's Interservices Intelligence Directorate (ISID), knowledge of which is critical to understanding Islamabad's counterterrorism policies and how far it is willing—or able—to go in supporting US efforts.

Policymakers in democratic and authoritarian states use CI analysis differently, however. In democratic states, leaders tend to overlook the contribution that counterintelligence analysis can make to their decisionmaking. In many cases, as the WMD Commission noted, they view CI as either a law enforcement issue or an internal matter for their intelligence services, and pay attention to it only in the wake of high profile espionage cases, like those of the Walker family or Aldrich Ames.[14]

In my own experiences, I have noticed that policymakers often are unaware of the unique characteristics or activities of intelligence services that, as in the case of ISID, can have a large impact on US interests.

Because of this, raising and maintaining policymaker awareness of the potential for CI to assist them is a constant challenge for analysts. (It says a great deal about US policy processes that the index for Christopher Andrews' book on US presidents' use of intelligence, *For the President's Eyes Only* (1995), has no entry for counterintelligence.)

Generalized counterintelligence training, while useful, does not bring with it expertise in specific services or aspects of CI work.

Leaders of totalitarian and authoritarian states, in contrast, are avid consumers of counterintelligence information. Always on the watch for spies and other security threats, real or imagined, they hunger for information on any plots that could threaten their rule. This was the case in the Soviet Union, up to the collapse of the communist state, as the KGB kept watch on all dissent and provided the leadership with detailed, if fanciful, reports on dissidents' foreign links. There is no reason to believe that the leaders of Syria, Iran, China, Russia, and North Korea today are any less eager readers of CI reporting.[15]

Operational Support

Services have long understood that CI plays an important role in their operations. Because of this, they train their officers in a variety of CI tools and methods. This generalized training, while useful, does not bring with it expertise in specific services or aspects of CI work. Indeed, CI officers often are case officers on limited tours and, while they learn much about the discipline and services, often move on without having gained great depth in the field. This is unfortunate, for the greater the available CI expertise on any given service or country, the greater are a service's chances of operational success against that target. Analyses of individual services, especially, are important in every phase of an operation, even if the target is not an intelligence officer or service.

- *Planning.* Counterintelligence research and analysis are obviously important for operations aimed at penetrating intelligence services, as they enable operations officers to identify and target components and individuals. For operations aimed at other entities, however, CI research can provide important information about the relationship

between the targeted organization and any intelligence services or officers charged with overseeing its security—the FSB, for example, has a presence in most Russian scientific and defense installations—and therefore inform planners about threats to the security of their operation.
- Similarly, operational planning requires an understanding of the CI environment where the operation is taking place; this, in turn, necessitates research to determine the capabilities and potential vulnerabilities of any services that may be present.
- *Operational vetting.* Counterintelligence analysis already has a well-established role in vetting operations and assets. Beyond monitoring individual cases to ensure their security and the validity of assets, however, counterintelligence analysts can make a broader contribution by comparing a particular case with other, similar, current cases to discern patterns or warning signs that may not be evident from monitoring one case at a time. Similar results may be obtained by examining and comparing historical and present cases.
- *Lessons learned.* Every case, from the spectacular success to the complete failure, has its lessons. For this reason, CI analysts should review cases on a regular basis, and summarize any lessons they hold so that operational procedures can be modified as required. Even if the lessons simply confirm what we already know, this serves to ensure that our CI knowledge base is current.

Record keeping

This function is integral to CI support to operations, but it is often neglected. Every operation produces counterintelligence information, even if it does not target an intelligence service. This information can include case officer observations about surveillance and the local CI environment, an asset's offhand remarks about security procedures or his identification of other intelligence officers, as well as small and seemingly insignificant details about how a service or other entities operate.

These details often are lost, even though they can be important to updating our knowledge about services and providing baseline information for vetting future reporting. In many cases this is because CI information is not seen as the objective of the case and therefore is not formally extracted and reported; in other cases, because of compartmentation, the CI details first are not reported and then are forgotten and left irretrievable

after the case has ended and the officers involved have moved on to new assignments.

