A New Counterintelligence Map for the AI Age

PREPARED STATEMENT BY
David Feith
Former Deputy Assistant Secretary of State for East Asian and Pacific Affairs, National Security Council Senior Director for Technology and National Security

BEFORE THE
Permanent Select Committee on Intelligence
United States House

HEARING ON
Persistent Competition and Legacy Architectures

Chairman Crawford, Ranking Member Himes, and members of the Committee: Thank you for the opportunity to testify.

Imagine that, in a future crisis over Taiwan, Chinese attack drones suddenly rise from trucks, warehouses, or farms deep inside the United States, just across the fence line from our nuclear-bomber bases. As U.S. forces mobilize, compromised Chinese-origin equipment inside large U.S. data centers rapidly shifts electrical load, destabilizing the power grid across 20 states. Chinese hackers, using AI systems trained on massive volumes of smuggled and remotely accessed U.S. compute, blind America's Golden Dome missile defenses. With a frontier model stolen from a compromised American AI lab and schematics stolen from a California-based space-communications startup, China's army exploits weak points in U.S. military networks and knocks U.S. Pacific forces offline at the decisive hour.

None of these scenarios is science fiction. We have already seen pieces of each one.

My central argument is simple: The United States needs a new counterintelligence map for the AI age.

During the Cold War and even after 9/11, much of our most sensitive technology lived inside government laboratories, military facilities, classified programs, and a relatively bounded defense-industrial base. Today, an extraordinary share of strategically important technology lives in private companies and commercial infrastructure: frontier AI labs, venture-backed quantum or fusion companies, semiconductor fabs, cloud platforms, data centers, drone manufacturers.

China's intelligence and technology-acquisition apparatus has every reason to follow American innovation into those places. Our own national-security

institutions must do the same.

In this testimony, I will describe the “Sputnik” problem in our approach to China, identify five key ecosystems requiring greater counterintelligence attention, and offer recommendations for protecting them.

1. THE SPUTNIK PROBLEM

We have had many supposed "Sputnik moments" in the China competition. The phrase is usually applied to an adversary's breakthrough: a Chinese hypersonic test, a new AI model, a military exercise, a supply-chain shock.

But that is not what made Sputnik, back in the 1950s, historically important. The Soviet satellite mattered because of what America did next.

The United States mobilized. It reorganized. It funded science and engineering. It created new institutions. It changed education, defense, space policy, and national priorities. The test of a Sputnik moment is not the adversary's accomplishment. It is our response.

By that standard, much of the China challenge has produced Sputnik warnings without a Sputnik response.

For more than a decade, Washington has recognized Chinese military modernization, cyber espionage, technology theft, supply-chain leverage, and subversion of critical infrastructure. We have made some important changes, but far too few.

The great American rethink on China has coincided with a great American rethink on America. Americans are skeptical of government competence and tired of ambitious national programs. Policymakers must respect popular sentiment. But we cannot allow justified skepticism to become strategic paralysis. If the government lacks capacities that national security requires, the answer is to build better capacities, not simply accept the vulnerability.

We now face compounding risks from China – those we have known about for years and still not adequately addressed, and those created by technologies and business models that didn’t exist even five years ago. The question is whether we will secure these points of vulnerability before Beijing exploits them.

2. SENSITIVE SITES AND THE SPIDERWEB PROBLEM

The first ecosystem of novel, AI-age national-security and counterintelligence risk I would highlight is military installations and other critical infrastructure now exposed to direct threats, especially from drones, that have matured with astonishing speed over the last five years.

The most vivid warning was Ukraine's Operation Spiderweb on June 1, 2025. Ukraine secretly trucked some 117 small drones deep into Russia and used them to attack Russian strategic bombers at four airfields, demonstrating that inexpensive systems pre-positioned inside an adversary's territory can produce strategic effects without penetrating its defenses from abroad. Israel demonstrated a related model weeks later, reportedly using drones and weapons pre-positioned inside Iran

against military and nuclear targets. Iran's own extensive use of drones across the Middle East has likewise shown how relatively inexpensive systems can threaten valuable targets while imposing enormous burdens on defenders. Counter-drone defenses and facility hardening are still struggling to catch up.

Apart from lessons from other countries' wars, our own experience at home should make us uncomfortable. Unidentified drones repeatedly appeared over Virginia's Langley Air Force Base and nearby sensitive facilities for roughly 17 nights in December 2023. In March this year, in the early innings of the Iran war, Louisiana's Barksdale Air Force Base – home to B-52 bombers and Air Force Global Strike Command – experienced several unauthorized drone incursions that remain under federal investigation.

See also Missouri's Whiteman Air Force Base, the operational home of America's B-2 stealth bombers. A trailer park immediately adjacent to the base was purchased through a web of companies controlled by foreign owners whom press reporting and members of Congress linked to individuals with alleged Chinese-intelligence ties. After that reporting, Missouri last year initiated cancellation proceedings against the operating partnership for violations of state corporate-registration requirements. Separately, a Chinese national pleaded guilty this year after repeatedly photographing Whiteman's perimeter, infrastructure, and military equipment.

