Redmond Counterintelligence Chapter 2010

Loch Johnson, *The Oxford Handbook of National Security Intelligence*, New York: Oxford University Press, 2010, pp. 537-554.

CHAPTER 33

THE CHALLENGES OF COUNTERINTELLIGENCE

PAUL J. REDMOND

1. COUNTERINTELLIGENCE DEFINITIONS

Counterintelligence, known in the trade as "CI," is a complex, controversial subject that is hard to define. Only at the strategic level are there reasonably consistent definitions of counterintelligence. According to the current, official U.S. government definition: "Counterintelligence means information gathered and activities conducted to identify, deceive, exploit, disrupt or protect against espionage, other intelligence activities, sabotage or assassination conducted for or on behalf of foreign powers, organizations or persons or their agents, or international terrorist organizations or activities."[1] A former senior counterintelligence officer of the KGB's First Chief Directorate[2] defines CI as "special activities of security organizations authorized and directed by the government to protect the State and its citizens against espionage, sabotage and terrorism."[3]

The Russians also have an institutional definition for counterintelligence or *kontrrazvedka*--"State agencies granted special powers in the fight against the intelligence services (*razvedka*) of other states and the subversive activity of organizations and individuals used by those services. Counter-intelligence is one of the instruments in the hands of the political authorities of the state" (Mitrokhin 2002).

As is the case with the Russians, a British definition of counterintelligence includes countersubversion--". . . protection of national security against threats from espionage, terrorism and sabotage from the activities of foreign powers and from activities intended to overthrow or undermine parliamentary democracy by political industrial or violent means.[4]"

---

[1] Executive Order 12333, Sec. 3.5, as amended on July 31,2008.
[2] The First Chief Directorate was the foreign intelligence arm of the Soviet KGB, and is now named the SVR.
[3] Colonel General Oleg Danilovich Kalugin, former Chief of Directorate K (Counterintelligence) of the KGB First Chief Directorate, October 2008.
[4] British Security Service Act of 1989.

While these strategic definitions are mostly in agreement in that they mention espionage, sabotage, and terrorism, they encompass a wide diversity of activity, a variety of professional skills, and a range of tactical purposes and means. As a former national counterintelligence executive observed) "Across the profession, there are vast differences in understanding of what counterintelligence means, and how it is done, and even the basic terminology it employs" (Van Cleave 2008). CI means different things to different organizations and intelligence officers) and encompasses a wide continuum of activities from analysis of observed events through the aggressive operational activity of mounting deception operations, from conduct of espionage investigations to the intensely personal, clandestine activity of recruiting and securely managing human sources among the enemy-without simultaneously being deceived.

The U.S. military, which runs "offensive" counterintelligence operations against the enemy, places CI under the overall umbrella of "force protection."[5] The FBI, which is part of the U.S. Department of Justice and is the "lead" U.S. agency in the field, does engage in operational CI activity but it tends to emphasize CI as a law enforcement activity) counterespionage, or the identification and successful prosecution of spies

.

The Central Intelligence Agency embraces under the rubric of counterintelligence a very wide variety of activities. They include the recruitment and management of sources within foreign intelligence services; "asset validation" to prevent the opposition from deceiving the U.S. intelligence community by running sources they actually control; the maintenance of good operational "tradecraft" to prevent the opposition from uncovering American intelligence-collection operations; analysis of the capabilities and intentions of the foreign intelligence opposition; and counterespionage operations with the FBI. To other national security or defense agencies not engaged in operational intelligence activities but rather consumers and analysts of intelligence information or custodians/producers of other sorts of national-security data, counterintelligence means primarily programs to prevent the enemy from stealing secrets. Agencies such as the United States Department of Homeland Security actually engaged in government operations have to design programs to protect not only sensitive technical programs and intelligence data but also to defend, at the tactical level, against terrorist organizations suborning employees to facilitate the infiltration of terrorists and/or weapons into the United States.

539

The end of the Cold War brought even more complications to. the definition and conduct of counterintelligence by the United States. While U.S. intelligence agencies tried) with an almost complete lack of success, to run deception operations against the Warsaw Pact during the Cold War, counterintelligence meant mostly counterespionage

---

[5] Defined as "[p]reventive measures taken to mitigate hostile actions against Department of Defense Personnel (to include family members), resources, facilities, and critical information." Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms, a 0073, amended through October 17, 2008.

against the efforts of the Soviet Union, its allies and, to a lesser degree, China to steal secrets. The break-up. of the Soviet Union mostly eliminated the espionage activity by the states of Eastern Europe but Russia and China have remained counterintelligence threats. Moreover, a host of new ones have emerged including "non-State actors" such as terrorist organizations and the drug cartels. The post-9/11 era has further complicated matters by raising the bureaucratic and operational issues of the relationship between. counterterrorism and counterintelligence, not to mention the perennial conundrum of defining and coping organizationally with the overlapping roles of counterintelligence and security. The intersection of the roles of CI and security leads, in turn, to the question of where the CI function should reside within an organization. Further confounding the definition of CI, the advent of the "cyber" era has raised the issue of "cyber CI" and how a national defense entity protects itself against attacks on its databases, electronically controlled operations, and digital communications.

