
From AFIO's THE INTELLIGENCER
JOURNAL OF U.S. INTELLIGENCE STUDIES
VOLUME 28 • NUMBER 1 • Winter-Spring 2023 $15 SINGLE COPY PRICE

Association of Former Intelligence Officers
7600 Leesburg Pike, Suite 470 East
Falls Church, Virginia 22043
Web: www.afio.com * E-mail: afio@afio.com

I. CURRENT ISSUES

U.S. Counterintelligence

One Team, One Plan, One Goal – or Not?

by Michelle Van Cleave
Former National Counterintelligence Executive

Twenty years ago, Congress established a new national office to lead U.S. counterintelligence: the National Counterintelligence Executive (NCIX).[1] Unfortunately, based on the ensuing record and my experience as the first statutory NCIX, I must report that the national office has failed to accomplish the principal goals for which it was created.[2] While there are many factors at play, the most significant in my view is the lack of consensus on what those goals are – calling to mind Yogi Berra's famous maxim, "If you don't know where you're going, you're likely to wind up somewhere else."

Today, U.S. counterintelligence (CI) is still struggling with many of the same systemic difficulties that drove Congress to act 20 years ago – along with some new ones laid bare by the upsurge in malign influence operations directed against our democracy. In 2014, the national CI office was renamed to include protective security, which now receives the lion's share of its attention; but security measures alone, while vitally important, will never be enough. Without a renewed emphasis on the core business of U.S. counterintelligence, the United States will continue to forfeit the initiative to foreign adversaries and suffer costly losses to hostile intelligence threats from Russia, China, and a long list of others.

With the benefit of hindsight and lessons learned over the last two decades, the time is ripe for a fresh look at the U.S. counterintelligence enterprise, the meaning of "strategic counterintelligence," and the need – if any – for a national CI mission and leader.

Significance of the *Counterintelligence Enhancement Act of 2002*

Despite a history of damaging CI failures, U.S. counterintelligence has been largely immune from reorganization schemes because it never had a conscious organization plan to begin with. The National Security Act of 1947 established the basic contours of the post-war U.S. intelligence community, but (apart from defining the term[3]) said nothing about counterintelligence.

Unlike most modern nation-states, the United States has never had a national counterintelligence "service." Instead, CI operational authority was split in gross terms between the needs of domestic security (assigned to the FBI), and the operational needs of intelligence collection (assigned to CIA) and military operations/force protection in the field (assigned to DoD and the military services). There was no overarching national leadership to provide cohesion or strategic direction for America's CI activities.

Twenty years ago, Congress took a look at the enterprise and saw that it was little changed from the set pieces that emerged after World War II. The lead operational agencies each had a vital CI mission shaped and executed as part of their own organizational responsibilities. But they had the barest understanding of what resources and capabilities the others possessed, much less their operational, analytic, or resource plans beyond the current budget year; or how "foreign intelligence threat" was defined or assessed beyond their own area of responsibility.

There were no agreed guiding principles or CI doctrine across the discipline, nor a standard approach

1. In 2014, Director of National Intelligence (DNI) James Clapper reorganized and renamed the office the National Counterintelligence and Security Center (NCSC).

2. As then SSCI Chairman Bob Graham explained ("Intelligence Authorization Act for Fiscal Year 2003" *Congressional Record*, Vol. 148: September 25, 2002, p S9352):

> At the urging of our committee, the President created the NCIX in 2001 to provide the U.S. Government in the counterintelligence area with (1) strong, policy-driven leadership; (2) new and enhanced counterintelligence capabilities; and (3) coherent program, strategies and cooperative approaches. The committee's oversight of this fledging effort revealed problems, however, that [this Act] is designed to remedy. By establishing the NCIX in statute and placing it in the Executive Office of the President, with oversight by the intelligence committees, the committee believes that the NCIX leadership problems, resource constraints and, overall, lack of sufficient status and visibility within the Government, will be remedied.

In 2005, the NCIX was moved under the Director of National Intelligence, and later became one of several ODNI centers.

3. "Counterintelligence means information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons, or international terrorist activities." 50 USC 3003(3).

to targeting, much less a coherent joint strategy or national program to disrupt hostile intelligence operations. Given the extremely close-hold nature of counterintelligence, interagency information sharing was poor, and infrastructure support even worse. Even the modest national mechanisms developed to deconflict offensive CI activities stopped at the water's edge, a legacy of the old divide between foreign and domestic operational realms. And there was no shared concept of a national or strategic version of the CI mission.

