From AFIO's THE INTELLIGENCER
JOURNAL OF U.S. INTELLIGENCE STUDIES
VOLUME 20 • NUMBER 2 • $15 SINGLE COPY PRICE Fall/Winter 2013 ©2013, AFIO

ASSOCIATION OF FORMER INTELLIGENCE OFFICERS
7700 LEESBURG PIKE, SUITE 324
FALLS CHURCH, VIRGINIA 22043
Web: www.afio.com, E-mail: afio@afio.com

Guide to the Study of Intelligence

What is Counterintelligence?

A Guide to Thinking and Teaching about CI

by Michelle K. Van Cleave

WHY STUDY COUNTERINTELLIGENCE?

The study of "counterintelligence" is rare in academia. While modern courses on international relations often include intelligence, they usually fail to consider how countering foreign intelligence activities is also an instrument of state power. No inquiry into intelligence theory or practice is complete without addressing the meaning and scope of counterintelligence.[1] What is the value of intelligence if you cannot assess its reliability or truth?

Counterintelligence (CI) is intertwined with our history, laws and ethics, and major espionage cases have affected American society and politics from German saboteurs and communist movements to terrorist cells today.[2] The CI mission that supports and is governed by our Constitution and democratic institutions is utterly different from that practiced by security states such as the former Soviet Union (and its successor).

Also, the counterintelligence "mindset," its puzzles and intellectual challenges, stretch the imagination and provide insight into how we think. How do we know what we perceive is correct? How do we measure what an adversary knows about us? How do we determine whether or not we are successful in keeping our secrets and projecting the image we wish to project? How do we know what and whom to trust?[3]

This article is a short cut to some basic concepts about counterintelligence: what it is and is not. Educators in history, government, political science, ethics, law and cognitive psychology should consider whether and how lessons on counterintelligence might enrich their courses. Recommended additional readings are suggested in the footnotes.

A general introductory course on U.S. counterintelligence should have five key learning objectives:

1 Understanding the meaning of counterintelligence, its place within intelligence studies, and its role in international relations as an instrument of statecraft.[4]

2 Understanding the difference between tactical and strategic CI,[5] the difference between CI and security,[6] and the range of foreign intelligence

1. John Ehrman, "Toward a Theory of CI: What are We Talking About When We Talk about Counterintelligence?" *Studies in Intelligence*, Vol. 53, No 2, (Washington, DC: Center for the Study of Intelligence) at *https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol53no2/toward-a-theory-of-ci.html*.

2. Michael J. Sulick, *Spying in America: Espionage from the Revolutionary War to the Dawn of the Cold War* (Washington DC: Georgetown University Press, 2012).

3. Consider for example the deception paradox: "Alertness to deception presumably prompts a more careful and systematic review of the evidence. But anticipation of deception also leads the analyst to be more skeptical of all of the evidence, and to the extent that evidence is deemed unreliable, the analyst's preconceptions must play a greater role in determining which evidence to believe. This leads to a paradox: The more alert we are to deception, the more likely we are to be deceived." Michael I. Handel, "Intelligence and Deception" in Roger Z. George and Robert D. Kline, eds, *Intelligence and the National Security Strategist: Enduring Issues and Challenges* (Washington, DC: National Defense University Press, 2004), 379, quoting Richards Heuer, "Strategic Deception: A Psychological Perspective" a paper presented at the 21st Annual Convention of the International Studies Association, Los Angeles, California, March 1980, 17, 28. Handel's article is a nice primer on deception: how to do it and how to avoid it.

4. CIA Historical Review Program, "Counterintelligence for National Security" *Studies in Intelligence*, Vol. 2, No. 4, at *https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol2no4/html/v02i4a10p_0001.htm*.

5. Michelle Van Cleave, "The Question of Strategic Counterintelligence: What is it, and what should we do about it?" *Studies in Intelligence*, Vol. 51, No. 2, at *https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol51no2/strategic-counterintelligence.html*.

6. Counterintelligence complements but should not be confused with security. Center for the Study of Intelligence, "Counterintelligence for National Security," *Studies in Intelligence* Vol. 2, No 4, see esp. section entitled "Counterintelligence as Activity." *https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol2no4/html/v02i4a10p_0001.htm*. The practical objectives of CI and security are not always in concert – which Christopher Felix (TN James McCargar) called "one of the classic conflicts of secret operations." As he explains, "[CI] operations are offensive operations which depend for their existence as well as success on constant, if controlled, contact with the enemy. Security, on the other hand, is a defensive operation which seeks to destroy the enemy's operations and to cut off all contact with

activities from targeting national security secrets and proprietary corporate information to conducting operations to influence our policymakers and public attitudes.