Even the basic terminology of CI is not universally shared. Different intelligence/security services within the same government use different words. The German Federal Intelligence Service (BND) uses the term "Gegenspionage" which, translated literally, means "the countering of espionage," but the internal security service, Federal Office for the Protection of the Constitution, BfV, uses the term "Spionageabwehr" which means «counter espionage."[6] In English, "counterintelligence)) is even spelled differently: "counterintelligence," "counter intelligence" and « counter-intelligence."[7]

The various organizational positions and levels of status and influence within government agencies that the CI function occupies also reflect the complexity of the subject. Perhaps because of Russia's Byzantine cultural heritage and the conspiratorial roots of the Bolsheviks, the external part of KGB, the First Chief Directorate and its successor organization the SVR, places tremendous emphasis on CI. It maintains an entire organization, Directorate K, in Moscow. The SVR also has a CI career track and a CI section, referred to as Line KR, within each residency.[8] Except temporarily in the aftermath of spy scandals and major operational failures, the CIA historically has put less emphasis on CI. Although it has not established a separate CI operations officer track within the National Clandestine Service, it does have career CI officers at CIA Headquarters and some posted abroad. Perhaps most curiously, during the latter part of the Cold War, the head of CI in one European service also had as his duties legislative and public affairs.

[6] Dr. Dirk Doerrenberg, former Director of Counterintelligence for the BfV, December 2008.
[7] The terms counterintelligence and CI will be used interchangeably in this chapter.
[8] The Russian intelligence representation abroad, the equivalent of a CIA "station" is called a "residency."

This diversity of approach is also reflected in CI's relationship to the security function in various organizations. In the U.S. National Security Agency, the functions are fully merged in the Associate Directorate for Security and Counterintelligence. From the Edward Lee Howard spy case[9] the CIA learned the painful lesson that lack of internal communication can lead to disaster. In this instance, there had been no effective sharing of information among the Directorate of Operations, Office of Security, and Office of Medical Services. As a result, the CIA as an institution did not recognize Howard as a CI threat. At the CIA, counterintelligence and security are still separate organizations, but the interchangeability of personnel appears to make for effective cooperation.

In addition to the complexity of the subject, one other factor makes CI hard to discuss in public. It is probably the most arcane and certainly among the most secret, conspiratorial, and "sensitive" of intelligence activities. Thus, it is a very hard subject to describe to the "uncleared" reader in anything but the abstract. The following discussion of the multifarious aspects of CI endeavors to overcome this difficulty by describing situations and cases. In the interests of security and ease of getting publication clearance, some of these cases have been "sterilized;' but the writer hopes they remain faithful to the lessons they reveal.

Regardless of the complexity of the subject, the diversity of the functions and activities it encompasses, and the "spooky" nature of the business, one basic rule must apply to counterintelligence: "all things in moderation:' Because there was a belief that the Soviets had penetrated the CIA, during the 1960s and early 1970S CI reigned supreme, paralyzing operations against the Warsaw Pact by assuming that the KGB knew of and controlled all operations. During the tenure of DCI William Colby in the mid-1970S, there was a reaction to this mindset that destroyed CI at the CIA and lead to spies in the Agency going undetected and the flowering of opposition-controlled cases. These two periods represent a typical sine wave of either too much or too little CI in the U.S. intelligence community. The waves oscillate in radical reaction to the previous peak, rarely staying in the moderate range required to deal rationally with the hard issues of counterintelligence.

2. THE VARIOUS ASPECTS OF COUNTERINTELLIGENCE

2.1 Counterintelligence as Counterespionage

"Catching spies;' or counterespionage, which is the detection and neutralization of human spies, is probably the first thing that comes to mind when the general public

thinks of "counterintelligence." It is also the easiest to describe since there are many well-documented, important spy cases. This is indeed a very important aspect of CI. During

[9] Howard, a former CIA case officer, was identified in 1985 as spying for the KGB, and escaped to the USSR where he subsequently died.

the Cold War, the Warsaw Pact and its allies such as Cuba had spectacular success in penetrating every U.S. government agency engaged in national security (except apparently the Coast Guard), most defense contractors, and the U.s. Congress. An informal historical review of Cold War spy cases shows that at anyone time there were at least seven significant spies working for the enemy in the U.S. national security establishment.

During that tense era in international affairs, four spy cases alone could have given the Soviet Union a decisive advantage if war had broken out. The Walker spy case in the U.S. Navy[10] provided cryptographic key material and encryption equip¬ment design data enabling the KGB to read over a million messages, which would have allowed the Russians virtually to neutralize the deterrence of the American submarine-based missile systems. The Clyde Conrad spy ring[11] provided the Soviets, via the Hungarian military intelligence service, the details of the U.S. Army's operational plans and communications in Western Europe, which could have provided the Warsaw Pact a decisive advantage in a ground war in Western Europe. Robert Hanssen, who worked for both the KGB and GRU[12] off and on for about twenty years before his arrest in 2001, passed the Soviets enough documentary data to neutralize U.S. efforts to continue a viable democratic government in time of a nuclear war. Aldrich Ames, an equally notorious spy who worked for the KGB for about nine years until he was arrested in '994, compromised nearly all the CIA's human sources working against the Soviet Union in the mid-1980s.

These four spy cases capture the spectrum of ways in which espionage cases begin. The Ames case resides at the end of the spectrum that is hardest to pursue, empirical indications that there is a problem-secrets are getting to the opposition but no clues as to how. In the mid-1980s, the KGB started, in a rather rapid-fire manner, to arrest CIA's Soviet sources. After a period of analysis, false trails, and inattention to the problem, a joint CIA-FBI examination of the very large number of officers aware of the compromised cases produced a small number of people on whom to concentrate. This process eventually focused on Ames, chronologically linking his operationally approved contacts with a Russian in the Washington embassy to financial transactions. When combined with some suggestive source reporting, this effort enabled the FBI to mount a very skillful investigation culminating in his arrest.