To prevent this, counterintelligence specialists should continuously monitor cases and apply a comprehensive system for identifying, filing, disseminating, and retrieving CI information, thereby making it easily available to operations officers, investigators, and analysts. The lack of such a system has a high cost—MI5 let its CI recordkeeping slide during the interwar years, with near-disastrous results in 1939 and 1940—and, sadly, few such systems exist in the US Intelligence Community today. Indeed, my own experiences and discussions with colleagues at the CIA and FBI have convinced me that such recordkeeping is spotty and agencies often cannot take advantage of the large amount of CI information in their case files.[16]

Counterintelligence Operations

Counterintelligence operations may be defined as operations undertaken to collect information about intelligence services. They are a specialized subset of intelligence operations in general and when successful can create endless feedback loops. Undertaking a counterintelligence operation requires the application of previously collected CI information—for example, it would be extremely difficult to target an intelligence organization without knowing how it is organized, what types of people work for it and how they are trained, and where they operate. All counterintelligence operations have the goal, therefore, of obtaining additional information about how the target service works and details of its operations that, in turn, can be used to refine the understanding of the service's behavior and then be used to feed another round of operations or investigations.

CI operations are a specialized subset of intelligence operations in general and when successful can create endless feedback loops.

Broadly speaking, there are three types of counterintelligence operations. The first is the classic penetration, in which an officer of a service is recruited and provides information from within. Such an operation has

tremendous potential. As the pseudonymous Christopher Felix wrote, a successful penetration "puts you at the very heart" of the target service, and "you are in a position to control [its] actions." More concretely, a penetration may be able to identify spies in the service running him or other services; even if the penetration does not know the identities of any spies, he may provide pieces of information that can lead to their unmasking.[17]

Penetrations also are the best sources of information about the service itself. Even a low-ranking officer will know the service's organization, be able to provide biographical data on colleagues, hear about internal political squabbles, and can provide details on training and operational methods. He or she can also be tasked to fill gaps in reporting, as well as to learn if old reporting remains valid. Over time, a penetration may move up the ranks of the service and gain access to ever more important information, as Kim Philby did for the Soviets and Oleg Gordievskiy did for the British, though even mid-ranking penetrations can be devastating to a service if in the right spots, as was Aldrich Ames.

Unlike in novels or movies, spy hunts often take years as investigators pore over files and assemble fragments of evidence.

The second type of counterintelligence operation involves double agents. A double agent is one who appears to be working for one intelligence service but, in reality, is controlled by another. There are many types of double agents. One may be, for example, either an agent sent by one service to volunteer to another, or an asset of a service who has been discovered by a second service and turned—sent back to spy on the original handlers. Another type of double agent operation is the dangle, in which one service makes a tempting target—say, a military officer, diplomat, or scientist—available to another service to recruit; the dangle behaves passively, allowing the target service to initiate contact and thus believe it has spotted, developed, and recruited an agent.

Both cases have the same goals: if the target service swallows the bait and accepts the agent as a genuine asset (or continues to have faith in a turned asset), the controlling service can learn the identities and vulnerabilities of some of the target's officers, its collection requirements, and tradecraft. These operations can also be used to feed disinformation to the target service as the double agent responds to taskings—in the best

known case of this, the British in World War II turned all the German agents in England and used them in a massive deception operation to fool Berlin.[18]

In most cases, however, doubles and dangles have serious drawbacks. The service running the operation still is looking at the target from the outside and the value of the information it gains likely will be marginal. At the same time, the service must come up with a constant stream of material to feed to the target service, and ensure that it is of high enough quality to encourage the target to keep running the agent rather than to terminate him. Doubles and dangles usually do not provide enough information about the target service to justify the effort.

The final type of CI operation is one that works systematically in a particular location to identify a target service's officers and then, through access agents or physical and technical surveillance, to uncover their activities and contacts. Such operations are rare, however, as it requires many months to identify adversary officers while recruiting, vetting, and training the access and surveillance assets; as the operation reveals more about the target and its assets, the operation grows and requires still more time, expertise, and resources.

The payoffs of this kind of effort, however, can be large. If a service gradually identifies the target's officers and assets, not only does it gain near-real-time information on how an opponent operates—ideally with the target service unaware that it is under close scrutiny—but it can also neutralize the threat from the target by using dangles and double agents or warning off his potential targets. In his memoirs, KGB counterintelligence officer Victor Cherkashin described just such a situation in Beirut, recounting how the local Russian CI chief, Rem Krassilnikov had "set up a good network of agents and was running successful surveillance and eavesdropping operations" against the SIS. A similar operation by the CIA in Vienna resulted in the unmasking of State Department officer Felix Bloch as a Russian spy.[19]

Counterintelligence operations often are described as either defensive or offensive, but the foregoing shows that this is a false dichotomy. Penetrations, for example, usually are classed as offensive operations because the goal is to gain some degree of control over the target service. At the same time, however, a large reason for penetrating an opponent is to uncover any spies in your own service—certainly a defensive move. Similarly, a double agent operation can start as a defensive effort to

identify another service's officers, but may eventually move to offense, as manipulating the target becomes the goal. As with an army's machine guns, all types of counterintelligence operations serve effectively on both the offense and defense, and it is misleading to try to classify them rigidly as one or the other.