3 Exploring the history of CI in the United States, the roles and missions of government CI organizations, and how CI functions as an input and tool for national security policymaking and execution.[7]

4 Appreciating the ethical principles, laws and oversight governing counterintelligence in the United States.

5 Identifying the sub-disciplines of both offensive and defensive CI and the concepts of deception operations and analysis, double agents and asset validation.[8]

WHAT IS COUNTERINTELLIGENCE?

It is both an intelligence discipline and a national security mission and involves

- catching spies and putting them in jail;
- a set of tactical activities to protect and enable successful intelligence operations;
- the national security function that supplies insights into foreign intelligence threats to the United States, including options to defeat them as national policy may direct; and
- "an intellectual exercise of almost mathematical complexity"[9]

Counterintelligence is perhaps the least understood of the intelligence disciplines.[10] The popular notion is that of catching spies and putting them in jail, but spy catching is only the most visible part of a far more complex concept that encompasses all of the above. CI is arguably also the most essential of the intelligence disciplines. Why? Because even if you were able to collect vast quantities of secret information and produce exquisite analysis, without effective counterintelligence you could not have confidence in any of it.

With both a national security and homeland security mission CI has defensive and offensive components. It is an instrument of statecraft, just as intelligence is serving to advance the objectives of nation states. When successful, CI contributes to national security by serving both as a shield (guarding against penetrations of our government and our allies and alerting security) and a sword (conducting offensive CI operations that shape foreign perceptions and degrade foreign intelligence capabilities).[11]

The first clue to understanding counterintelligence is in the word itself. What is it that counterintelligence is "*counter*" to or against? If you answered, "foreign intelligence threats" you are correct.[12] But what does that mean? By statute...

> *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.* (50 USC 401a)

Counterintelligence encompasses both "information" and "activities." When we collect intelligence

him as dangerous." Christopher Felix, *A Short Course in the Secret War, 4th ed*, (Lanham, Maryland: Madison Books, 2001), 126. The interdependency between CI and the security disciplines has led to some long-playing theoretical discussions about which – if either – may be said to encompass the other; in practice, at a minimum, the two must be closely linked.

7. Michelle Van Cleave, *Counterintelligence and National Security* (Washington DC: National Defense University Press, 2007). The current article draws heavily from this source.

8. Asset validation is "the process used to determine the asset authenticity, reliability, utility, suitability and degree of control the case officer and others have." (US Department of Defense Joint Publication 2.01.2) For an understanding of the importance of asset validation and especially what can go wrong if it isn't done right, see the example of "Curveball" and the Iraq war, examined by the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction ("WMD Commission") Laurence H. Silberman and Charles S. Robb (Co-Chairmen) *Report to the President of the United States, March 31, 2005*, Chapter 7; for insight into broader reforms needed in U.S. counterintelligence, see Chapter 11, available at *http://www.fas.org/irp/offdocs/wmdcomm.html*.

9. Felix, *op cit*.

10. For excellent overviews of U.S. counterintelligence by two former heads of CIA's counterintelligence, see James Olson, "The Ten Commandments of Counterintelligence" *Studies in Intelligence*, Winter-Spring 2001, at *https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/fall_winter_2001/article08.html*; and Paul Redmond, "The Challenges of Counterintelligence," in *The Oxford Handbook of National Security Intelligence*, Loch Johnson, ed. (New York: Oxford University Press, 2010), 537-554.

11. For purposes of simplicity and richness of insights, this guide is written from the perspective of U.S. counterintelligence. Other nation states have different counterintelligence practices and histories.

12. A note on terminology: You may hear the oxymoron "counterintelligence threat". This is incorrect in the same way one does not speak of a "counterterrorist threat" or a "counterproliferation threat;" rather they are terrorist or proliferation threats, respectively. The correct terminology is a foreign intelligence threat to which counterintelligence is the response. (Strictly speaking there is such a thing as a CI threat but that refers to the narrow case in which the intelligence operation itself must contend with the CI activities of its target or within its theater of operations.)

on what foreign intelligence services are doing that intelligence is called "counterintelligence information." For example, who are their spies? Where and how do they operate? Who are their sources? What are their means of collection and communication? What are their vulnerabilities? When we conduct activities to stop, disrupt or exploit foreign intelligence operations those actions are counterintelligence operations. They may include both defensive activities (such as technical countermeasures to protect sources and methods of collection) as well as offensive operations (such as passing "feed material" through a double agent that helps persuade an adversary to take the action you want him to take).