The Ames episode represents the extreme difficulty of pursuing a case when the only way to attack the problem is massive analysis of the people aware of the cases compromised. So-called knowledgeability or "bigot lists" are a farce in the U.S. government.

---

[10] 10 John Walker, a U.S. Navy Communicator, started working for the KGB in 1968 and along with his brother, son, and a friend spied for the Soviets for about seventeen years.
[11] Conrad, a retired U.S. Army Sergeant, was arrested in 1988 as part of a spy net in the U.S. Army, which by that time had existed for seventeen years.
[12] The GRU is the Russian military intelligence service.

Even in the rare cases where good records actually exist, they are almost useless because hundreds of employees can know about an operation. The FBI found in the mid-1980s [?] they could not pursue the compromise of a Soviet source because about 250 people in one field office alone had knowledge of the operation (Bromwich 1997). On the other hand, non-American CI officers can have an easier time both in protecting their operations and investigating losses. Knowledgeable CI professionals in the U.S. government estimate that fewer than ten KGB officers knew the identities of Ames and Hanssen, and a former senior Greek intelligence officer recently stated to the media that only three of his colleagues knew the identity of Steven Lalas, a State Department communications officer who spied for the Greeks from 1977 to 1993.[13]

So-called lead information is helpful in starting and pursuing an espionage investigation in direct proportion to its specificity. Multiple CIA human sources in three different Warsaw Pact intelligence services provided information over many years that the Hungarian Military Intelligence Service had a very valuable source in the U.S. Army's V Corps in Germany. Through one human asset involved in the actual processing of the product but not knowledgeable about the source, the CIA was even able to inform the Army of specific documents passed and the disturbing fact that amendments to operational plans were occasionally reaching the Red Army Headquarters in Moscow before they were issued to U.S. forces. Eventually, after many years and a massive investigation based on a large accumulation of diverse lead material, plus some good luck, the Army was able to identify Clyde Conrad (and a net of associate spies) as the source. Conrad was subsequently arrested and successfully prosecuted by the Federal Republic of Germany. The CIA had multiple sources reporting on the case. However, because of excellent compartmentation within the Warsaw Pact intelligence services, no single source had more than a few small pieces of the puzzle. As a consequence this very damaging operation ran for many years before enough information accumulated to allow the U.S. Army investigators to focus on Conrad.

While "lead information" is much more valuable than a well-founded suspicion of a CI problem, the pursuit of leads can be extraordinarily difficult and fraught with the potential for mistakes. For years the CIA and FBI fruitlessly pursued lead information from the 1960s indicating that a CIA officer had volunteered to provide information on the Agency's operations in the USSR. Many years later during the course of the intensive research which led to the Aldrich Ames spy case, it became clear that this "old lead" from a Soviet intelligence source was his garbled version of a U.S.-controlled volunteer, a walk-in to a Soviet installation in the United States. In the early 1980s, the CIA received from two separate, well-placed KGB officers similar information that a CIA "communicator" had an operational meeting with the KGB in a North African city during a particular time period. The Agency and the FBi chased that "lead" for years until it became clear, following his arrest, that John Walker was the person the Soviets met on

[13] Statement of retired General Nikolaos Gryllakis, former head of Greek security. Undated translation/transcription of Greek television show, "Fakeli" (files).

that occasion. At that time, senior and middle-grade KGB officers apparently assumed all communicators worked for the CIA.

The Walker spy case illustrates how empirical data pointing to a CI problem and general lead information is not enough to unearth a spy. During the 1970s and early 1980s, Navy flag officers had expressed anger and extreme frustration that Soviet electronic collection ships seemed to appear regularly at just the right places and times to conduct intercept operations during U.S. naval maneuvers, particularly in the Mediterranean. This was an obvious indication that the Soviets somehow had insight into U.S. operational planning. During this period the CIA did disseminate one CI report from a Soviet intelligence officer who alleged that the USSR had achieved massive success in reading U.S. Navy communications. Even if these two straws in the wind had been considered together, which they probably were not, they did not provide a sufficient basis to attack the problem. The start of the case had to wait until the best kind of lead came along, the specific identification of a spy by a source, or, as in this case, a "snitch." Walker's former wife, apparently drunk, called an FBI office to say her husband as a spy; the FBI acted on the lead and Walker was eventually arrested. Often the problem with pursuing snitch leads is persuading superiors to take them seriously, as happened in a case involving another KGB penetration of the U.S. Navy, when security authorities discounted the statement of a discontented wife that her husband was a spy and his espionage career thus ran four years longer than it should have.

The other cases illustrate the supreme value of specific source information, the other end of the continuum from purely empirical indicators of a CI problem. Resourceful and persistent operational work by the FBI, with help from the CIA led to source reporting unambiguously identifying Robert Hanssen as a spy (Risen, 2003 A1). Likewise, the KGB defector Vitaliy Sergeyevich Yurchenko[14] provided enough specific information to enable the CIA within minutes to identify former employee Edward L. Howard as a KGB asset.

Other factors also play a role in starting espionage investigations. Through the security/polygraph process the CIA has identified individuals who had been directed to apply for employment by foreign intelligence services and most recently, apparently by terrorist organizations.[15] The espionage investigation of Jonathan Pollard[16] was started because of the alertness and CI consciousness of a fellow employee. While the KGB, with its massive resources, caught U.S. spies in the USSR through surveillance of CIA officers, only rarely have Western security services had similar success.