Counterespionage

The final area of applied counterintelligence is counterespionage. Counterespionage, which may be defined as investigations or operations undertaken to uncover a spy, is exceptionally difficult work. Unlike in novels or movies, where a dynamic hero finds the spy in a brief, action-packed period, spy hunts often take years as investigators pore over files and assemble fragments of evidence (the Ames investigation took nine years, and finding Hanssen ultimately took about 15 years). Nor is this a job for a lone operator—spy hunting takes experienced analysts, operations officers, technical specialists, lawyers, financial investigators, law enforcement officers, and psychologists, all working as a team. It also requires patience, attention to detail, and a high tolerance for frustration and ambiguity.[20]

Successful counterespionage brings with it new or enhanced knowledge of the adversary.

As with all other counterintelligence work, knowledge of service behavior is fundamental to counterespionage. Some of this is general knowledge of intelligence—how services target and recruit, the principles of running clandestine agents, evaluating conflicting information, and so on. But expertise on particular services or technical areas often is crucial, which means that, while skills such as computer forensics or accounting can be applied to cases across the board, most counterespionage officers still need to specialize in a particular service. The French, Chinese, Israelis, and Russians all operate differently, for example, and finding a spy from one of these services will be a different problem than finding a spy from another.

Successful counterespionage brings with it new or enhanced knowledge of the adversary. When a spy is found, a service may observe his activities

and learn how the other side runs him, or may double him and begin gathering information that way. When a spy is arrested and confesses (as most do), his interrogations will yield a wealth of information about the other side, as well as lessons for his own.

Areas for Further Research

Much work remains to be done in counterintelligence studies and theory building. We may know a great deal about the organizations and selected capabilities of the major intelligence services, but there are none for which we have a comprehensive understanding or catalogue of knowledge at our fingertips, especially beyond the English-speaking countries. Filling these gaps and working toward knowing the inner lives of services would do much to improve US counterintelligence operations and counterespionage capabilities, as well as help develop a theory of counterintelligence. This work will take many years, but work in several areas where relatively little research has been undertaken could quickly pay significant dividends.

The politics of services
Looking at the politics of services should be the highest priority for counterintelligence research. Understanding the internal and external politics of foreign services will give US analysts insights into their strengths and weaknesses, where they can help us or where they will try to harm us, and where we might be able to exploit internal conflicts or other weaknesses.

Service sociology
This is an area that could make a tremendous contribution to our CI operations. Understanding the people who make up a service—their class, ethnic, and social backgrounds, and their values—has the potential to make our own targeting and recruiting efforts more effective. Similarly, understanding the organizational cultures of other services can help identify weak points in their procedures that may provide us with operational openings.

Economics of counterintelligence
No one, to my knowledge, has tried to apply economics to counterintelligence. This is unfortunate, as economics has the potential to help answer some important operational and counterespionage questions.

For example, labor economics can tell us not only how much a spy should be paid, but can also point toward incentive systems—signing and performance bonuses, retirement packages—that might make spying more attractive and hence bring us more volunteers. Similarly, behavioral and organizational economics might contribute to political and sociological studies of services.

Comparative studies
Comparative studies of services is another unexplored field. How various services approach problems that all have in common—coping with political problems, internal security procedures, handling problems with counterpart agencies, how they react when they suspect they have traitors within their ranks—is another avenue for identifying strengths and weaknesses that we can use to our benefit.

Much work remains to be done in counterintelligence studies and theory building.

Literary Studies
While reading spy novels is usually a leisure activity rather than part of the study of services, some espionage writers have much to say that is worth considering in CI work. Joseph Conrad's classic novel The Secret Agent (1907) has much to say about the role of ideology in intelligence work, and Graham Greene's The Human Factor (1978) is an excellent study of the motivations of spies—both should be required reading for counterespionage officers. John Le Carré's early novels, especially The Spy Who Came in From the Cold (1963) and The Looking Glass War (1965) also have valuable insights into CI tradecraft, the politics of CI work, and the bureaucratic workings of services.