Counterintelligence may also refer to the mission or organizations that gather the information and conduct the activities to counter foreign intelligence activities; for example, "I work for counterintelligence." In the United States, operational counterintelligence responsibilities are split in gross terms between the needs of domestic security against foreign agents (FBI), and the operational needs of intelligence collection (CIA) and military actions abroad. The FBI, responsible for enforcing the espionage laws of the United States, has the lion's share of U.S. counterintelligence duties. CIA's counterintelligence role is to protect our spies and ensure that we are not misled by foreign deception or denial. Counterintelligence elements in the Defense Department protect its warfighting components against enemy intelligence operations.[13] To tie it all together, the National Counterintelligence Executive serves as head of U.S. counterintelligence.[14]

Counterintelligence is perhaps the least understood of the intelligence disciplines. Spy catching is only the most visible part of a far more complex concept.

WHAT ARE FOREIGN INTELLIGENCE THREATS?

To understand counterintelligence, we must first ask how foreign governments and other entities employ intelligence capabilities against us. You might think, well, isn't that obvious? Don't they use their spy services just like the U.S. does – to collect secret information of value? Yes, but that is not the complete story.

Espionage. Foreign adversaries use their intelligence capabilities to penetrate, collect, and compromise U.S. national security secrets (plans, intentions and capabilities vital to protecting our security and well-being and that of our friends and allies) in order to advance their interests and defeat U.S. objectives. They also target critical technologies and other sensitive proprietary information to achieve economic advantage over U.S. business and industry (*economic espionage*). This includes intelligence collected from human sources (HUMINT) as well as from technical means including signals intelligence and computer network exploitation (*cyber espionage*).

Deception/Perception Management. Adversaries seek to manipulate and distort the picture of reality upon which policymakers plan and implement national security strategies, R&D and other programs, and economic policies. These foreign intelligence activities include corrupting the intelligence we gather through deception or denial, and conducting influence operations aimed at decision-makers.

Other intelligence operations. Finally, adversaries may use intelligence activities to disrupt and counter our operations (e.g., covert action, special operations, and other sensitive military and diplomatic activities).

In short, foreign governments as well as terrorist organizations and criminal cartels use intelligence to achieve advantage. "Every intelligence operation has a political object," Lenin once instructed. Counterintelligence helps find what that objective is and provides options to defeat it.

THE FUNCTIONS OF COUNTERINTELLIGENCE

America's defense has long depended on strate-

13. In addition to the operational elements (FBI, CIA, and the three military services), other Departments and Agencies that are particular targets of foreign interest have constituted CI offices to meet their individual needs for analytic support or to address insider threat concerns. Key examples include the CI offices within the Department of Energy and the National Nuclear Security Administration, the CI offices within the several intelligence agencies (e.g., the NRO, NSA, NGA, DIA), and other Departments and agencies with intelligence missions (Treasury Department, the Coast Guard), a number of DoD entities engaged in classified R&D (e.g., the Defense Threat Reduction Agency, the Ballistic Missile Defense Office) and the important CI support functions at the State Department and the Department of Homeland Security.

14. Counterintelligence Enhancement Act of 2002 (50 USC 401 *et seq*).

gic secrets — the locations of our hidden retaliatory forces; the codes by which we protect our military and diplomatic communications; intelligence sources and methods that give us warning and permit us to understand the threats and opportunities we face; and the sensitive technologies that give us military and commercial advantage. To survive with our values intact, the United States needs a clear appreciation of which secrets and other strengths we must protect, and the will do to so.

It is the job of U.S. counterintelligence to 1. *identify*, 2. *assess*, 3. *neutralize*, and 4. *exploit* the foreign intelligence activities directed against us.

1. Identify:

Most Americans would be astonished by the extent to which foreign intelligence services have stolen our Nation's secrets, often with impunity. With the possible exception of the Coast Guard, every department and agency with sensitive national security responsibilities has been penetrated by hostile intelligence services, most more than once. The former Soviet Union was especially successful in stealing U.S. secrets, a tradition that continues unabated under Vladimir Putin's Russia.[15] But the Russians are far from alone; other hostile services have literally gone to school on the practices of the old KGB. And then there is China. As reported a decade ago by a special Congressional Commission, the Chinese stole all U.S. nuclear weapons design secrets enabling them to leapfrog generations of technology development.[16] To this day, we do not know how China acquired those volumes of supremely guarded national security information; but we do know that Chinese intelligence is still at work, aggressively targeting not only America's defense secrets but our industry's valuable proprietary information as well for commercial advantage.

