Michelle Van Cleave[i]
Former National Counterintelligence Executive
Senior Fellow, George Washington University

Statement before the
House Committee on Science, Space, and Technology
Subcommittee on Oversight, Subcommittee on Research and Technology
April 11, 2018

Joint hearing on foreign nations' exploitation of U.S. academic institutions for the purpose of accessing and exfiltrating valuable science and technology (S&T) research and development

Co-Chairs Abraham and Comstock, Ranking Members Beyer and Lipinski:

It is a privilege to appear again before this Committee, where early in my career I had the honor of serving as Minority Counsel. The last time I testified before the Oversight Subcommittee was five years ago, also on the subject of espionage threats to America's science and technology base. I recall nodding in agreement with my fellow panelists:

- *The open exchange of ideas is essential not only to discovery and research, but also to America's leadership and values,* said one of the country's most distinguished engineers.
- *China is saving incalculable amounts of time, money and research effort through espionage and intellectual property theft directed against the U.S*, said the expert from the U.S. China Commission.
- *The numbers of economic espionage cases and export control violations are increasing every year, and we don't have the resources to keep up with them,* said the former FBI special agent.

So what should we do? asked the Chairman. What indeed.

For even as our hearing was underway, surveillance cameras at NYU's medical center were capturing an associate professor of radiology and two research assistants – all from China – secretly photographing MRI technology developed by another team under a $4 million NIH grant, which (the criminal complaint alleges) they were "sharing" with a research institute sponsored by the Chinese government.[1] Their subsequent arrests and later plea deals are but a drop in an overflowing bucket.

[1] Department of Justice https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-and-fbi-assistant-director-charge-announce-criminal-complaint

As this Committee is well aware, American R&D -- the engine for new ideas and products and capabilities and wealth -- is systematically targeted by foreign collectors to fuel their business and industry and military programs at our expense. By far the vast majority of foreign acquisition of U.S. technology is open and lawful, as are the transactions of individuals and businesses involved in international commerce, as well as the free exchange of ideas in scientific and academic forums. Even so, while the United States leads in the world in R&D spending, with annual investments of some $510 billion,[2] we are losing most if not more of that dollar amount every year through systematic theft.[3] It continues to be what Gen. Keith Alexander, then Director of the National Security Agency, memorably called "the greatest transfer of wealth in history." That was six years ago … and counting.

China, which accounts for nearly a third of the growing foreign student population in the United States[4] and the lion's share ($385 billion in 2017) of our trade deficit,[5] easily tops the threat list. It's not just that there are a lot of Chinese nationals working in American companies or laboratories, or studying or teaching at American universities, picking up whatever happens to come their way. No. As the Defense Department has reported,[6] China has a government-directed, multi-faceted secret program whose primary task is technology acquisition, as well as a highly refined strategy to develop and exploit access to advantageous information through the global telecommunications infrastructure.

In fact, China and Russia both have detailed shopping lists of targeted U.S. technologies and specific strategies for clandestine acquisition, ranging from front companies to joint R&D projects to cyber theft to old fashioned espionage; nor are they alone. There is also a third party black market for that stolen S&T, for both commercial and military buyers.

In other words, foreign targeting of the U.S. science and technology base is driven by purposeful collection, tasking and exploitation by foreign nations who employ the full reach of their intelligence capabilities to that end. And business is booming.

Indeed, the United States is a spy's paradise. Our free and open society is tailor-made for clandestine operations. Most of the golden eggs worth collecting are found within our borders: military plans, diplomatic strategies, weapons designs, nuclear secrets, proprietary R&D from companies such as Bell Labs or Dupont or Boeing. And foreign powers are running intelligence operations throughout the United States with unprecedented independence from the safe havens of their diplomatic establishments, leaving our counterintelligence efforts in the dust.