A Final Word

As I noted at the beginning, this essay is only a start for the work of developing a robust theory of counterintelligence. The strength of its approach, in my view, is that it places analysis at the center of counterintelligence work but also makes clear the need for a multidisciplinary approach and integrates analytical with operational activities. Nonetheless, as a foundation for theoretical work it remains

incomplete and, in an age when technology and nonstate actors have become important in world politics, probably is too human- and state-centric. With these points in mind, I hope others will contribute to the development of counterintelligence theory and help further develop what this article attempts to begin.

The author: John Ehrman, a frequent contributor, is a CIA officer who specializes in CI issues.

Endnotes

1. George Kalaris and Leonard McCoy, "Counterintelligence for the 1990s," *Studies in Intelligence* 32 (Spring 1988): 75; *The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, Report to the President of the United States* (Washington: 2005), 486 (hereafter, the *WMD Commission*). Michelle Van Cleave, "What is Strategic Counterintelligence and What Should We do About It?" *Studies in Intelligence* 51, No. 2 (2007); and "Foreign Spies are Serious. Are We?" *Washington Post*, 8 February 2009: B3. See also Frederick Wettering, "Counterintelligence: The Broken Triad," *International Journal of Intelligence and Counterintelligence* 13 (September 2000): 265–300.

2. Many of the works on intelligence theory that have been published during the past two decades are notable for having little or no discussion of counterintelligence. See, for example, Richard Betts, *Enemies of Intelligence* (New York: Columbia University Press, 2007); Gregory Treverton, et. al., "Toward a Theory of Intelligence," RAND Corporation Workshop Report, 2006; Len Scott and Peter Jackson, "The Study of Intelligence in Theory and Practice," *Intelligence and National Security* 19 (Summer 2004): 139–69; Loch Johnson, "Preface to a Theory of Strategic Intelligence," *International Journal of Intelligence and Counterintelligence* 16 (September 2003): 638–63; Loch Johnson, "Bricks and Mortar for a Theory of Intelligence," *Comparative Strategy* 22 (January–March 2003): 1–28; Michael Warner, "Wanted: A Definition of 'Intelligence,'" *Studies in Intelligence* 46 (Fall 2002): 15–22; David Kahn, "An Historical Theory of Intelligence," *Intelligence and National Security* 16 (Autumn 2001): 79–92; Stafford Thomas, "A Political Theory of the CIA," *International Journal of Intelligence and Counterintelligence* 11 (Spring 1998): 57–72; and Michael Handel, "The Politics

of Intelligence," *Intelligence and National Security* 2 (October 1987): 5–46.

3. Paul Samuelson and William Nordhaus, *Economics*, 14th ed. (New York: McGraw-Hill, 1992), p. 53.

4. For comparisons of the internal structures of major intelligence services, see Jeffrey Richelson, *Foreign Intelligence Organizations* (Cambridge: Ballinger, 1988).

5. In addition to FISA, some of the major intelligence legislation from the 1980s and 1990s includes the ASIO Act 1979 (Australia); the CSIS Act of 1984 (Canada); the Security Service Act 1989 (UK); the Intelligence Services Act 1994 (UK); the Intelligence Services Act and the National Strategic Intelligence Act (South Africa, 1994); On the Organs of the Federal Security Service in the Russian Federation (1995) and On Foreign Intelligence (Russia, 1996); and the Israel Security Agency Statute (2002).
For analyses of intelligence legislation, see Americo Cinquegrana, "The Walls (and Wires) Have Ears: The Background and First Ten Years of the Foreign Intelligence Surveillance Act of 1978," *University of Pennsylvania Law Review* 137 (January 1989): 793–828; J. L. J. Edwards, "The Canadian Security Intelligence Act 1984—A Canadian Appraisal," *Oxford Journal of Legal Studies* 5 (Spring 1985): 143–53; Murray Rankin, "National Security: Information, Accountability, and the Canadian Security Intelligence Service," *University of Toronto Law Journal* 36 (Summer 1986): 249–85; H. P. Lee, "The Australian Security Intelligence Organisation—New Mechanisms for Accountability," *International and Comparative Law Quarterly* 38 (October 1989): 890–905; Ian Leigh and Laurence Lustgarten, "The Security Service Act 1989," *Modern Law Review* 52 (November 1989): 801–36; John Wadham, "The Intelligence Services Act 1994," *Modern Law Review* 57 (November 1994): 916–27; K. G. Robertson,

6. For the impact on services of oversight, see Loch Johnson, "Ostriches, Cheerleaders, Skeptics, and Guardians: Role Selection by Congressional Intelligence Overseers," *SAIS Review* 28 (Winter Spring 2008): 93–108, and Antonia Diaz Fernandez, "Halfway Down the Road to Supervision of the Spanish Intelligence Services," *Intelligence and National Security* 21 (June 2006): 440–56 For improvements in a service because of legal reforms and oversight, see Royal Commission on Australia's Security and Intelligence Agencies, *General Report* (Canberra: Australian Government Publishing Service, 1985).