The first priority of counterintelligence is to identify the foreign intelligence activities directed against the United States and our interests so that action can be taken. This includes answering such questions as: Who are they (which governments, entities, services, individuals)? What are they doing (e.g., recruiting sources, stealing documents, setting up front companies)? Where/against what targets are they operating (e.g., American businessmen travelling abroad, national security laboratories, military computers or communications systems, CIA stations in third countries, company x)? This threat data triggers protective security measures (personnel screening, information handling, computer security, physical security) and operational security efforts for intelligence collection, military activities, and other sensitive national security operations.

The activities of foreign intelligence services can be an indicator of emerging threats. Intelligence activities are classic precursors to attack. During the Cold War, when NATO was concerned about a possible Warsaw Pact attack through the Fulda Gap, U.S. intelligence kept watch for missile and aircraft readiness stages and forward movements of armor and personnel. Warning of attack today is more subtle; but intelligence preparation is a necessary precondition even for terrorist attacks. As the Defense Science Board pointed out, "No observation is more important in countering terrorism than to understand that would-be perpetrators, to succeed, must participate in the gathering and application of intelligence."[17]

All intelligence services practice deception, from the mundane practices of lying and falsifying documents to elaborate double and triple agent operations to the exploitation of channels of communications known to be compromised. Adversaries (and even friends[18]) attempt to mislead U.S. intelligence and to sway decision makers. And the more they know about U.S. intelligence, the greater their chances for success.

Successful penetrations have netted an enormous amount of U.S. classified information, enabling ene-

15. The Russian intelligence presence in the United States is now equal to its Cold War levels, a sizing decision presumably indicative of the return on investment. A compelling perspective on contemporary Russian intelligence operations in the United States – and to a lesser extent, U.S. naiveté – can be found in Pete Early, *Comrade J: The Untold Story of Russia's Master Spy in America After the End of the Cold War* (New York: Putnam's Sons, 2008). As summed up on the book's the front cover: "When the Soviet Union disappeared, the spies did not."

16. Report of the Select Committee on U.S. National Security and Military/Commercial Concerns with the People's Republic of China ("Cox Commission"), 105th Congress, 2nd session, 1999; Report 105-851, at *http://www.house.gov/coxreport/pref/preface.html*.

17. Defense Science Board, Task Force on Strategic Intelligence Needs for Homeland Defense, Report to the Secretary of Defense, No. 308 (Fall, 2001).

18. For an accounting of British influence operations against the U.S. in the lead-up to America's entry into World War II, see Thomas E. Mahl, *Desperate Deception: British Covert Operations in the United States, 1939-1944* (London: Brassey's Inc., 1998). Among other things, Mahl recounts how the SIS, under the direction of William Stephenson, counterfeited and passed to the U.S. government a Nazi map that purported to show Hitler's designs on the Western hemisphere; the fake map was a featured exhibit by the unwitting President Roosevelt in his 1941 Navy Day speech calling for the repeal of the remaining neutrality legislation. The original map and the other deception material may be found in the official history by Nigel West, *British Security Coordination: The secret history of British intelligence in the Americas*, (London: St Ermin's Press, 1998).

mies to hide from or deceive U.S. intelligence. One of the greatest bargains in espionage history was the Soviets' purchase in 1977 of the technical manual for the new KH-11 reconnaissance satellite from former CIA employee (now convicted spy), William Kampiles, for a paltry $3,000. As a result of this and other compromises, U.S. intelligence must assume as a matter of course that overhead imagery and other technical collection will be met by denial and deception efforts.

There is a continuing market for stolen U.S. secrets, which may be sold or bartered to third parties. The knowledge gained of U.S. sources and methods – through spies, unauthorized disclosures, and even some authorized disclosures – has aided extensive concealment and denial programs that increase our uncertainty about foreign capabilities and intentions, and more effective foreign deception operations. India's nuclear tests in 1998 – which came as a shock to U.S. intelligence – were a prime example. Many nations have learned how to present a false picture of reality. These foreign denial and deception practices by denying vital information or distorting analysis can lead to faulty judgments. The danger is that useless or deceptive information – whether from human or technical collection – may be integrated into reports to policymakers, weapons designers, war-fighters or the warning community as if it were true.[19]

The possibility of deception is ever-present in intelligence work. Like intelligence, scientific inquiry seeks knowledge about the unknown. The difference is that microbes under a microscope are not purposefully trying to hide and deceive the biologist; intelligence adversaries are. Deception analysis focuses on providing a quality check on the information gathered about foreign nations in order to uncover the purposeful falsehoods sent out by others.