As a consequence, no one had a common operating picture of the foreign intelligence threats arrayed against the United States, or (equally important) the "blue side" forces available to counter those threats. With three operating elements, each with differing missions, responsibilities, and resources, all the incentives were to address agency-specific matters, case by case, rather than to work as one team to identify and counter hostile intelligence threats to the United States. Where coordination was required by policy, it was for the purpose of deconflicting the tactical environment rather than supporting strategic objectives.

Taken together, this inchoate architecture of U.S. counterintelligence has been costly. Foreign powers have rigorously leveraged the resulting gaps in the U.S. CI framework, especially as they presented opportunities in relatively non-hostile, third country operational environments. Adversary intelligence services found they could exploit DOD's dependent authorities to conduct counterintelligence for an other-than-force-protection purpose, overwhelm CIA's limited CI resources, and take advantage of the FBI's constrained ability to work abroad.

Congress decided it was time to put someone in charge of the enterprise.

The *Counterintelligence Enhancement Act of 2002* established in law a national head of U.S. counterintelligence, who would be responsible for providing strategic direction and integrating activities across U.S. counterintelligence. Drawing on an in-depth Clinton-era interagency study ("CI-21") and ensuing Presidential Directive (PDD-75), the purpose was twofold:

- To close the seams that existed between the fiefdoms of the several operating agencies, which were being exploited by spies seeking a way into U.S. national security secrets, to devastating effect.[4]
- To develop and execute a national-level counterintelligence strategy to protect and defend the United States and our vital interests against foreign intelligence threats.

The *Counterintelligence Enhancement Act*, together with "CI-21," represented a conceptual breakthrough in American counterintelligence. They judged that the central strategic core that is needed to identify, assess, and defeat hostile intelligence threats had been missing. This is the fundamental flaw in the architecture of U.S. counterintelligence which the new national office was created to remedy—not by its mere existence, but by leading the transformation and strategic integration of our Nation's CI capabilities.

And that is where the new office has fallen short.

First National Counterintelligence Strategy and Its Aftermath

9/11 taught us a hard lesson. It is not acceptable to wait until the terrorists are here in our own backyard, where we are most vulnerable and at risk. The objective must be to find them, and stop them, before they can strike. That requires identifying and assessing their "order of battle" – their training camps, hiding places, headquarters' cells, support networks, recruitment nets, logistics infrastructure, targeting plans, etc. Based on this now well-understood target set, operational plans can be developed to exploit their vulnerabilities, including the execution of carefully orchestrated pre-emptive actions when so directed.

There were lessons here for U.S. counterintelligence as well. In the past, America's default CI strategy has been to wait to engage the foreign intelligence adversary in our own backyard, rather than in theirs. Over half of the U.S. CI budget post -World War II has been devoted to activities within the United States carried out by the FBI. In addition, most of the remainder allocated to CIA, the Defense Department, and to small pockets elsewhere in the government, has gone to programs and personnel based wholly or in part within U.S. borders. The result of this insular posture? A long history of devastating losses to espionage and other hostile intelligence operations. Something had to change.

4. Of note, CIA officer Aldrich Ames and his Soviet/Russian handlers had benefited from those seams for 9 years, FBI special agent Robert Hanssen for 21, and DIA analyst Ana Montes – Cuba's star asset – for 17. Waiting in the wings was Katrina Leung, whose prosecution as an 18-year Chinese double-agent was truncated by management and oversight failings documented in the follow-up Justice Department Office of the Inspector General report *https://oig.justice.gov/sites/default/files/archive/special/s0605/index.htm*. Of course, there would be more to come.

Go on the Offense

As Jim Olson, former head of counterintelligence at CIA, explains in his classic article *The 10 Commandments of Counterintelligence*, "CI that is passive and defensive will fail... Our CI mindset should be relentlessly offensive. We need to go after our CI adversaries."[5] While this imperative has long been understood and practiced at the tactical level, its application as declared national-level strategy was not.