---

[14] Vitaliy Sergeyevich Yurchenko, a senior KGB counterintelligence officer, defected to the CIA in Rome in August 1985 and redefected to the USSR three months later.

[15] The prospect of a polygraph examination has also deterred existing spies from applying to CIA for employment or accepting an assignment there.

[16] Jonathan Pollard, a U.S. Navy civilian intelligence analyst, was arrested in 1985 for spying for Israel.

Defectors represent a special case as sources of spy leads. Historically, they have been gold mines for data in starting investigations; but once the excitement of their defection is over, they have told all that they know and attention toward them lags, they often start to make up stories. During the effort which led to Ames's

identification as a spy, a defector from the then KGB's internal security component, the Second Chief Directorate (now FSB), concocted a story for his American handler about the recruitment of a CIA officer in Moscow. It turned out that he made up the story to retain the attention of the CIA and FBI. All espionage investigations should view all spy leads with skepticism, at least initially, and they should judge leads on Oscar Wilde's principle that "the truth is rarely pure and never simple."

Another maxim which applies to counterespionage and CI in general is "your CI capability is only as good as your records." Leads to spies are more often than not ambiguous and fragmentary. CI analysis has been described as trying to do a monocolor jigsaw puzzle with pieces fitting in multiple places or not at all, or more simply, the archaeological reconstruction of shards from a broken pot. Records in the form of formal data in storage or, as was the case in the two examples cited below, institutional memory, are invaluable in resolving leads. In the mid-1980s, a European service obtained from a source in a Warsaw Pact intelligence service the detailed description for a dead drop site that the source knew only had been cased and. written up for an important spy. Investigation and surveillance of the site proved fruitless. Several years later, a CIA source in another country identified a spy who was connected to the dead drop site, thus reinforcing the evidence against the spy and resolving the original lead. The connection was made only because the intelligence officers involved happened to remember the original dead drop data, not because there were organized holdings of such information.

Another case where institutional memory played a major role involved an informal discussion between a CIA officer and a senior member of a European service. The subject was lead information to KGB penetrations in the U.S. computer industry, where the principal spies had European and South Asian connections. The Western European officer noted the leads "sounded" similar to information acquired from a completely different source several years earlier. He went home and confirmed his suspicions from his service's rather good records and the CIA eventually found similar data residing in the proverbial shoe box under a desk. The connection of the data considerably expanded and refined the investigation. It is hoped that the advent of the cyber era and "link analysis" is now being used to correlate leads and identify spies more systematically. However, data processing and manipulation should not be viewed as a substitute for professional expertise gained by career CI professionals with years of experience. The two CIA officers who played the major role in identifying Aldrich Ames as a spy followed their instincts in focusing on him as a candidate and, using their vast knowledge and experience, were even able to accurately construct, from fragmentary data before his arrest, a significant part of his KGB meeting plan.

2.2 Counterintelligence as "Asset Validation"

The vetting of sources or "asset validation" usually, and too narrowly, is applied to human sources by American intelligence services. This counterintelligence function is at the very heart of all human collection operations and it should be applied also

to technical collection and SIGINT operations.[17] It is critically important to determine to the degree possible that the source is not a fabricator or under opposition control. The disastrous CURVEBALL source, who reinforced the Bush administration's predisposition to believe Iraq had a weapons-of-mass-destruction program, is a classic example. He was a source of German intelligence that was dealing with the Pentagon's Defense Humint Service (DHS), and he was never properly vetted until after his data were used to support the invasion of Iraq. It is equally critical to determine, if possible, whether a source may be under the control of the opposition and thus used to provide disinformation or lure officers out onto the street for a contact, where they can be apprehended and noisily declared persona non grata.

During the Cold War, the Warsaw Pact and its allies enjoyed spectacular success in running controlled cases against the CIA. During much of the Cold War, all the ('sources" the CIA was running against Cuba were controlled by its intelligence service. With a very small number of possible exceptions, the same parlous state of affairs existed in the operations against East Germany. The KGB, unlike most Western intelligence services, reflexively favored running controlled cases and mounted many "dangle" operations.[18] The same conspiratorial mindset that motivated the KGB to attempt many controlled operations led them, as a matter of course, not to trust their own sources. Thus they engaged intensively, one might say obsessively, in testing and validation. In the mid-1980s American CI officers were amazed to learn that a former U.S. military officer was still the subject of elaborate testing by the KGB about ten years after he started working for the Soviets and had been of enough value to meet personally with a KGB general and directorate chief.

It is clear that the Warsaw Pact's success in running cases against American intelligence was at least partly a function of American naïveté, lack of professionalism,

---

[17] SIGINT or signals intelligence is one of the many examples of "int" terminology including MASINT, IMINT, and HUMINT imposed on the U.S. government by the Department of Defense. Some civilian, professional intelligence officers prefer "human espionage" to HUMINT.