2. Assess: Analysis of the intelligence activities of adversaries or allies, competitors or partners, provides a window into their interests, purposes and plans, and options for defeating them. In practice, CI tasks must be prioritized by a sophisticated assessment of threats, which proceeds from an understanding of how others' intelligence capabilities are used to advance their objectives.[20] CI operations have positive intelligence requirements, which include answering such questions as:

- What is the "American Targets" capability of the adversary service? (Foreign intelligence services have a set cadre of personnel trained to go after American targets; U.S. counterintelligence needs to understand who they are and how they operate.)
- What is the doctrine by which the service deploys?
- What are its budget, training, and personnel records?
- What are its liaison relationships? And what are their resources, their targets?
- What are the critical nodes of foreign collection against us?
- What are the signatures of the intelligence precursors to an attack?
- What is their leadership structure?
- How and by whom are they tasked?

This analytic work, in turn, should lead to refined collection requirements to fill in the blanks in U.S. knowledge and to support operational planning to exploit foreign intelligence vulnerabilities.

The intelligence activities of adversaries and friends are important factors to consider as part of sound national security policymaking. Each of the major challenges confronting America – defeating global terrorism, countering weapons of mass destruction, ensuring the security of the homeland, transforming defense capabilities, fostering cooperation with other global powers, promoting global economic growth — has an embedded counterintelligence imperative. For instance, our insights into the intelligence activities of the other main centers of global power may confirm or otherwise shape prospects for cooperative action.[21] Consider the case of

19. Modern technology compounds the avenues for deception; but the problem is one known to the ancients. The notion that "all warfare is based on deception" dates from the 6th century B.C. writings of Sun Tzu, who devotes the closing pages of *The Art of War* to the classes and value of spies, how to convert enemy spies to one's own service, and how to use "doomed spies" as double agents "to carry false tidings to the enemy." To these instructions to the successful general he adds the strong caution that the use of spies to deceive and mislead is a two-way street, and that "without subtle ingenuity of mind, one cannot make certain of the truth of their reports."

20. Over the course of 70 years U.S. and British intelligence acquired many insights into the operations of the KGB. See for example Wayne Lambridge "A Note on KGB Style: methods, habits and consequences" *Studies in Intelligence*, Volume 11, Summer 1967, 65-75, at *https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol15no1/html/v15i1a08p_0001.htm.*

21. U.S. policy toward Russia is a case in point. Much of the old KGB's Cold War activities are recounted by Christopher Andrew and Vasili Mitrokhin in *The Sword and the Shield: The Mitrokhin Archive and the Secret History of the KGB* (New York: Basic Books, 1999). Drawing on unprecedented access to over 25,000 pages of KGB files, the book documents the breadth and weight and

China's intelligence activities, which increasingly rival those of Russia as a U.S. counterintelligence concern. We know that the most likely conflict between the United States and China would be over Taiwan and that such a conflict would likely involve naval engagements. There are specific dimensions to those engagements, which would shape Chinese intelligence collection objectives against U.S. targets, within Taiwan, and globally. Scenario-driven logic trees of this kind can yield a taxonomy for prioritizing CI analytic efforts and drive collection to support that analysis.

Assessments of foreign intelligence capabilities can shape policy deliberations and frame options for actions, answering questions as:

- If confronted with the prospect of war with Iran, what operations will Iranian intelligence conduct against the United States and what are our options to neutralize those operations?
- If North Korea attempts to sell and deliver a nuclear device or nuclear materials, what contribution can our counterintelligence forces make in the efforts to detect and intercept such activities?
- What hostile intelligence activities directed against the United States might neutralize our capacity to exercise effective control of outer space?
- To what extent are the intelligence elements of South Korea and Taiwan susceptible to deception by their adversaries and can we discern that and guard against efforts to misdirect us?
- What role do Cuban intelligence personnel play in Venezuela, and what influence does Havana exercise over that government?
- What efforts might undermine the effectiveness of our ballistic missile defense system? How effective are our security preparations in protecting against these actions?

3. Neutralize:

Counterintelligence has a positive intelligence role in identifying threats and assessing foreign intelligence capabilities, but that is only the beginning. The most distinguishing feature of counterintelligence is that it is an operational function protecting intelligence collection and analysis and other national security activities. "For the intelligence-minded man, to know about the opposition and his installations is the whole goal; for counterintelligence, knowing is only the beginning of the road – something has to be done about the information."[22] The emphasis on doing extends beyond the intelligence community to include law enforcement. When a spy is arrested, or a pseudo "diplomat" caught in flagrante delicto and expelled, or an asset discredited as working for the other side, the CI elements that neutralized the foreign intelligence operation have done their job.

Counterintelligence goes after the adversary

The neutralization of foreign intelligence threats is an essential part of protecting secrets. Sound security measures such as locks, guards and gates, background investigations and polygraphs, computer firewalls and document controls are unquestionably vital, but they can only protect so far. One can pile on so much security that no one can move and still there will be a purposeful adversary looking for ways to get at what it wants. Counterintelligence goes after the adversary.