The first *National Counterintelligence Strategy*, issued by President Bush in 2005, was a sharp departure from the past. Rather than wait until the foreign intelligence threat is here, at our doorstep, the Bush *Strategy* directed that U.S. counterintelligence go on the offense, to exploit where we can, and interdict where we must, with the purpose of degrading the adversary service and its ability to work against the United States.

Executing an offensive national CI strategy begins with working the target abroad. How are foreign intelligence personnel recruited, trained, tasked? Who are their leaders, reporting chains, liaison relationships? Where do they operate? How? What are the gaps in our understanding? How can we gain the insights and capabilities we need to identify and exploit adversary vulnerabilities? As directed by national security priorities, the considerable resources of the members of the U.S. intelligence community that have global reach would be directed to help identify and then neutralize or exploit the intelligence activities of foreign adversaries. One team, one plan, one goal.

The need for this capability was driven home in America's experience with the war against Iraq. In the lead-up to "Operation Enduring Freedom," an interagency CI strategic planning team came together to develop a common operating picture of Iraqi intelligence operations worldwide. In response to Command Authority direction, the "Imminent Horizon" team was chartered to render Iraqi intelligence ineffective. While this effort resulted in some important successes, the CI community learned its lessons the hard way.

Strategic operational planning to degrade foreign intelligence capabilities has long lead times. Beginning at D minus 6 months – as was the case with Iraq – is too little too late. Even though Coalition Forces had technically been at war with Iraq for ten years, flying daily combat missions, the CI community could identify and contain an unacceptably low percentage of Iraqi intelligence assets.

The Iraq War after-action reports confirmed, once again, the compelling need for standing joint strategic planning, for building interoperability across CI agencies, and for proactive operations to degrade foreign intelligence threats. But here we had a problem. The U.S. CI enterprise was not designed to preempt.

The CI enterprise was neither configured to serve a strategic purpose, nor postured globally to disrupt a foreign intelligence service. Apart from wartime, the U.S. government has not routinely addressed foreign intelligence capabilities as part of a national security threat calculus informing national strategy and planning. While DoD owns or controls most of the secrets worth stealing, it does not command the suite of resources necessary to counter foreign intelligence operations directed against those secrets; nor does it have the authority to take on that mission alone. Those responsibilities fall respectively to CIA abroad, and FBI at home. Yet here we had another problem.

CIA was not directed and did not attempt to create a worldwide CI service designed to detect, analyze and counter hostile intelligence operations directed at the U.S. and its interests. Far from being a partner with the FBI to build a global perspective on the operations of foreign intelligence services, CIA has interpreted its CI job as confined to protecting its own house and mission. Across the board, U.S. CI capabilities are tailored to meet agency-specific needs, but not designed to operate jointly.

While one of the inherent strengths of U.S. counterintelligence is the diversity of skills, methodologies and resources across the profession (in contrast to a single national service, such as MI-5), there was neither process nor infrastructure to marshal them to common end. And such disunity leads to an inherent weakness: seams that adversaries could exploit.

In short, the whole was less than the sum of its parts. That needed to be fixed.

New CI Business Model

To that end, the Bush *Strategy* called for a new business model for the CI enterprise, to provide the strategic coherence to go on the offense against select targets. The goal was to create an additional CI capability at the national level, in service of a new and interdepartmental mission that would address the increasing success of the intelligence services

5. James M. Olson, "The Ten Commandments of Counterintelligence," *Studies in Intelligence*, Fall-Winter 2001, CIA Center for the Study of Intelligence, Washington DC.

of foreign powers in their exploitation of the 'gaps' described above.

Conceptually, this undertaking consisted of two parts: first, a global CI assessment of foreign intelligence presence, capabilities and activities; and second, a CI "doctrine" – the fundamental principles that guide military or other operations in support of national objectives—for attacking adversary services systematically via strategic CI operations. At home, the proactive CI mission called for a coordinated, community-wide effort of aggressive operational activity and analysis to obtain the intelligence necessary to neutralize the inevitable penetrations of our government.

National teams, consisting of representatives from key CI components, would be responsible for this centralized strategic planning against designated high-threat foreign intelligence adversaries. Upon the direction of the NCIX, departments and agencies would pre-obligate certain of their resources to the new national program (or acquire new resources as approved by Congress) sufficient to meet their new obligations under the *Strategy*. Operational responsibility for distributed execution was assigned to CIA, DoD, or the FBI as appropriate, each of which would retain budget and program control over their respective CI activities.