7. Author's discussions with US and foreign intelligence officers.

8. For examples of post-failure investigations, see *The 9/11 Commission Report* (New York: Norton, 2004), and *The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction*.

9. For insights into organizational behavior in intelligence services, see Louis Garicano and Richard Posner, "Intelligence Failures: An Organizational Economics Perspective," *Journal of Economic Perspectives* 19 (Fall 2005): 151–70, and Geoffrey Weller, "The Internal Modernization of Western Intelligence Services," *International Journal of Intelligence and Counterintelligence* 14 (September 2001): 299–322. For bureaucratic competition among intelligence services, see Handel "Politics of Intelligence," 17–23, and Thomas, "Political Theory of the CIA," 66–68. For a case study of bureaucratic behavior that may be applied to intelligence services, see Albert Breton and Ronald Wintrobe, "The Bureaucracy of Murder Revisited," *Journal of Political Economy* 94 (October 1986): 905–26. For bureaucratic competition, the classic books remain Graham Allison, *Essence of Decision* (Boston: Little, Brown, 1971), Morton Halperin, *Bureaucratic Politics and Foreign Policy* (Washington: Brookings Institution, 1974), and James Q. Wilson, *Bureaucracy* (New York: Basic, 1989). For the CIA-FBI competition, see Mark Riebling, *Wedge* (New York: Alfred A. Knopf, 1994). Another insightful examination of bureaucratic competition between two intelligence services is John Le Carré, *The Looking Glass War* (New York: Coward McCann, 1965).

10. On the Franklin case, see Stephane Lefebvre, "Spying on Friends? The Franklin Case, AIPAC, and Israel," *International Journal of Intelligence and Counterintelligence* 19 (September 2006): 600–21.

11. For an example of Okhrana penetrations, see Richard Pipes, The Dagaev Affair (New Haven, CT: Yale University Press, 2003), and for the Okhrana's surveillance efforts, see Jonathan Daly, *The Watchful State* (DeKalb: University of Northern Illinois Press, 2004).

12. Richelson, *Foreign Intelligence Organizations*, 72. See also Louise I. Shelley, "Policing Soviet Society: The Evolution of State Control," *Law & Social Inquiry* 15 (Summer 1990): 479–520.

13. Luis Garicano and Richard Posner, "Intelligence Failures: An Organizational Economics Perspective," *Journal of Economic Perspectives* 19 (Fall 2005): 151–70, and Amy Zegart, "9/11 and the FBI: The Organizational Roots of Failure," *Intelligence and National Security* 22 (April 2007): 165–84; Author's discussions with US intelligence officers.

14. *WMD Commission*, 487.

15. For the KGB and dissidents, see Robert Pringle, "Andropov's Counterintelligence State," *International Journal of Intelligence and Counterintelligence* 13 (June 2000): 193–203, and Joshua Rubenstein and Alexander Gribanov, eds., *The KGB File of Andrei Sakharov* (New Haven, CT: Yale University Press, 2005).

16. Alastair Black and Rodney Brunt, "Information Management in MI5 Before the Age of the Computer," *Intelligence and National Security* 16 (Summer 2001): 158–65.

17. Christopher Felix (James MacGarar), *A Short Course in the Secret War* (New York: Madison Books, 2001), 121.

18. For the British use of double agents in World War II, the classic work is J. C. Masterman, *The Double-Cross System* (New Haven, CT: Yale University Press, 1972). Soviet counterintelligence had a similar effort against the Nazis, described in Robert Stephan, Stalin's Secret War (Lawrence: University Press of Kansas, 2004).

19. Victor Cherkashin, *Spy Handler* (New York: Basic Books, 2005), 79; Mark Riebling, Wedge (New York: Alfred Knopf, 1994), 397–99; Milt Bearden and James Risen, *The Main Enemy* (New York: Random House, 2003), 371–75.

20. A good sense of the length and difficulty of spy hunting may be found in David Wise, Spy (New York: Random House, 2002), and Wise, *Nightmover* (New York: HarperCollins, 1995), on the Hanssen and Ames cases, respectively.