Campaigns to neutralize enemy intelligence capabilities have long been an essential part of war

audacity of the former Soviet intelligence attack on the U.S. – including notably its extensive active measures and disinformation campaign, which as it turns out would appear to have met even the most conspiracy-minded suspicions of the anti-communist American right wing. As one observer points out, the real importance of the book is "the sheer weight of accumulated detail which reveals a madly compulsive Soviet over-reliance on clandestine means for conducting its foreign policy, maintaining security and ideological control at home, and acquiring the technological infrastructure of a modern state." Thomas Powers, *Intelligence Wars: American Secret History from Hitler to Al-Qaeda* (NY: NY Review of Books, 2002), 96.

22. C.N. Geschwind, "Wanted: An Integrated Counterintelligence" *Studies in Intelligence*, Summer 1963, 15, at *https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol7no3/html/v07i3a02p_0001.htm*. This article, while very dated, offers some interesting insights into the differing tradecraft of clandestine HUMINT collectors and CI operations: "It is the job of intelligence to collect and analyze information. Espionage for this purpose, insofar as it is aggressive, acts only with the objective of getting past the opposing counterintelligence and security forces as uneventfully as possible. Since the gathering of intelligence is a secret preparatory function, agents doing it are not supposed to undertake executive action, agitate, or otherwise risk attracting attention. Counterintelligence, on the other hand, is engaged in covert war, all-out and immediate. It has to take action—at home by investigating, arresting, interrogating, doubling, and prosecuting Communist operatives, and abroad by carrying out recruitment, neutralization, harassment, diversionary, and psywar operations against their secret service system. These diverse concepts of responsibility for action not only are fundamentally incompatible but call for agents of fundamentally different temperament and attitudes."

planning. In preparation for the Iraq War, for example, U.S. counterintelligence's project code-named "Imminent Horizon" mapped Iraqi intelligence operations worldwide to render them ineffective. Such plans also have a place in national security strategy in times of peace.

One of the best examples of strategic CI operations was the effort in the early 1980s to stop the Soviets' illicit acquisition of advanced technologies. The détente policies of the Nixon administration had opened the flood gates to Soviet intelligence in their clandestine efforts to obtain scientific knowledge and technologies from the West.

> This effort was suspected by a few U.S. Government officials but not documented until 1981, when French intelligence obtained the services of Col. Vladimir I. Vetrov, [codenamed] *Farewell*, who photographed and supplied 4,000 KGB documents on the program. In the summer of 1981, President Mitterrand told President Reagan of the source, and, when the material was supplied, it led to a potent counterintelligence response by CIA and the NATO intelligence services.[23]

Farewell provided detailed information on Soviet technology acquisition efforts, including how it was run by Line X of the KGB and exactly what it was after. It set off a far-reaching technology control effort, including export control enforcement actions and effective international cooperation in interdicting unlawful transfers. U.S. intelligence developed new sources to expose end users and gain insights into Soviet activities. The ensuing CI operations to disrupt Soviet technology collection were broad and thorough. Within the U.S., and jointly with NATO governments in Western Europe and others, some 200 Soviet intelligence officers were expelled and their sources compromised. Line X was effectively out of business.[24]

Importantly, this CI campaign was part of the broad Reagan administration strategy toward the former Soviet Union. Embodied in National Security Decision Directive 75, the central objective was to "contain and over time reverse Soviet expansionism by competing effectively on a sustained basis with the Soviet Union in all international arenas."[25] The U.S. defense buildup of the 1980s was the centerpiece of this strategy. When Farewell walked through the door, the United States was just beginning its military modernization effort. R&D efforts supporting the Strategic Defense Initiative, and new composite materials enabling stealth capabilities, and breakthroughs in supercomputing and other extraordinary information technologies, among many, many other marvels of engineering and design, were all at stake and targeted by the KGB.

4. Exploit:

By exploiting insights into foreign intelligence activities, counterintelligence can help turn events to our advantage. For example, Morris Childs was deputy head of the Communist Party of the USA and trusted confidant of his former instructors, Yuri Andropov (later head of the KGB and the Soviet Union) and Mikhail Suslov (later the Politburo's chief ideologist). Childs was also working for the FBI — a highly successful double agent operation called "Operation Solo" that continued for 23 years.[26]

How does an intelligence service know when it has the upper hand? Or when it is being played or misled by the other side? It needs a feedback mechanism, e.g., sources inside the adversary's intelligence apparatus that can provide a check on their perceptions, doubts or beliefs. The ultimate goal of offensive CI...