Based on this model, and with Congressional support, we initiated a pilot program against a high priority target.

Just as this work was getting underway, major change was sweeping across the U.S. intelligence community: the creation of the office of the Director of National Intelligence (DNI). Authority and responsibility for overseeing CI budgets, collection and analysis, previously under the NCIX, became part of the portfolios of the various DNI functional deputies. The pilot strategic CI program ran into stiff resistance, especially from CIA, which was straining to meet all of the extra staffing requirements imposed by the numerous new DNI centers, directorates and mission managers.

After I left office, I learned the pilot program had been terminated, the group's funding and a related activity transferred to the National Clandestine Service at CIA. The experiment in national strategic integration came to an abrupt end. As before, individual department and agency priorities would take precedence over any national level CI effort. And they in turn would have to compete with other national priorities for funding and attention.

The Fatal Flaw

The *Counterintelligence Enhancement Act* and the standup of the NCIX should have heralded a new chapter in U.S counterintelligence, enabling the strategic direction and integration of U.S. counterintelligence capabilities to common end. So why did it all fall apart?

As envisioned by the *Counterintelligence Enhancement Act*, the President issued a strategy to array U.S. counterintelligence activities to a common purpose. The express intent was to create a strategic CI capability to identify, assess, and proactively disrupt foreign intelligence threats to the United States. But there was no means of carrying that out.

Effective integration and coordination across the interagency require the discipline of a national program: budgets, billets, authority and accountability to meet defined ends. It is not enough to exhort cooperation through national guidance or interagency meetings. Even strong national leadership, charismatic personalities and popular ideas will falter absent the institutional tools that drive, capture and internalize the results needed to enable strategic coherence.

Yet in establishing the NCIX as the head of U.S. counterintelligence, the law did not create a corresponding national CI program by which the strategic direction and integration of U.S. CI capabilities could be accomplished. Subsequent national CI strategies have omitted this seminal goal altogether. Funding and resources devoted to traditional CI targets have continued to decline in the face of competing priorities, while the Office of the NCIX (now called the NCSC, as discussed below) has turned its attention to other concerns.

As a consequence, U.S. counterintelligence has been stuck in neutral for 20 years now while the threats — and our vulnerabilities — continue to grow.

Talk to the heads of the several CI components today and you will learn that no one of them knows what the other has to bring to the table. Why does this matter? Because it is impossible to match means to ends if you do not know what means are at your disposal – much less to assess where or how far you have fallen short.

You will also learn that, twenty years after the creation of the national CI office, no one has a common operating picture of what the United States is doing against foreign intelligence targets. Last summer, the head of the British Secret Intelligence Service reported that, subsequent to Russia's invasion of Ukraine, European governments had expelled over 400 Russian intelligence officers serving under diplomatic

cover – adding that he hoped that others will consider turning on Putin (*"Our door is always open."*) So, who is keeping book on how many cases the FBI has today on the Russian target (never mind the specifics of who/what/when/where, or the possibilities for operational exploitation)? The same holds true for U.S. efforts to identify, assess, neutralize or exploit the intelligence activities of the Chinese, the Iranians, and other adversaries working actively against us.

It is yet another step to be able to answer the question, "Are we winning or losing?" How does one measure, for example, the relentless Chinese and other collection operations directed against U.S. business and industry and commercial wealth? Cyberattacks against critical infrastructures and sensitive databases have grown so aggressive that they have been assigned as part of the defensive mission of a unified combatant command (USCYBERCOM) and a dedicated agency (CISA) at the Homeland Security Department. Indeed, these threats, it is often said, require a "whole of government" response, including specialized analytic and operational contributions that only counterintelligence can make.

At the same time, hostile penetrations into sensitive government activities, as well as foreign deception operations, have grown far bolder and deeper than the CI resources we have available to counter them, putting lives and treasure and U.S. supreme national interests at risk. A few examples:

China: According to media reports,[6] significant U.S. intelligence operations in China have been compromised, which, if true, raise many troubling questions. For example, how were these operations discovered? How long were they being observed ... and played back against us? How many other losses have yet to come to light? What more do the Chinese know about U.S. intelligence operations? And how are they using those insights to hide what they are doing or otherwise deceive us? Simply put, if you thought we had good intelligence on the Chinese, think again.