---

[2] National Science Foundation https://www.nsf.gov/statistics/2018/nsf18306/

[3] 2017 Update to the IP (Blair/Huntsman) Commission Report "We estimate that at the low end the annual cost to the U.S. economy of several categories of IP theft exceeds $225 billion, with the unknown cost of other types of IP theft almost certainly exceeding that amount and possibly being as high as $600 billion annually."

[4] Institute of International Education https://www.iie.org/Why-IIE/Our-Vision

[5] U.S. Trade Representativehttps://ustr.gov/countries-regions/china-mongolia-taiwan/peoples-republic-china

[6] Department of Defense http://archive.defense.gov/pubs/2013_China_Report_FINAL.pdf

U.S. academic institutions, with their great concentration of creative talent, cutting edge research endeavors, and open engagement with the world of ideas, are an especially attractive environment for foreign collectors targeting America's R&D wealth. The advent of social media has opened the door even wider. As FBI Director Christopher Wray explained before the Senate Intelligence Committee earlier this year,

> The use of non-traditional collectors, especially in the academic setting — whether it's professors, scientists, students — we see in almost every field office that the FBI has around the country. It's not just in major cities. It's in small ones as well, it's across basically every discipline. And I think the level of naiveté on the part of the academic sector about this creates its own issues.
>
> They're exploiting the very open research and development environment that we have, which we all revere. But they're taking advantage of this. One of the things we're trying to do is to view the Chinese threat as not just a whole of government threat, but a whole-of-society threat, on their end. And I think it's going to take a whole-of-society response by us. It's not just the Intelligence Community, but it's raising awareness within our academic sector, within our private sector, as part of defense.[7]

Raising awareness is obviously an important part of the answer. But so is raising our ability to act. And that's not a private sector job; it's a U.S. government job.

Year after year, we dutifully collect data about how much of our nation's wealth is hemorrhaging out the door through illicit foreign collection. For its part, the Congress properly attempts to raise awareness through hearings such as this, passes new legislation to strengthen law enforcement's reach and victims' legal recourse, gives the President sanctions authority, and advances security measures to protect against these activities. Yet, as important as they are, more robust security programs, awareness training, FOCI regulations, diplomatic demarches and tech transfer laws alone – the current suite of our technology protection efforts – will never be enough to stop these massive programs of state-orchestrated technology theft.

Which brings me back to our hearing, five years ago. Toward the end, one of the Members asked pointedly, *Isn't there a way we can go on offense?* Yes, I answered, there most certainly is – but national leadership must be willing to revamp our counterintelligence enterprise to get there.

Today I thought we might pick up where that conversation left off. To be sure, counterintelligence is only one part of the policy mix that is needed to effectively counter illicit technology acquisition. But I have observed that the government's ability to identify and disrupt foreign intelligence operations is the piece too often neglected in open discussions such as this … or even within national security councils behind closed doors.

---

[7] https://www.intelligence.senate.gov/hearings/open-hearing-worldwide-threats-hearing-1

Why is that? Perhaps because counterintelligence is seen as the purview of intelligence and therefore not usefully addressed in the open. Or perhaps because its potential contributions to national security are simply not generally understood. Yet if war is too important to be left to the generals, as Clemenceau famously said, then counterintelligence is too important to be left to the intelligence community.

Accordingly, I'd like to provide some background on how U.S. counterintelligence has evolved over the years, why it is not optimized for sweeping strategic challenges such as the subject of today's hearing, and what needs to be done now.

The work of clandestine services, engaged in intelligence collection and other activities, is an arena of international competition where the advantage does not necessarily go to the rich or the otherwise powerful. Foreign adversaries may not have a prayer of fielding costly and technologically demanding technical collection suites, but they can organize, train, equip, sustain and deploy impressive numbers of case officers, agents of influence, saboteurs, hackers and spies; and the United States has become the single most important collection target in the world. Intelligence operations against the United States are now more diffuse, more aggressive, more technologically sophisticated, and potentially more successful than ever before, especially within U.S. borders, where America's rich, free society and an extensive foreign presence provide opportunity and cover for intelligence services and their agents.