> is to penetrate the opposition's own secret operations apparatus: to become, obviously without the opposition's knowledge, an integral and functioning part of their calculations and operations... [A successful CI penetration] puts you at the very heart of his actions and intentions towards you.... Most importantly, you are in a position to control

23. Gus W. Weiss, "The Farewell Dossier" *Studies in Intelligence*, Vol. 39, No.5, 1996) 121-126. *https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/96unclass/farewell.htm.*

24. *Ibid*. In the Fall of 1986 another 80 Soviet intelligence officers, assigned under diplomatic cover in New York, San Francisco and Washington, were ordered to leave the country — the culmination of a series of diplomatic and CI moves to curtail Soviet intelligence operations in the United States. See David Major, "Operation 'Famish'" *Defense Intelligence Journal* (Spring 1995).

25. "The contest would range from buildups in nuclear and conventional weaponry through new and openly discussed war-fighting strategies, economic sanctions, the aggressive promotion of human rights, overt and covert support for anti-Soviet resistance movements in Eastern Europe and Afghanistan as well as for opponents of Marxist regimes in Angola, Ethiopia, and Nicaragua, and the vigorous employment of rhetoric as an instrument of psychological warfare, a trend which culminated in the President's March, 1983, claim that the Soviet Union was 'the focus of evil in the modern world.'" John Lewis Gaddis, "Strategies of Containment: Post-Cold War Reconsiderations," lecture presented at The Elliott School of International Affairs, George Washington University, April 15, 2004.

26. John Barron, *Operation Solo: The FBI's Man in the Kremlin* (Washington DC: Regnery Publishing, 1996).

his actions, since you can, by tailoring intelligence for him to your purposes, by influencing his evaluation, mislead him as to his decisions and consequent actions.[27]

As described above, *Farewell* gave U.S. counterintelligence the keys to neutralize the KGB's campaign to piggyback on U.S. technology investments. But that was not all. Having the Line X shopping list also meant that it might be possible to control some part of their collection, to "turn the tables on the KGB and conduct economic warfare of our own." As the late Gus Weiss tells the story,

> *I met with Director of Central Intelligence William Casey on an afternoon in January 1982. I proposed using the Farewell material to feed or play back the products sought by Line X, but these would come from our own sources and would have been "improved," that is, designed so that on arrival in the Soviet Union they would appear genuine but would later fail. U.S. intelligence would match Line X requirements supplied through Vetrov with our version of those items, ones that would hardly meet the expectations of that vast Soviet apparatus deployed to collect them.*
>
> *If some double agent told the KGB the Americans were alert to Line X and were interfering with their collection by subverting, if not sabotaging, the effort, I believed the United States still could not lose. The Soviets, being a suspicious lot, would be likely to question and reject everything Line X collected. If so, this would be a rarity in the world of espionage, an operation that would succeed even if compromised. Casey liked the proposal.*
>
> *As was later reported in* Aviation Week and Space Technology, *CIA and the Defense Department, in partnership with the FBI, set up a program to do just what we had discussed: modified products were devised and "made available" to Line X collection channels.*[28]

Golden opportunities of the kind *Farewell* provided do not come knocking every day. The national CI enterprise needs to seek out high value insights into foreign intelligence activities, recognize gold when it appears (and fools' gold for what it is), and be creative and agile and competent enough to seize the moment.

The world of offensive counterintelligence is most familiar in its supporting role to military operations.[29] The finest historic example, of course, is Operation Overlord, the Allied landing at Normandy. D-Day was a huge risk, which succeeded because of masterful planning, including the most sweeping deception in military history. The Allies could not hope to hide the fact that they intended a cross-Channel invasion; but through the use of elaborate decoys and ruses, misleading communications, finely orchestrated double agent operations,[30] and a host of other inventive measures, they led the Germans to believe the landing site would be at Pas de Calais. The surprise was total.[31]

For deception to be successful, "two things are imperative: First, the enemy must be kept totally in the dark about what you don't want him to know, and second, you must know everything he is thinking all the time, especially when he's confronted with what you want him to believe." In any deception campaign, the feedback loop is all-important. Cambridge University World War II historian F.H. Hinsley continues,

> *We were able to locate, early on, the entire German espionage network in Britain, eliminate parts of it and use others to feed Hitler disinformation. We were also able to learn Hitler's thinking about where and when the invasion would eventually come, play to his prejudices and hunches, and learn when and whether he took our bait. We were reading his mind all the time.*[32]

27. Felix, *op cit*, 121.

28. Weiss, op cit, 124.

29. The use of strategic deception in peacetime presents its own set of special considerations. Actions taken to manipulate, distort or falsify information to mislead the enemy may have the unintended consequences of deceiving the public, calling into question core democratic values. The law is unclear and the ethical questions even more challenging when deception may work to save lives and advance freedom; the practical questions concerning the design and employment of deception are no less complex for national security decision makers, as well as for members of the press. For a discussion of these and other matters see U.S. Army War College and Triangle Institute for Security Studies, Conference Brief "Strategic Deception in Modern Democracies: Ethical, Legal, and Policy Challenges" compiled by Dr. Carolyn Pumphrey and LtCol Antulio Echevarria II (2003), accessible over the internet at *http://www.pubpol.duke.edu/centers/tiss/pubs/Summary.html*.

