McCRARY INSTITUTE
FOR CYBER AND CRITICAL INFRASTRUCTURE SECURITY

Statement of Frank Cilluffo

Before the

House Permanent Select Committee on Intelligence

Hearing:

"Persistent Competition and Legacy Architectures"

Wednesday, September 2, 2026

Chairman Crawford, Ranking Member Himes, and distinguished Members of the Committee, thank you for the opportunity to appear before you. I commend the Committee for holding this rare public hearing and for bringing greater public visibility to the consequential work of the Intelligence Community. Today's subject, the changing counterintelligence threat, is both timely and troubling. The People's Republic of China is conducting a sustained campaign to acquire and exploit American innovation, technology, talent, and industry in ways that threaten not only our economic competitiveness, but our national security.

The nature of the counterintelligence challenge has evolved considerably, but too much of our architecture for confronting it has not. For the last several decades, counterintelligence was understandably focused on protecting government secrets, identifying foreign intelligence officers, uncovering penetrations, and preventing adversaries from gaining access to sensitive national security information. Those missions remain essential, but they are no longer sufficient to protect the full range of assets that determine American power and strategic competitiveness. Our approach to the counterintelligence landscape must protect America's strategic advantage, not merely its secrets.

Today, an adversary does not necessarily need to penetrate a classified facility or recruit a government official to acquire something of enormous strategic value. It may instead target a researcher at a university, an engineer at a technology company, a promising start-up, a venture capital firm evaluating emerging technologies, or the supply chain supporting a critical American industry. In many cases, the technology or knowledge being sought is not classified at all. Yet its loss can still have profound consequences for our national security. That distinction matters. We should not allow a twentieth-century definition of what constitutes a national security asset to constrain our response to a twenty-first-century counterintelligence threat.

The United States faces a stark mismatch in how we approach the counterintelligence threat. Our adversaries, most notably the Chinese Communist Party, run campaigns. We open cases. What's more, our interagency structures remain ill-equipped to recognize and act against threats that cut across institutional and jurisdictional boundaries. That difference is not merely semantic; it goes to the heart of the problem before us. Our institutions are very good at investigating

identifiable incidents. We can open a case, determine whether a law has been violated, identify the responsible actors, pursue an investigation, and, where the evidence permits, bring an enforcement action. Those are important capabilities and we should continue to invest in them.

But a strategic competitor is not measuring success one prosecution at a time. They are looking across years, industries, institutions, and technologies. Further, they can pursue multiple avenues simultaneously and accept failure in any individual effort because the objective is cumulative. A failed acquisition, an unsuccessful recruitment effort, or an exposed cyber operation does not necessarily end the campaign. The adversary simply moves to another company, another researcher, another investment vehicle, another intermediary, or another means of access.

We, therefore, need to become much better at seeing the whole picture. A series of seemingly disconnected events can take on a very different meaning when viewed together. Information held by the FBI may be important to understanding activity seen by the broader Intelligence Community. That information may, in turn, illuminate something being experienced by the Department of War, the Department of Homeland Security, the Department of Energy, or a company that has never considered itself part of the national security enterprise at all. The individual pieces may reside in different places, under different authorities, and for perfectly legitimate reasons. The adversary does not organize its campaign around our organizational charts.

National security and economic security are inextricably interwoven. We are no longer dealing only with spy versus spy, nation versus nation, or the protection of military or intelligence secrets. All of those still matter, but far more is now at play. Increasingly, the technologies that shape our military power, intelligence capabilities, economic competitiveness, and geopolitical influence are developed outside government. American strategic advantage is increasingly generated through private-sector technological innovation.

This represents a fundamental change in the environment in which counterintelligence operates. Many of the technologies that will shape military power, intelligence capabilities, economic competitiveness, and geopolitical influence over the next generation are being developed primarily or substantially in the private sector. Artificial intelligence is perhaps the clearest example, but the same dynamic is visible in biotechnology, quantum technologies, advanced computing, autonomous systems, space, energy technologies, and other fields.

The government, therefore, cannot protect America's strategic advantage simply by building higher walls around classified information. In some instances, by the time a technology becomes incorporated into a classified government program, the underlying research, talent, intellectual property, capital, and supply chain have already been the subject of foreign attention for years.

Frontier artificial intelligence companies illustrate the problem particularly clearly. Their model weights, training techniques, proprietary data, compute infrastructure, specialized talent, and knowledge of emerging capabilities may all be of significant intelligence value even when they are not classified and the company has little history of working with the national security community. Foreign collection may target not only the company itself, but its employees, investors, cloud providers, vendors, overseas facilities, and research partners. A counterintelligence model centered predominantly on classified government programs will arrive too late to protect much of what matters.