By contrast, counterintelligence (CI) – identifying, assessing and neutralizing foreign intelligence threats -- has been little more than an afterthought in U.S. national security strategy,[8] a legacy of neglect that has cost us dearly in lives lost, resources squandered, and dangers unchecked.

Sixteen years ago, in the wake of a devastating espionage case that shook the U.S. intelligence community to its core,[9] with worse to come,[10] Congress took a hard look at the CI enterprise and saw that it was little changed from the set pieces that emerged after World War II. The three major operating elements each had become highly proficient in their respective CI responsibilities: 1) the FBI, far and away the largest CI organization in the U.S. government, whose principal job is to find the spies and arrest them; 2) CIA, whose main CI concern is to make sure our spies succeed; and 3) the Defense Department, charged with protecting against enemy intelligence operations. These are all vital missions.

Yet foreign intelligence services don't target an FBI field office, or a CIA station, or a military installation abroad; they target the United States.

---

[8] Notably, none of the National Security Strategy guidance issued by U.S Presidents over the past four decades has addressed countering foreign intelligence threats as part of national policy or strategy... including the latest iteration in 2017 https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf

[9] Aldrich Ames - SSCI https://www.intelligence.senate.gov/sites/default/files/publications/10390.pdf; D/CIA https://www.cia.gov/news-information/press-releases-statements/press-release-archive-1995/ps103195.html

[10] Robert Hanssen DOJ/IG https://oig.justice.gov/special/0308/index.htm

So whose job was it to perform systematic collection or analysis of foreign intelligence threats to the United States? To build a common operating picture of the threat against which to array our CI operations? To ensure a coherent assignment of resources to counter foreign intelligence activities?

Historically the answer was "no one." The *National Security Act of 1947* established the basic contours of the post-war U.S. intelligence community, but (other than defining the term[11]) said nothing about counterintelligence. In the decades since, we had no central leadership of U.S. counterintelligence, no agreed guiding principles or CI doctrine common to the discipline, and no national-level orchestration of U.S. counterintelligence activities against foreign intelligence threats to the United States.

In other words, while the threat is strategic, our CI enterprise was not designed to enable a strategic response. There was no overarching national leadership to provide cohesion or strategic direction for our CI activities. And no government entity had been given responsibility to ensure that foreign intelligence threats *to the United States* were identified, assessed and neutralized to protect America's national and economic security and advance our country's vital interests.

The Counterintelligence Enhancement Act of 2002 stepped into the void to create for the first time a national head of U.S. counterintelligence. The purpose was twofold:

- First, 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. (*E.g.*, Russian agents inside the U.S. government like Aldrich Ames at CIA and Robert Hanssen at the FBI had benefited from those seams for 9 and 21 years respectively, and DIA analyst Ana Montes – Cuba's star asset – for 17.)
- The second, equally compelling purpose was to develop and execute a national counterintelligence strategy to protect the United States against foreign intelligence threats targeting the riches of our economy and the openness of our society – a growth industry leading into the 21st century.

When President Bush appointed me to the new post, we conducted a top-to-bottom review of the U.S. counterintelligence landscape and concluded that tinkering around the edges wouldn't do. The national counterintelligence enterprise needed to be reconfigured to go on the offense, to exploit where we can, and interdict where we must, with the purpose of degrading adversary intelligence services and their ability to work against us.

The first *National Counterintelligence Strategy of the United States*, issued by President Bush in 2005, had this proactive reorientation as its central goal. "[E]ach member of the counterintelligence community must be prepared to assume new responsibilities, and join

[11] As defined in the National Security Act of 1947, **"**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".

together in a unity of effort…"[12] But before the ink was dry, the new office of the Director of National Intelligence (DNI) was established along with a new bureaucracy that steered policy and funding away from our nascent efforts to create a strategic CI capability.[13]

Unfortunately, the backsliding continued under President Obama. A directive (ICD 750) issued by DNI Jim Clapper in 2013 and still in force explicitly devolves authority and responsibility for all CI programs down to the department/agency level.[14] The national head of counterintelligence was rebranded director of a security and CI center, his duties further dissipated by the fixation on leaks and insider threats driven by the grievous harm done by Snowden, Manning, *et al*. Gone was any dedicated strategic CI program, while elite pockets of proactive capabilities died of neglect. Read between the lines of existing CI guidance and you will not find a whiff of a national-level effort left, other than caretaker duties such as taking inventory and writing reports.