[18] 18 "Dangle" is the term of art for an individual controlled by a CI service who is put in the way of a hostile service, making himself as attractive as possible in the hope the service will take him on as an agent, a "double agent." The American media, displaying their usual ignorance of the intelligence business, have taken to describing spies such as Aldrich Ames and Robert Hanssen as "double agents," apparently because they were employees of intelligence organizations. They should be labeled spies or penetrations.

and the refusal of officers to believe their case could be a fabricator or controlled by the opposition, particularly when promotions were involved. It must be emphasized, however, that asset validation is a very difficult task, particularly when the source is handled in a "denied area"[19] and there are few, if any, other sources of "collateral" information on which to rely for comparison. Most Western intelligence sources in denied areas are "met" only briefly for a very quick passage of information or are handled impersonally by dead drops or clandestine electronic communications. There is no regular opportunity for personal meetings and the type of

systematic debriefing that can identify and pursue issues related to the source's validity. In the absence of any sources of its own within the opposition service to warn them, Western services running cases in denied areas have had to rely on the value of the intelligence provided, corroboration of its validity by other sources, if available, and the operational circumstances surrounding the case-particularly how it started.

This is a very complicated, difficult business. It is not a science. In one Warsaw Pact country in the 1970s, an individual purporting to be an officer of the internal security service volunteered by note to the CIA. He was handled impersonally by dead drop over many years and provided valuable information concerning his service's plans to run controlled cases against the CIA and other operations against the U.S. embassy. He even warned of an impending ambush by the internal security service. Because he had been of established value, CIA CI officers were stunned to learn, at the end of the Cold War, that the case had been controlled from the begiuning. It appears that his country's internal security service, taking the long view so alien to Western services, was trying to establish him as a contingency asset for a major disinformation operation in the future. It is noteworthy that the only doubts about the case were expressed by the iuitial case officer who picked up the first dead drop. He observed people in the area and expressed the view that they might have been surveillants. This case reinforces the informal maxim of some CI officers: "the answer (to the validity of the case) always resides in the first 10-15 pages of the file."

A source in another Eastern European country had been providing valuable, validated military R&D data for many years when his handling officer was ambushed by the security service when meeting the asset on the street in the capital. CI officers at the CIA assumed the source had been compromised because of a mistake on his or the Agency's part and only learned to their amazement after the Cold War that the case had been controlled all along. The Eastern European service had been running the case for years to have something "on the shelf" to use against the CIA, should the need arise. As the chief of the service said, he did not care that they were passing valu¬able information because it hurt only the Russians, not his own country.

---

[19] "Denied area" is an intelligence term of art describing an extremely hostile operational environment with heavy surveillance.

Three other cases illustrate another aspect of how the validation of sources is not easy and a decision to declare a case controlled should not be made lightly. At the height of U.S.-Soviet tensions in the 196os, an East European intelligence official living behind the iron curtain volunteered to American intelligence and started providing CI information on Warsaw Pact spies in the West. While the information appeared to have potential, CI officers began doubting his bona fides when he also began suggesting that Western intelligence officer's travel into other Eastern European countries to recruit senior communist intelligence officers whom he believed to be disaffected. Given the Cold War atmosphere and the operational con¬ditions then prevailing behind the iron curtain, such suggestions were ludicrous. Some CI officers, not unreasonably, concluded that he was a controlled case trying to lure the CIA into an operational fiasco, in Eastern Europe. Nonetheless, the CIA and an allied service continued to run the case and he turned out to be the one of the most valuable sources of CI information in history. It became clear over time

that the individual was mentally unstable and his outlandish operational suggestions were the result of his ignorance of life on the other side of Lthe iron curtain and his assumption that Western services were as powerful as those in the Soviet Bloc.

The Soviet engineer who started volunteering by note during a- period when timid management precluded the Agency from replying tohis overtures is another example illustrating the need to persevere despite well-founded, in fact compelling, doubts. Because of the CIA's passivity over a considerable period of time, the engineer eventually out of frustration pounded on the trunk of the car of a U.S diplomat who was filling his tank at one of the diplomatic gas stations in Moscow, an area very well covered by KGB surveillance, both static and mobile. The combination of this suicidal means of volunteering, plus the obscurity and initially incomprehensible nature of the data provided, logically led officers at the CIA to believe he was a controlled case, until knowledgeable engineers and experts in the DOD determined that his production was extraordinarily valuable. That case turned out to be the most significant run by the CIA against the USSR during the Cold War.

Another case involved risk taking. The CIA had been running a source in Europe who returned to Moscow with the expectation of being assigned to an office with access to a veritable gold mine of military information. After his return home) a source provided the CIA enough information to make it clear that the KGB had learned something of the operation but was apparently following an investigative avenue that probably would not lead quickly to this potentially superb source. He eventually signaled for a contact and CI officers had to calculate the odds on whether the KGB had found him and was setting the Agency up for an ambush. Based on a seat-of-the-pants assessment of known KGB investigative intentions, the likelihood of a huge payoff in intelligence product, plus a lot of hope, the CIA decided to make the contact. It came off without incident and produced a massive amount of very valuable intelligence.

The in-place source or defector who does not tell you all he knows, either to protect himself or to apply future leverage, is another challenge to asset validation. The most famous such case is Alexander Orlov, a senior Bolshevik intelligence officer, who defected in Canada in 1938 because he thought he was about to be assassinated as part of the Great Purge. He knew the identities of most of the important spies working for the Soviets in the West, including the high-level penetrations of the British government; but he did not reveal this information, having sent a message to Stalin via the head of Bolshevik intelligence saying that he would tell all if anything happened to himself or his family. The only effective way to get a full debriefing from a source inclined to hold back is to subject him to an officer with an in-depth, intimidating knowledge of the subject matter and good human-relations skills. When the principal CIA case officer handling Colonel Oleg Penkovskiy[20] first met him in a hotel room in London, he asked him whether so-and-so (by first name

and patronymic) had issued him the dreary sack of a suit he was wearing. So-and-so was the apparatchik who issued civilian clothing to Soviet military intelligence officers traveling abroad. The intimate knowledge on the part of the CIA officer would have sufficiently impressed Penkovskiy and created enough rapport to minimize any inhibitions.