How all this might have happened appears to be a matter of dispute. What is not in dispute is how thoroughly devastating such losses could have been and continue to be to U.S. intelligence – and all who depend on that intelligence to make life and death decisions.

Russia: Human intelligence is still Russia's forte. For the Russian intelligence services, America has always been deemed the "main enemy:" the outcome of the Cold War has only reinforced their focus, not changed it. By contrast, the West's intelligence efforts against Russian targets were sharply reduced as the U.S. waged a global war on radical Islam – and also because we thought a post-Cold War Russia would no longer be counted among our adversaries. Then Putin invaded Ukraine. And now we're playing catch-up.

Major Soviet/Russian espionage cases (i.e., penetrations into the U.S. government, run directly or through proxies) numbered 16 in the 1980s, 10 in the 1990s, one in 2001 ... and then nothing, until a former Army Special Forces officer was arrested in 2021 for selling the Russians information about weapons and troop deployments. And no, the sharp decline in arrests and prosecutions is not good news.

While the numbers have fluctuated over time, there are well over 60 Russian intelligence officers stationed in the United States today (not counting illegals or those here under non-official cover). Their highest priority? To recruit assets inside the U.S. intelligence community. Putin is a former KGB/FSB head. He's grading their performance. How likely is it that they're just sitting around with nothing to show for it? Yet we found no penetrations for two decades. If you do the math, it's not reassuring.

Cuba: "Havana syndrome" – unexplained and sudden brain injuries affecting dozens of American personnel – may or may not have involved the hand of the Cubans when first reported there in 2016. But at a minimum it poses the troubling question of why we don't have deeper insights into the secret operations of the Cuban government, especially ones that put Americans at risk? In all likelihood, U.S. intelligence insights into Cuba have been thin to nonexistent for decades, thanks to the stunningly successful deception and denial campaigns of Cuban intelligence operating under our noses here in the United States. You can't get an accurate read on foreign threats if your sources are corrupt, your agents doubled back against you, and your intelligence collection apparatus blind and deaf and dumb - but you don't know it.

Recent press reports[7] suggest that troubling compromises continue to plague U.S. intelligence, putting uncounted lives at risk, clouding the integrity of intelligence reporting, and bringing deep poignancy to the question, now what?

6. "Killing C.I.A. Informants, China Crippled U.S. Spying Operations," *The New York Times*, May 20, 2017.

7. "Captured, Killed or Compromised: C.I.A. Admits to Losing Dozens of Informants" T*he New York Times*, October 5, 2021.

The Strategic CI Mission

The central judgment of the *Counterintelligence Enhancement Act* is clear. There is a national CI mission that is beyond the ability of any individual Agency to fulfill. This mission can only be accomplished by ensuring the integration and strategic direction of CI community operations and resources. The law places the responsibility for that coordination on the statutory head of U.S. counterintelligence. But responsibility without the means of carrying it out is illusory.

The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction ("WMD Commission"), chartered to review intelligence failures in the aftermath of the Iraq War, devoted substantial attention to U.S. counterintelligence. In welcoming the President's 2005 *National Counterintelligence Strategy*, they cautioned that a strategy alone is not enough:

> Our counterintelligence philosophy and practices need dramatic change, starting with *centralizing counterintelligence leadership*, *bringing order to bureaucratic disarray*, and *taking our counterintelligence fight overseas* to adversaries currently safe from scrutiny.[8]

I believe the principal obstacle to effecting this change was then and remains today the lack of consensus on the job that the national office and the CI components together were being asked to accomplish.

Despite the WMD Commission's indictments and calls for change, despite the passage of the *Counterintelligence Enhancement Act* and the searching critique of CI-21, there were then and are still many CI professionals in intelligence and law enforcement who believe the United States is already doing all that can be done against the foreign intelligence threat. That self-evaluation might well be accurate in the context of traditional CI responsibilities with very limited budgets—but it misses the point behind the strategic CI mission.

The 2002 reform legislation charges U.S. counterintelligence with executing a new mission that cannot be performed by independent entities acting without central direction or strategic coherence. The intent was not to impose a new layer of bureaucracy, or peel away authority or responsibility from the several operational organs, but to assign additional duties to each of them to meet strategic CI objectives. The objective was to integrate the diverse capabilities of the U.S. CI enterprise at home and abroad to go on the offense against hostile intelligence threats directed against the United States.