The security perimeter of our most sensitive facilities must now extend well beyond the fence line. In a Spiderweb world, nearby farms, warehouses, and commercial properties can matter as much to base security as gates, guards, and guns.

Congress gave CFIUS authority to review certain foreign real-estate transactions near sensitive military installations, and Treasury expanded the list and geographic reach of covered installations in 2024. That was important. But implementation of the America First Investment Policy memo, issued by the Trump administration in February 2025 to tighten investment rules regarding farmland and other concerns, has been slow and limited.

The Spiderweb lesson suggests that land-security policy should be continually stress-tested against new operational realities, as warehouses, farms, commercial properties, and storage sites near critical facilities can become operational assets of strategic importance.

3. THE POWER GRID AND DATA-CENTER HARDWARE

A second ecosystem is America's power grid, especially where it now converges with the massive buildout of data centers.

Data centers create a novel grid-security challenge because of their scale and responsiveness. A major AI campus can draw 300 megawatts, 500 megawatts, or increasingly a gigawatt or more. Unlike traditional industrial loads, these facilities are densely computerized and can change their electricity consumption almost instantaneously. This can threaten the power grid, across vast geographies, in novel ways that were impossible just a few years ago.

We saw a hint of things recently, on July 22, when a routine transmission fault in Northern Virginia caused roughly 3,800 megawatts of data-center load to transfer rapidly from the grid to backup generation. The resulting imbalance produced large swings in voltage and frequency across the eastern United States, from Virginia to Chicago. Operators stabilized the system, and there was no blackout. It was not a cyberattack. But it demonstrated the physics an attacker would study: Several gigawatts of digitally controlled demand can move within seconds, with effects across a vast geography.

That makes the hardware inside these facilities a national-security concern. An adversary with synchronized access to enough inverters, batteries, uninterruptible-power systems, or other energy controls could potentially manipulate enormous blocks of demand to produce voltage excursions, frequency instability, or oscillations across a much larger grid.

A more obscure version of this problem is already with us in the form of cryptocurrency mines. A crypto mine is essentially a specialized data center: warehouses filled with computers operating continuously and drawing enormous amounts of electricity. Almost all U.S. crypto mines rely on Chinese-made compute and other equipment, and many have Chinese ownership and control, too.

In 2024, President Biden ordered the divestment of a PRC-owned crypto-mining operation within a mile of Wyoming's Warren Air Force Base after CFIUS found that its foreign-sourced equipment could facilitate surveillance or espionage against a key node of America's nuclear deterrent. The Senate Intelligence Committee has since warned about Chinese-made mining machines that can be remotely controlled from China and about the counterintelligence and grid risks created by large concentrations of them.

Remote control is not theoretical. Chinese inverter manufacturer Deye demonstrated in 2024 that it could remotely disable installed equipment abroad during a commercial dispute. Meanwhile, the research firm Strider has identified more than 2,700 Chinese research papers studying grid vulnerabilities, including hundreds it assesses as highly relevant to potential U.S. grid attacks and research involving PLA institutions.

The risk now extends far beyond crypto. AI data centers contain power equipment, servers, racks, networking gear, optical components, firmware, and cloud-connected control systems sourced through enormously complicated global supply chains.

Even a trusted allied company can carry substantial China exposure. Foxconn, for example, is Taiwanese and a critical partner to American AI companies, but its central role in AI-server and rack manufacturing alongside its longstanding Greater China footprint illustrates why a company's flag alone cannot answer the supply-chain-security question.

This is emphatically not an argument against building data centers. America needs to build them faster and at extraordinary scale to lead in AI and maintain military superiority. The question is whether we build that infrastructure securely.

President Trump's AI Action Plan got the principle right: America's AI stack and the energy and telecommunications infrastructure supporting it should be free of foreign-adversary technology. The FCC's recent action on foreign power inverters is an important start, as is President Trump's recent executive order restricting the use of foreign-adversary hardware in the bulk-power system. But we need greater visibility into the installed base, trusted-supplier and firmware standards, elimination of adversary remote access, better network segmentation, and grid rules designed for gigawatt-scale digital loads.

We should build America's AI infrastructure at speed – but not with an adversary's kill switches buried inside it.

4. FRONTIER AI LABS AND SUPERCHARGED IP THEFT

A third novel and vital ecosystem is America's frontier AI labs. These are private companies, but the capabilities they hold are strategic national assets—and prime targets for foreign intelligence services.

In the 1940s, America's nuclear monopoly lasted only as long as it took Soviet espionage to penetrate the Manhattan Project. But today's labs are not hidden away in the New Mexico desert. Their employees travel, change jobs, publish research, work with contractors and cloud providers, and operate enormous commercial networks. That openness helps drive American innovation while also creating a massive attack surface.

Government and the frontier labs should therefore organize around at least three key threats: cyber penetration, insider compromise, and industrial-scale distillation.