While it depends on disciplined attention to detail, great expertise, unbiased analysis, healthy skepticism, and sense of conspiracy, asset validation, like counterespionage, is not a science or a bureaucratic exercise. It is an art which is aided greatly by an experiential, intuitive understanding, in other words, "feel." One noteworthy case involved an engineer who volunteered in Moscow with plans for a new Soviet aircraft. The initial approach of this would-be source and data provided simply did not "feel" right to the CI officers examining it in Washington. There was simply something "off" about his "presentation." When overhead satellite coverage imaged an aircraft on a runway which resembled the volunteer's reporting, some CI officers asked "How much plywood and balsa wood did it take to build that fake?" The volunteer did turn out to be controlled. On the other side of the coin, similarly skeptical officers were on too many other occasions successfully fooled by the KGB, which resulted in the loss of operational techniques, noisy persona non grata decla: rations, and some successful disinformation operations.

The vetting of SIGINT information and sources, and the product of other technical collection operations, is one of the most difficult and perhaps the most controversial aspect of "asset validation." The SIGINT practitioners stand on the assertion, "SIGINT never lies." SIGINT is often based on cryptanalytic successes or major technical collection breakthroughs and it is almost impossible for intelligence officers to gain enough access to the operations to make independent judgments about the

[20] Penkovskiy was a Soviet military intelligence officer who worked for the United States and Great Britain from 1960 to 1962.

sources. SIGlNT, as now practiced in the West, presents a fertile area for the opposition to engage in deception and disinformation operations.

3. COUNTERINTELLIGENCE AS DISINFORMATION OPERATIONS

The section above on source vetting described the difficulties of determining whether a human source is valid. This section looks at the issue from the other side: the purposes and techniques of running operations against the opposition, in order to control their activities, misinform them, trap them, or get them to reveal their operational techniques and capabilities. In the early 1920S, the State Political Directorate (OGPU) of the Soviet Union penetrated existing, anti-Communist· organizations. Instead of eliminating them, it co-opted and expanded them into an organization that had the operational name, "The Trust." This control enabled the OGPU effectively to neutralize a large part of the opposition to the Bolsheviks.

During World War II deception and disinformation played a vital role in operations against Germany. Prior to the Normandy invasion in 1944, the British used apprehended Nazi -spies, along with a massive disinformation campaign involving the creation of an entirely fictitious Allied army corps, to persuade the Germans that the invasion would be directed against the Pas de Calais, not Normandy. The success of this operation was, of course, founded on superb British CI operations, which identified and neutralized all Nazi sources in Great Britain, thus eliminating any sources still working for the Germans who could have cast doubt on the information provided by those under British control. The British were also greatly aided in this effort by excellent intelligence on German reactions to the deception campaign afforded by successful decryption of German military communications. Another spectacular World War II success involved au elegant, if macabre, operation in which the British arranged to have float ashore in Spain the perfectly documented corpse of an ostensibly drowned British officer carrying fake war plans. The corpse successfully misled the Germans into thinking the allies intended to invade Sardinia and Greece instead of Sicily. In this operation, the British illustrated their skill at disinformation, counterintelligence, and attention to detail, by using the corpse of an individual who had died of pneumonia, a cause of death that appar¬ently displays pathological signs similar to drowning.[21]

After receiving data from Aldrich Ames on almost all CIA's human source operations against the USSR in 1985, the KGB, apparently under pressure from the Soviet leadership, quickly started arresting these sources, which ran the risk of alerting CIA to a CI problem and jeopardizing Ames. To mitigate this risk, the KGB CI Directorate conducted a number of disinformation operations to try to explain away the compromises of the American sources. In the summer of 1985, a KGB officer working for the CIA in Africa who was compromised by Ames went on home leave carrying operational directions to a dead drop containing a large number of rubles, which he

[21] This operation is described in the 1956 movie, *The Man Who Never Was*.

planned to spend while on vacation. He did not return from home leave. Instead the CIA received information from a source in Europe that the officer had been arrested picking up the dead drop in Moscow. At about the same time, the CIA and FBI received essentially the same story about this compromise from another KGB source. After Ames was identified as a spy, it became clear that the KGB knew that both the sources were working for the Americans and, to protect Ames, used them as unwitting vehicles to misinform U.S. Intelligence before they found ways to lure the officers back to the USSR.

The United States intelligence community has not distinguished itself in running controlled sources against the opposition. While the U.S. military allegedly had success in running "perception management" operations against Iraq before operation Desert Storm, the American effort during the Cold War was consistently unsuccessful. The U.S. military policy is that "Offensive Counterintelligence Operations" (OFCO) are run to protect and enhance national security. The Defense Intelligence

Agency subscribes to the following succinct objectives of double agent operations as summarized from the book, *The Double-Cross System* by Sir John C. Masterman. The objectives are: 1. Control the adversary's espionage system and by doing so, in effect make him work for you. 2. Identify, neutralize or suppress new agents and spies. 3. Obtain information on the personnel and methods of the adversary service. 4. Secure access to adversary codes and ciphers 5. Gain evidence of the adversary's intentions. 6. Influence the enemy's operational intentions. 7. Systematically deceive the enemy (Masterman 1972). Item 5 represents a very important example where "counter" intelligence can greatly assist "positive" intelligence. Considerable insight into an adversary's policies and intentions can be gained from knowing the thrust and focus of his intelligence-collection activities.