CIA, in particular, would need new resources and focus. During the Cold War, the CIA/DO correctly understood one of its primary tasks, the clandestine penetration of the KGB, to be an important contribution to the overall, but generally undefined, national U.S. CI mission. But the Agency has never seen itself with a comprehensive overseas CI mission corresponding to the mission that evolved for the FBI domestically.

To be sure, foreign intelligence personnel are already at or near the top of the DO targeting list. (Clandestine HUMINT, of course, is not the only collection means of value against foreign intelligence operations.) But it is one thing to check the box for recruitment opportunities, and quite another to have a top down, strategically orchestrated effort to disrupt and degrade the operations of a foreign intelligence service. Moreover, while there is no question that the orientation and work ethic of individual FBI agents and other CI professionals are very proactive when it comes to working individual cases, there is a vast difference between the personal initiative exhibited by a law enforcement officer or a CIA station and the coordinated strategic initiative demanded of the Nation's lead executing agencies for CI.

The challenge remains how to pull together a strategic CI capability—one team, one plan, one goal. To that end, CI professionals need to have a clear understanding what we are trying to achieve… of what they together are being asked to achieve. And here we have yet another problem.

Neither "strategic counterintelligence" nor a strategic CI program is defined in law, policy guidance, or anywhere else.[9] The very concept of a national counterintelligence mission, different from what the operating arms are already doing, remains new and untested. And their CI leadership knows that objectives set forth in a national strategy one year can change in the next—and have.

8. The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, Report to the President of the United States, March 31, 2005, p485; emphasis added.

9. In testimony last year before the SSCI, I offered these draft definitions:

> **Strategic Counterintelligence:** the direction and integration of counterintelligence activities to compromise or disrupt the ability of foreign intelligence services to harm U.S. national security interests at home or globally.
>
> **Strategic CI Program:** U.S. national counterintelligence shall develop options to degrade the ability of [nation state] to project force or prosecute national objectives, establish or maintain hostile control, or conduct operations or collect intelligence against U.S. interests globally, by means of their intelligence activities.

The President can issue strategies, the interagency can table implementation plans, the budget examiners can have their say, but at the end of the day it is what the operators actually do against the adversary that will matter most. Without the discipline of a national program, CI management will continue to measure performance against the individual agency metrics for which they are accountable, as they must. But is that enough to counter the foreign intelligence threats directed against the United States?

Unique Roles/Responsibilities of Counterintelligence

A fundamental purpose behind creating a head of U.S. counterintelligence was to hold someone accountable to the President and the Oversight Committees for answering that question. In particular, does the federal government have the capabilities required to influence by deception, compromise by penetration, or disrupt by arrest, expulsion or exposure the threats posed to the United States by hostile intelligence services, their officer cadre, agents and proxies? That scorecard today may be very much in doubt.

By default, the field gets occupied by security or risk management practices on the one hand, and collection on the other, with far less attention or resources devoted to the operational responsibilities of U.S. counterintelligence. The two-way relationships with security and collection are intricate and absolutely essential – but there is a field of endeavor that is uniquely CI which is too often neglected because these other things have metrics and immediacy that are so much more familiar and demonstrable.

Indeed, the practical objectives of CI and security are not always in concert, "one of the classic conflicts of secret operations."[10] It is the duty to engage the adversary (an anathema to security, which wants to keep the adversary as far away as possible), and the duty to take action to exploit or disrupt them (which is at odds with collection), that form the heart and soul of counterintelligence. While there are defensive aspects to CI tradecraft, the imperative to penetrate and control the adversary service is what the CI mission is all about.

The Senate Intelligence Committee called attention to the importance of the security/CI distinction in its 1986 report, *Meeting the Espionage Challenge*:

> An effective response to the foreign intelligence threat requires a combination of counterintelligence and security measures. The Committee believes it is important to distinguish between counterintelligence efforts and security programs, while ensuring that both are part of a national policy framework that takes account of all aspects of the threat.[11]

In practice and by executive order, counterintelligence is closely related to, but distinct from, the security disciplines:

- Counterintelligence authorities and responsibilities are assigned by Executive Order 12333. Those 17 entities – not every potential foreign intelligence target – make up the CI enterprise.
- Security by contrast is a "command function" (in military terms), meaning that the head of each department/agency/office/post/private enterprise is responsible for the guards, gates, locks, personnel, firewalls, etc., protecting their assets and operations against foreign intelligence threats as well as other compromise, theft or loss.
- As the 1986 Senate report explained, "counterintelligence measures deal directly with foreign intelligence service activities, while security programs are the indirect defensive actions that minimize vulnerabilities."[12]
- The CI mission includes providing threat assessments to federal departments and agencies, as well as outreach to the private sector; but their respective security offices are responsible for developing and implementing the plans and programs they deem necessary to reduce their vulnerabilities. In practice, there are very close working relationships between security and CI officials, with especially well-developed protocols for handling insider threat issues.
- Other government entities such as the Committee on Foreign Investment in the United States also need insights into foreign intelligence activities (e.g., supply chain exploitations, front companies) in the course of their work; again, they are consumers of CI analytic products but not part of the CI enterprise.

Why do these distinctions matter?

Under DNI James Clapper, the Office of the NCIX was rebranded the National Counterintelligence and

10. Christopher Felix, *A Short Course in the Secret War*, 4th ed. (Lanham, Maryland: Madison Books, 2001), 126.

11. *Meeting The Espionage Challenge: A Review of United States Counterintelligence and Security Programs*, Report of the Select Committee on Intelligence, United States Senate (99th Congress 2nd Session) October 3, 1986, p38.

12. Ibid.

Security Center (NCSC)—one of four such centers within the Office of the DNI. While co-mingling the two may seem benign, in practice that model has a long-standing track record of drawing time, attention and budgets away from the very difficult business of identifying, assessing, disrupting and exploiting foreign intelligence operations. By its nature, security has an unbounded appetite for dollars and attention. It is the here and now versus the longer-term, strategic needs of counterintelligence. And the here and now always gets priority.

Counterintelligence may be the most manpower-intensive mission of all the national security disciplines, short of war. Espionage investigations, in particular, require the investment of years of detailed analysis, surveillance, translations, asset development, intelligence collection and other operations. While just one well-placed spy can exact a tremendous amount of damage, the hunt to find him or her typically involves a huge amount of work often around the clock by teams of people with nothing to show for it for years at a time, if ever.

That workload did not diminish when the Cold War came to an end. The freer movement of people and goods across borders also meant more freedom of movement for adversary intelligence services targeting the United States. Even so, after the "peace dividend" cuts of the mid-1990s, followed by the sweeping, overnight reprogramming of personnel from CI to counterterrorism after the terrible events of 9/11, CI resources at the FBI dropped 50 percent from Cold War levels, where they have hovered ever since.[13]

Today, the FBI must cover more than 800 trained and state-sponsored foreign intelligence officers embedded within a standing foreign diplomatic community of more than 30,000, which provides operational cover-for-action from more than 800 buildings in more than 30 American cities, each of which enjoys diplomatic immunity. Of the foreign intelligence services highest on the annual National Threat Identification and Priority Assessment, U.S. counterintelligence has resources to cover fully less than 10 percent of their personnel residing in or transiting the United States. And according to FBI Director Christopher Wray,[14] the FBI is opening a new China-related counterintelligence investigation every 12 hours (not to mention all the others).

By any measure, U.S. counterintelligence resources are stretched very, very thin.

As national leadership looks increasingly to our CI agencies to shoulder the security mission, it may well be exacerbating the problem, as scarce CI resources are diverted to other purposes – giving adversary intelligence services an even freer playing field in which to operate. Paradoxically, if more robust security is bought at the expense of the U.S. government's ability to counter hostile intelligence operations, then America's national security secrets, critical infrastructure and technologies, and proprietary information will end up more at risk.

With the best of intentions, our CI leadership may be making matters worse by broadening its use of the term "CI community" to include government departments and agencies, along with private industry and academy, who are responsible for their own security plans and programs and thus need to be aware of foreign intelligence threats. Here, the FBI has taken the lead in standing up joint "CI" task forces, engaging interagency partners and reaching out to community leaders, in all 56 field offices, plus a National Counterintelligence Task Force to consolidate and build upon those efforts. But security is not CI.

In London during the Blitz, air raid sirens warned the population of approaching enemy bombers so they could take cover, while anti-aircraft artillery and fighter interceptor squadrons were deployed to take out the bombers. Protection is vital – and so is offense. Similarly, while the security mission is vital, so is countering hostile intelligence threats. It's up to counterintelligence to find and take out those allegorical "bombers" – preferably long before they reach their targets.