This is particularly important when thinking about China. Beijing does not draw the same clean distinctions we often do between economic competition, technological development, intelligence collection, and national security. We should not mirror the Chinese system, nor should we abandon the openness that has been central to American economic and technological success. But we do need to understand the strategic environment as it actually exists.

The United States derives tremendous strength from being an open society. We attract talent and encourage investment. We collaborate across universities, companies, and borders. We reward entrepreneurs willing to take risks on technologies that may not pay off for years. Those characteristics are strategic advantages, not vulnerabilities to be engineered out of our system. The goal is not to put walls around American innovation. It is to prevent our openness from becoming an adversary's operating model.

That last point deserves particular attention. Much of the activity we should be concerned about may fall below the threshold for a traditional counterintelligence or law enforcement response. A transaction may be legal. A business relationship may appear legitimate. A researcher may receive an invitation that, viewed by itself, raises no obvious alarm. An investor may be several steps removed from a foreign government. A company may encounter repeated attempts to acquire information without having any visibility into similar approaches being made to its competitors. No single event necessarily tells the story.

That is precisely why a campaign-based mindset to counterintelligence is important. The government has access to information that individual companies and institutions do not. That information should inform collection priorities and be integrated into campaign assessments that identify the adversary's objectives, priority targets, methods of access, intermediaries, recurring vulnerabilities, and likely next moves. At the same time, the private sector sees activity that the government may never observe unless companies have a reason and a mechanism to share it. Neither side possesses the entire picture. This creates a warning problem as much as an enforcement problem. The question should not simply be whether the government can investigate an incident after something has happened. We should also ask whether we can identify patterns early enough to warn those who are likely to be targeted next.

The Intelligence Community has extraordinary insight into foreign intentions and capabilities. But intelligence is useful only to the extent that it reaches the people who can

act on it. In this environment, those people increasingly include executives, chief technology officers, investors, university leaders, researchers, and others who may never hold a security clearance. We need to get better at translating intelligence into actionable information for those communities. That does not mean exposing sources and methods or indiscriminately sharing classified information. It means developing a more mature capability to provide companies and institutions with enough information to understand why they may be targets, what activity to look for, whom to contact, and what practical steps can reduce their risk. A warning delivered after the technology, talent, or access has been lost is not strategic warning.

That relationship must also run in both directions. Government cannot simply appear after an incident and ask the private sector for information. Trust is difficult to establish in the middle of a crisis. Companies need to know whom to call before something goes wrong, what information is useful, how information they provide will be handled, and what they can reasonably expect in return. A relationship in which information moves only toward government will not produce the sustained trust, visibility, or private-sector action that a campaign-based model requires.

For smaller and emerging technology companies, this challenge is especially acute. A major defense contractor or large technology company may have experienced security personnel, established government relationships, and employees who understand how the Intelligence Community operates. A ten-person biotechnology company or rapidly growing artificial intelligence start-up may have none of those things. Yet the technology being developed by that small company could be precisely what a foreign intelligence service or state-backed entity finds most valuable. We should not expect every American innovator to become a counterintelligence expert. The government needs to meet these companies where they are.

The objective should be informed openness: preserving the characteristics that make the United States the world's leading destination for innovation while becoming far more sophisticated about protecting the technologies, people, and institutions that create enduring strategic advantage.

Informed openness requires prioritization. The United States cannot protect every technology, company, and institution to the same degree, nor should every commercially valuable technology or foreign business interaction be treated as a counterintelligence matter. Government and industry should maintain a dynamic, intelligence-informed understanding of the technologies, talent, data, infrastructure, and supply chains whose compromise could materially erode American national security or strategic advantage. That assessment should evolve as technologies mature, adversary priorities change, and new dependencies emerge.

Once we have identified the assets and capabilities that matter most, the next question is whether the government can integrate the information necessary to recognize and counter the campaigns targeting them—and who is ultimately accountable for the outcome. Today, pieces of that picture are spread across the U.S. Government and Intelligence Community without being fully integrated. Form should follow function, not the other way around.

There are many agencies with legitimate responsibilities in this space. The FBI has an essential counterintelligence and law enforcement role. The National Counterintelligence and Security Center has an important integrating mission. Intelligence agencies like the CIA and NSA collect information about foreign actors and intentions. The Departments of Commerce and Treasury possess important economic and regulatory authorities. The Departments of Energy and War have deep relationships with strategically important sectors and technologies. Other departments and agencies bring additional pieces of the picture. The problem is not that these organizations lack talented people or important authorities. The problem is that distributed responsibility can easily become diluted accountability. When everyone owns a piece of a problem, it is sometimes difficult to identify who owns the outcome. That accountability gap deserves focused examination at the Executive Office of the President. Whether through a dedicated official, a strengthened existing role, or another mechanism, the essential requirement is a senior individual empowered to integrate the effort, drive action across organizational boundaries, and answer for outcomes.