Here's the problem. In creating a new head of U.S. counterintelligence, Congress sought to bring strategic coherence to our efforts to identify and neutralize the growing panoply of foreign intelligence threats: espionage, technology theft, deception and denial, and influence operations. But the means of execution – *a strategic counterintelligence program* -- was never put in place.

Sixteen years after the creation of the national CI office, we're back to square one.

U.S. counterintelligence is finely tuned to work individual cases, but it is not postured globally to detect, deter or disrupt the intelligence activities of China or any other foreign power, or to execute strategic counterintelligence operations. Under the current business model, there is no national level system that enables the integration and coordination of the diverse activities of U.S. counterintelligence to achieve common strategic objectives. There is no standard approach to targeting among the counterintelligence elements of the FBI, CIA and DOD; interagency information sharing is poor, and infrastructure support even worse. Even the modest national mechanisms developed to deconflict offensive CI activities stop at the water's edge, a legacy of the old divide between foreign and domestic operational realms.

In order to "go on offense," the U.S. government would need a means for identifying and neutralizing foreign intelligence activities directed against U.S. interests as an integral national security tool – something we do not have today. We know surprisingly little about adversary intelligence services relative to the harm they can do. And no single entity has a complete picture to provide warning of possible foreign intelligence successes, to support operations, or to formulate policy options for the president and his national security leaders.

[12] https://www.dni.gov/files/NCSC/documents/archives/FinalCIStrategyforWebMarch21.pdf
[13] Project on National Security Reform http://www.pnsr.org/wp-content/uploads/2007/12/michelle.pdf
[14] https://www.dni.gov/files/documents/ICD/ICD750.pdf

Going on offense also means not waiting until the threat is here, in our own backyard. We need to ask, how are adversary services trained, tasked, and funded? Where do they operate, against what targets, with what support? What is their leadership structure, their personnel rosters, their critical nodes of operation, the doctrine by which they deploy? And what are their vulnerabilities? What are the indicators that might give us warning of intelligence operations against us? Are there tripwires we can design to give us an edge? With such analytic insights, U.S. counterintelligence could seize the initiative and begin by working the target abroad, with the purpose of selectively degrading the foreign intelligence service and its ability to work against us.

To do that, the United States needs a strategic CI program – the budgets, billets, and processes -- to enable the integrated planning, orchestration and execution of CI operations to get inside hostile intelligence services, find their vulnerabilities, and neutralize them as national policy may dictate.

As the Congress considers how to close the floodgates of pilfered technology – or how to respond to Russian influence operations against our democratic institutions -- it would be instructive to take a fresh look at the Counterintelligence Enhancement Act, the performance of the national CI office, and the long-overdue modernization of our nation's CI enterprise. Successive administrations have let this vital mission slide, and we are paying the price in terms of America's vulnerability to technology theft and a long list of foreign adversaries and competitors who know an opportunity when they see it.

In my view, the choice is simple. We can handle these threats piecemeal, or we can pull together a strategic program -- one team, one plan, one goal -- to reduce the overall danger. We can chase individual spies or technology thieves case by case, or we can target the services that send them here. In short, we can go on offense … but national leadership must be willing to direct and empower America's counterintelligence enterprise to carry out that vital mission.

---

[i] *All statements of fact, opinion, or analysis expressed are those of the author and do not reflect the official positions or views of the U.S. Government, ODNI, or intelligence community.*