In its own operations and in cooperation with the military services, the FBI has sought to convince the opposition of a dangle's value in an effort to induce hostile intelligence services to handle the operation in the United States, which would give the Bureau very valuable information on how they operate in America. The CIA, with very rare exceptions, has not tried to run controlled operations; rather it has served merely to coordinate such operations run abroad by other agencies.

The lack of U.S. success in this area during the Cold War is at least partly attributable to the KGB's success in penetrating U.S. intelligence. Ames and Hanssen, complemented by other lesser-known sources in the military, provided the KGB with detailed information on the double-agent program, all the doctrine, the complete "play book" of operational techniques and many, if not all, the specific operations. The apparent success of deception operations against Iraq prior to Desert Storm bespeaks a salutary improvement in the U.S. CI posture, because it shows Saddam Hussein did not have the valuable sources within the U.S. intelligence establishment enjoyed by the KGB.

4. COUNTERINTELLIGENCE AS OPERATIONAL TRADECRAFT

In any organization engaged in intelligence collection, the imposition of the highest possible standards of operational security, or tradecraft, is a critical counterintelligence function, particularly in the intelligence services of Western democracies. Unless the discipline of good operational security is forcefully imposed on the average American case officer,[22] the default will be sloppy or non -existent tradecraft.

551

Putative sources will be met in the dining room of a posh hotel literally next to the U.S. embassy. Operational failures will be explained away by the case officer's statement that he was using "semi-clandestine" tradecraft, and officers operating in alias abroad will call home on cell phones. In the early twenty first century the use of sloppy tradecraft presents the U.S. intelligence community with a daunting and critical challenge. An entire generation of new American case officers is getting its initial, formative, "(on- the-street" experience in the war zone of Iraq, meeting sources with armed aud sometimes armored military or paramilitary escorts or within fortress compounds. This sort of "trade craft" bears' no resemblance to the clandestine operational activities required to recruit arid manage human sources elsewhere.

5. COUNTERINTELLIGENCE AS THE RECRUITMENT AND RUNNING OF CI SOURCES

The very best way to engage in counterintelligence activities is to have a valid source, or preferably sources, in the opposition service who can tell you what spies they have, or are trying to develop, in your government or defense industries; what technical, cyber, or disinformation operations they are running or plan to mount; and what they are doing to detect and negate your own intelligence-collection operations. The acquisition of such sources is a controversial subject. It is a fact that most of the productive counterintelligence sources acquired by the West during the Cold War were volunteers. Armchair media and academic experts advocate a passive approach, denigrating the use of resources to pursue actively the recruitment of foreign intelligence officers. This approach ignores a significant fact. Many of the volunteers acted only after, and probably as a result of, exposure to, and cultivation by, American intelligence officers. In addition, to get the most from a source requires cultural understanding and great substantive expertise, which cannot be learned from a file, book, movie, or television series, and can be gained only by close, long-term engagement with the opposition.

---

[22] 22 The term "case officer" has been used to designate the operations officer who manages a human source or, in a broader sense, the officer in charge of a technical collection project. Under the influence of Washington-based personnel professionals, this title apparently has been replaced by the bureaucratic term "core collector."

Unfortunately, the best example of an extraordinarily productive counterintelligence human source is FBI Special Agent Robert Hanssen, who volunteered to and worked for the KGB and GRU off and on for about twenty-one years. Over his spy career Hanssen informed the Soviets/Russians of human-source operations the CIA and KGB were running against the Soviet Union/Russia; some truly exquisite and productive technical and SIGINT collection operations; details of the double-agent program; and, of signal importance, full details of the FBI's counterintelligence program and operations against the Russians. This latter body of data gave the KGB/ SVR an enormous advantage in acquiring and managing sources in the United States.

6. COUNTERINTELLIGENCE: DEVELOPING ISSUES AND CHALLENGES

Much of the material used above to describe the various aspects of counterintelligence is of Cold War vintage. Even though that body of historical data continues to shed light on the modalities of CI, several new factors and issues must be taken into account, not least the role of counterterrorism.

6.1 Counterintelligence and Counterterrorism

The practical goals of counterintelligence and counterterrorism (CT) are identical: the identification and neutralization of secret organizations engaged in secret operations to attack the United States and its allies. However, the difference in the nature of the threats has caused U.S. bureaucracies to separate the functions, particularly at the CIA and the FBI. Counterintelligence professionals thus face the challenge of ensuring that all the rules and standards of their discipline, such as operational security/tradecraft, asset validation) and counterespionage, aIe observed in the CT arena.

Since the Cold War never led to a military clash between the superpowers, the CI emphasis was on uncovering and neutralizing espionage, that is, on the stealing of secrets. The United States and some of its allies are now engaged in shooting wars and it must defend against sabotage and terrorist attacks both by state and "non-state" entities. Therefore CI must work to protect not just secrets, but installations, operations, comn1unications, and data storage as well as people. Today a hostile intelligence entity might be just as likely to be planning to kill or kidnap a U.S. official as to recruit him as a spy. Civilian CI officers should recognize the increasing relevance of the U.S. Department of Defense's concept of "force protection," which includes CI in a broad program of security disciplines to protect people, facilities, equipment, and operations.