I agree with the Committee's focus on achieving better counterintelligence outcomes rather than beginning with a presumption that a new agency, office, or organizational box is inherently required. Structural change may prove necessary, but form should follow function. The better starting point is to define what the government must be able to accomplish, determine whether the existing architecture can perform those functions, and then decide whether specific organizational reform is required.Who is responsible for identifying a coordinated foreign campaign that cuts across intelligence, economic, academic, and commercial activity? Who is responsible for integrating the information necessary to understand that campaign? Who decides when the government has enough information to warn the private sector? Who ensures that the warning reaches the right people? Who identifies gaps in authorities or information sharing? Are our actions changing adversary behavior and reducing adversary access? And, importantly for this Committee, who is accountable to Congress for whether that system delivers? Those are functional questions. Once they are answered, Congress can determine whether the existing architecture is capable of performing those functions or whether structural change is necessary.

Building on the logic of CIA's mission-center model, which brings multiple disciplines together around priority threats, Congress should examine whether that approach can be adapted more broadly across the counterintelligence enterprise. An enterprise-wide mission-center approach could integrate relevant information and expertise from the Intelligence Community, law enforcement, economic and regulatory agencies, and affected industries; produce a common campaign picture; identify opportunities for warning and disruption; and support the senior official accountable for the mission. It need not require a new agency or the transfer of existing statutory authorities. Its essential value would be to organize existing capabilities around adversary campaigns and national outcomes rather than organizational boundaries.

Identifying a campaign and warning its targets are necessary, but they are not the end state. Once a sustained foreign campaign is understood, the government should bring together the full range of lawful diplomatic, intelligence, law enforcement, economic, cyber, and regulatory tools to disrupt it. Depending on the circumstances, that may mean denying access, exposing

intermediaries, blocking transactions, disrupting technical infrastructure, strengthening a targeted supply chain, or imposing costs on those directing and enabling the activity.

Our metrics should reflect the threat we are actually trying to defeat. Arrests, prosecutions, intelligence reporting, and disrupted operations remain important, but they measure only parts of the mission. If our adversaries are conducting campaigns, we should ask whether we are reducing their access to priority technologies, increasing the time and cost required to achieve their objectives, preventing repeated exploitation of the same seams, and delivering warning early enough to change outcomes. Success cannot simply mean that we investigated yesterday's compromise. It should increasingly mean that we prevented tomorrow's while simultaneously making the adversary's next attempt more difficult, costly, and likely to fail.

We have to find a way to thread the needle that fosters the very innovation that gives us strategic and security advantage while also protecting the private sector now being targeted by our adversaries. That will require a different conception of counterintelligence than the one with which many of us grew up. It must remain rooted in the traditional mission of identifying and countering foreign intelligence activity, but it also has to account for where American power resides today and where it is going tomorrow. The objective is not to turn Silicon Valley, our universities, or American investors into extensions of the Intelligence Community. Nor is it to place government in the position of deciding which technologies or companies are worthy of protection. It is to recognize that the front lines of strategic competition increasingly run through institutions that were never designed to think of themselves as part of a counterintelligence contest. Government has to adapt to that reality.

For Congress, I believe a more effective counterintelligence model should be built around four essential functions. First, identify and continually reassess the technologies, talent, data, infrastructure, and supply chains most consequential to American national security and strategic advantage. Second, integrate information across agencies and the private sector so that seemingly isolated incidents can be understood as elements of a sustained foreign campaign. Third, translate intelligence into timely, actionable warning that enables companies, universities, investors, researchers, and other institutions to protect themselves. Fourth, use the full range of lawful national instruments to disrupt those campaigns, impose costs, deny repeated access, and measure whether adversary effectiveness is actually declining.

Clear accountability must run through all four functions. Congress should be able to determine who is responsible for integrating the campaign-level picture, who can drive a coordinated response, whether warnings reached those capable of acting on them, and whether the government's actions materially protected the assets at risk.

None of this will be easy. China and other sophisticated adversaries have studied our strengths, our institutions, and the boundaries between them. They understand that the advantage in this century will be determined not onlyby who possesses the best military platforms or the most closely guarded government secrets, but by who leads in the technologies that will shape economic and military power for decades to come. The United

States begins that competition with extraordinary advantages. We have the world's leading innovators, universities, entrepreneurs, capital markets, and research institutions. We have an Intelligence Community with capabilities that remain the envy of the world. And we have allies and partners who multiply those advantages.

Our task is not to fundamentally change those institutions. It is to connect them more effectively, protect what matters most, and make it considerably harder for our adversaries to exploit the gaps between them. The threat has changed. Our counterintelligence model must change with it.