Yes, strengthen security, educate the public, pursue legal remedies, engage social media platforms to block dangerous content, counter disinformation with the truth. These are all essential protective measures against foreign intelligence operations directed against us. But they are not enough. They will never be enough.

We are ceding the initiative to our adversaries. That has to stop. So whose job is that?

Leading U.S. Counterintelligence —the Job Ahead

One of the strengths of a democracy that holds Presidential elections every four years is the infusion

13. To add to the problem, in 2006 the DNI tasked this diminished CI workforce, subject to law and the protection of civil liberties, to take on a whole new job: to collect intelligence on the broad sweep of national intelligence priority targets – with no new resources assigned for that purpose. That tasking – as another duty as assigned – still stands.

14. Christopher Wray, "Countering Threats Posed by the Chinese Government Inside the U.S." Remarks delivered at the Ronald Reagan Presidential Library and Museum, Simi Valley, California, January 31, 2022.

of new ideas. Institutional memories and professional cadres are of unquestionable value to any government organization. But so is the opportunity for new leadership to bring fresh eyes, a new vision, and new energy.

The evolution of the NCIX, now the NCSC, is no exception. As I look back at the record of my time in office, and that of my four successors to date (with President Biden's head of counterintelligence, as of this writing, yet to be named), I see different paths, different priorities, and different outcomes. In particular, the need to respond to broader national level concerns has commanded the time and attention of the office.

I came into the job when the country was at war, still suffering from the wounds of 9/11 and determined never to let anything like that happen again. The strategic offensive orientation of the national CI mission, as captured in the 2005 National CI strategy, is in part a reflection of that determination. Cyberthreats would receive more prominent attention by the head of U.S. counterintelligence in years to come, as OPM data bases were raided by Chinese (and other) cyber intruders, along with countless other sensitive government and private sector IT infrastructure, with the true extent of damage still unknown—and growing.

And there is no question that compromises by insiders, especially the cases of Snowden and Manning, led to voluminous damage assessment work and the institutionalization of insider threat task forces and program metrics across the federal government, under the leadership of the national CI office.

The decision by DNI Clapper to merge the security portfolio under the head of U.S. counterintelligence further expanded the office's responsibilities. To date, the NCSC has compiled a solid record of accomplishment in outreach and public education, supporting interagency security efforts, and complementing the FBI's long-standing interactions with business, industry and academia.

By contrast, the imperative in creating the NCIX was to put someone in charge of U.S. counterintelligence, in order to bring strategic coherence to the enterprise. In 2016, we saw the first concerted effort by a foreign power to influence the course of a U.S. presidential election, which proved only a first wave of malign influence operations to come. In this fight, U.S. counterintelligence has specialized resources to bring to bear – and which, in my view, warrant the focused attention of the national CI office.

Unfortunately, two decades after its creation, there is no enduring agreed vision for what the NCIX/NCSC should be doing.

If the measure of effectiveness is how many awareness briefings have been provided to key industry leaders, how many educational materials have been disseminated, and how many agencies have met their insider threat program objectives, then I believe the record of the NCIX/NCSC will show important strides over the past 20 years.

But if the measure of effectiveness is how successful we have been in building a national-level, strategic capability to identify and disrupt hostile intelligence operations directed against the United States, then we need to give ourselves an "F."

Throughout history, America's counterintelligence professionals have made tremendous contributions to the security of our Nation. Thanks to their dedicated work, there is no reason to doubt that we are deriving about as much value as possible from the old business model of U.S. counterintelligence. But the sum of what our CI agencies do will not bring us a strategic offensive gain against foreign intelligence threats unless orchestrated to a common end.

This essential orchestration was to have been the new and force-multiplying job of the national head of U.S. counterintelligence. One team, one plan, one goal. That job still needs to be done.

The Honorable Michelle Van Cleave was appointed National Counterintelligence Executive by President George W. Bush in 2003. She later served as Director of Security, United States Senate (2020-2021). This article is adapted from her September 21, 2022 testimony before the Senate Select Committee on Intelligence hearing on the National Counterintelligence and Security Center (successor to the NCIX). She currently is a member of AFIO's Board of Directors.