6.2 Counterintelligence: The Cyber Threat and Denigration of Compartmentation

The so-called cyber threat has recently been described as the "new frontier" of counterintelligence. The cyber era has greatly complicated the work of counterintelligence officers. It is now much easier for an insider to steal vast amounts of national security information simply by downloading data onto devices such as thumb

drives or to insert "malware" into networks to facilitate data exfiltration from remote platforms when plain hacking has been unable to penetrate the network.

There exists at the human, professional, and management levels a mutual dis-affinity between CI officers and the "computer people." The former are mostly the proverbial "social science majors" who are not computer experts and who, by experience, think in terms of human spies. The latter, by technical training and experience,

are motivated to create the smoothest flow of data to as many people as quickly as possible. The technical approach is best illustrated by Deputy Defense Secretary Paul Wolfowitz's statement that "the U.S. intelligence system needs to be adapted to the information age ... we must emphasize speed of exchange and networking to push information out to people who need it, when they need it, wherever they are" (Inside the Pentagon 2002)

The complications for CI created by the onset of the computer age are being exacerbated by the post -9/11 conventional wisdom that failure "to connect the dots" led to that disaster. The 9/11 Commission Report emphasized the need to change the "mind-set" in the intelligence community from "need to know" to "need to share" (Director of National Intelligence 2008, 6). The Director of National Intelligence, Vice Admiral J.M. McConnell (Ret.), and his Associate Director and Chief Information Officer Major General (Ret.) Dale Meyerosse, took the policy a step further by decreeing that "need to share" would become "responsibility to provide" (Director of National Intelligence 2008, 9). Regardless of the lip service paid to security and statements about "managing risk;' this new policy will inevitably lead to a further breakdown in compartmentation, as more and more networks are interconnected, easing the work of spies and making the work of identifying and neutralizing them more difficult.

In addition to the understandable tendency of the computer people to speed the widest possible dissemination of data and the post-9/n mindset to do away with "need to know;' the American tendency to think mostly in terms of technical solutions comes into play in the issues facing counterintelligence. The National Counterintelligence Executive has recently emphasized that " ... computer architecture and the soundness of electronic systems" are a key CI issue (Warrick and Johnson, 2008, AlA). Professional CI officers thus face three major challenges. One is to remind management that people are always involved, whether as an insider spy or as an opposition intelligence officer attacking U.S.-national-security organizations through electronic means. The second challenge is that CI professionals must learn enough about data processing and networks to communicate and work effectively with information management officers. Only with this basic knowledge can CI officers force a rational balance between information flow and dissemination and the need to find technical ways sensibly to restrict data and to establish techniques and procedures quickly to identify the inevitable hostile activity within and among networks. This issue presents intelligence officers with the third challenge: to

inculcate CI awareness into the professional culture of information-technology professionals, who alone have the expertise to design the necessary policies and systems.

6.3 Counterintelligence: Law Enforcement and National Security

Another dysfunction similar to that between CI officers and computer experts exists between CI officers and law enforcement. Counterintelligence officials are intent on protecting national security by identifying and neutralizing threats posed by hostile

intelligence entities. Law enforcement' officers at the U.S. Department of Justice (DOJ) are almost exclusively focused on making successful prosecutions, with the result that once the arrest of a spy is imminent or has taken place, CI considerations are not allowed to come into play. For instance, in one recent case, DOJ prosecutors included in the charging documents all of the considerable body of data known to have been passed to the opposition by the spy in order to intimidate him into accepting a plea agreement. While that ploy succeeded, CI officers were greatly hampered doing a damage assessment because the spy and his lawyer quickly figured out precisely what the government knew and refused, despite the terms of a plea agreement, to expand on its knowledge.

In another instance, CI officers gained personal access to a foreign intelligence officer who had been handling a minor spy in the United States. That officer, in effect, volunteered to help the CI officers but the government chose to go ahead with an arrest and well-publicized prosecution, which eliminated any chance the officer would help U.S. authorities identify other spies the foreign intelligence service was running against the United States. Another incident involved a technical collection operation uncovered by outstanding CI work. Law enforcement officers at the management level would not even consider using the still-secret discovery for a possible disinformation operation. Rather, they insisted on a public announcement of the find and a noisy expulsion of a foreign intelligence office. American CI professionals face the challenge of stimulating discussion at the National Security Council level to determine whether national security issues can be given equal importance to prosecutorial considerations in such cases.

REFERENCES

Bromwich, M. R.1997. *Office of the Inspector General Department of Justice Report, A Review of the FBI's Performance in Uncovering the Espionage Activities of Aldrich Hazen Ames*. Unclassified Executive Summary (April 21).

Director of National Intelligence. 2008. *United States Intelligence Community Information Sharing Strategy* (February 22).

Inside the Pentagon. 2002. *Deputy Defense Secretary Backs New Approach to Processing Intelligence* (September 26).

Masterman, J. C. 1972. *The Double-Cross System in the "War of 1939 to 1945*. New Haven, Conn.: Yale University Press, 1972.

Mitrokhin, V. 1., ed. 2002. *KGB Lexicon, The Soviet Intelligence Officer's Handbook* London: Frank Casso

Risen, J. 2003· "Jailing in Russia Is a Reminder that Spy Wars Still Smolder," *New York Times* (June 16): A1.

Van Cleave, M. 2008. "Meeting Twenty- First Century Security Challenges 2008 The NCIX and the National Counterintelligence Mission: What Has Worked, What Has Not and Why." *Washington Post* (April 3): A1.

Warrick, J., and C. Johnson, 2008. "Chinese Spy 'Slept' in U.S. for Decades." *Washington Post* (April 3): A1.