30. The use of double agents, which figured so prominently in WWII deception operations under the code name "Double-cross," is a complex and sophisticated counterintelligence technique. "A double agent is a person who engages in clandestine activity for two intelligence or security services (or more in joint operations), who provides information about one or about each to the other, and who wittingly withholds significant information from one on the instructions of the other or is unwittingly manipulated by one so that significant facts are withheld from the adversary... The double agent serves also as a controlled channel through which information can be passed to the other service, either to build up the agent in its estimation or for purposes of deception" (as was the case with Overlord). F.M. Begoum, "Observations on the Double Agent" *Studies in Intelligence*, Winter 1962, at *https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol6no1/html/v06i1a05p_0001.htm*.

31. For the full story see Ben Macintyre, *Double Cross*. (New York, Crown Publishers, 2012). Concerning British counterintelligence and its role in supporting deception for Operation Overlord and other actions in World War II, see Basil Collier, *Hidden Weapons: Allied Secret or Undercover Services in World War II* (London: Sword Books Ltd., 1982, 2006).

32. Quoted in "The Masters of Deception: At England's Bletch-

Offensive CI seeks to influence the adversary's decision makers by manipulating the intelligence product that informs their decisions, "luring your opponent into doing voluntarily and by choice what you want him to do."[33] This was the role counterintelligence played in Operation Overlord, luring the Germans to mass their forces in the wrong place.

In peacetime too, U.S. counterintelligence needs to think offensively — How does the foreign intelligence service operate? What are its vulnerabilities? How can they be exploited? What are the indicators that might give warning of intelligence operations against us? Are there tripwires we can design to give us an edge? Are there CI avenues available to influence foreign decision making to help achieve larger U.S. national security objectives?[34]

THE FUTURE OF COUNTERINTELLIGENCE

The litany of spies inside the U.S. government – from the British agents in the Revolutionary War to those stealing atomic secrets in World War II to traitors now in jail (such as former CIA officer Rick Ames and former FBI special agent Robert Hanssen) – spans our history and tells many stories: Who would spy against their own country? For whom, and why? What did they steal, and how? How were they caught? And what does the future hold?

At the start of the 21st Century, there are many more highly capable foreign intelligence services in the world than ever before, and we are only just beginning to understand their potentials. Today, these foreign services can also take advantage of the self-appointed revealers of Western secrets (like the stateless organization Wikileaks or former NSA contractor Edward Snowden, now living in exile in Russia) who at best have no way of knowing what harm their actions may cause. Furthermore, modern technologies, such as biometrics for identification and "big data" search and retrieval, offer U.S. and foreign CI organizations new tools, often difficult to counter. The future of counterintelligence may be even more challenging than its past.

A member of AFIO's Board, Michelle Van Cleave served as the National Counterintelligence Executive under President George W. Bush. As the head of U.S. counterintelligence, she was responsible for directing and integrating FBI, CIA, Defense and other counterintelligence activities across the federal government. She has also held senior staff positions in the Senate and House of Representatives, the Pentagon, and in the White House Science Office, where she served as Assistant Director and General Counsel under Presidents Ronald Reagan and George H.W. Bush. A lawyer and consultant in private life, she is a Senior Fellow at George Washington University and a principal with the Jack Kemp Foundation.

ley Park, Recalling the Code-Breakers and Illusion-Makers" *The Washington Post*, May 31, 1999, C-1.

33. Felix, *op cit*, 128.

34. Office of the National Counterintelligence Executive, "The National Counterintelligence Strategy of the United States" (Washington, DC: NCIX Publication No. 2005-10007, March 2005) *http://www.ncix.gov/publications/strategy/docs/FinalCIStrategyforWebMarch21.pdf*. This was the first national strategy developed to guide U.S. counterintelligence; it also set out for the first time the offensive dimension of counterintelligence at the strategic level. See also subsequent iterations of the national CI strategy, available on the webpage of the Office of Director of National Intelligence (*www.dni.gov/*).