- **Cyber.** Capable as they are, U.S. frontier labs face nation-state adversaries with capabilities and intelligence that no private company can match. Washington should establish durable channels for classified threat sharing, incident coordination, defensive assistance, and government vetting and investigative support. Labs, in turn, need defense in depth across model weights, internal systems, data centers, cloud providers, contractors, and trusted partners.
- **Insider Threats.** The case of Leon Ding and Google should be treated as a warning, not merely a successful prosecution. In January, a jury convicted the former Google engineer of economic espionage and trade-secret theft after he stole more than 2,000 pages of confidential AI information while secretly building a business in China. The question is not just whether Ding was caught. It is what government and industry learned, and what changed. Security must address privileged access, conduct, undisclosed affiliations, anomalous activity, and risk, while protecting civil liberties and openness.
- **Adversarial Distillation.** In April, the White House said it had information that foreign entities, principally in China, were conducting deliberate industrial-scale campaigns to distill U.S. frontier systems using tens of thousands of proxy accounts. With enough access to high-value outputs, an

adversary may reproduce strategically significant capabilities without ever stealing model weights. Counter-distillation therefore requires stronger identity controls, monitoring and rate limits, detection of coordinated activity through resellers and third-party routers, rapid revocation, intelligence sharing, and consequences for state-backed circumvention.

Fourteen years ago already, NSA Director Keith Alexander called China's cyber-enabled theft of U.S. intellectual property "the greatest transfer of wealth in history." We should not allow that failure to recur at AI scale. The value at risk now includes not merely individual trade secrets, but the returns on hundreds of billions of dollars of American investment and potentially decisive strategic capabilities. As one astute commentator recently put it, Chinese distillation threatens to bankrupt the U.S. economy.

There is also enormous opportunity here, to be sure. The same frontier models we need to protect are themselves instruments of national defense. AI can help defenders find vulnerabilities and harden the grid, hospitals, water systems, communications networks, and the labs themselves before advanced offensive capabilities diffuse more broadly.

So protect the labs—and put their capabilities to work protecting the country.

5. PROTECTING AMERICA'S AI COMPUTE ADVANTAGE

The next ecosystem is advanced compute and the semiconductor supply chain. This may be the most important technology-control advantage the United States possesses.

The U.S.-China AI competition will turn on talent, capital, energy, data, and computing power—or "compute." China has formidable strengths in almost all of these areas: world-class engineers, enormous energy resources, sophisticated AI companies, and a government willing to mobilize national resources behind strategic technologies. But compute remains China's principal chokepoint.

America's leading AI chips are today roughly five times more powerful than China's best, with public company roadmaps suggesting the gap could widen dramatically over the next several years. The production disparity is even greater. Estimates from the Institute for Progress suggest that Huawei may produce only about one to two percent as much advanced AI computing capacity as the United States this year. Chinese AI companies themselves regularly acknowledge that access to advanced chips is among their greatest constraints.

That advantage is not self-executing. It exists in significant part because U.S. and allied export controls have denied China both the world's best chips and the semiconductor-manufacturing equipment required to make equivalents at scale.

Our strategy therefore should not be organized around one export license or customs transaction. It should be organized around the capability. China should not be able to buy, rent, smuggle, steal, or build its way around American technology controls.

"Buy" means controlling direct sales of the most advanced AI chips.

"Rent" means closing the remote-access loophole. If a chip cannot legally be shipped to a Chinese AI company, that company should not be able simply to rent thousands of identical chips remotely in an overseas data center.

"Smuggle" means treating diversion as the industrial-scale enforcement problem it has become. Restricted GPUs and servers can move through distributors, shell companies, freight forwarders, and transshipment hubs in Southeast Asia. Enforcement must follow those networks, not stop at the first consignee on a shipping form.

"Steal" means recognizing that TSMC, ASML, American chip companies, and other critical firms are counterintelligence targets. If Beijing cannot purchase a technology, it will seek the people, processes, designs, and manufacturing knowledge behind it.

And "build" means semiconductor-manufacturing equipment. Restricting a finished GPU accomplishes much less if China can acquire the lithography, deposition, etch, metrology, packaging, servicing, and know-how needed to manufacture its own.

This is where export control becomes counterintelligence, and counterintelligence becomes economic security. The bureaucratic label matters less than the outcome.

Compute is the lifeblood of the AI economy. China has less of it, at lower quality. We should not help Beijing erase the most consequential technological advantage we possess.

6. STARTUPS AND THE COUNTERINTELLIGENCE THRESHOLD

A final ecosystem is harder to define precisely because, by definition, much of it is not yet obviously strategic.

An extraordinary share of America's most important technological innovation now occurs outside government—in startups working on space, quantum, fusion, biotechnology, advanced materials, autonomy, robotics, energy, manufacturing, and fields whose national-security significance may not yet be apparent.

This creates a recognition problem.

In the film *Oppenheimer*, Ernest Lawrence warns Robert Oppenheimer that the government is paying attention to his political associations. Oppenheimer asks why anyone would care what he does. Lawrence replies: “Because you're not just self-important, you're actually important.”

There is a useful analogy for today's technology ecosystem. A startup can move remarkably quickly from unimportant to promising to actually important. A prototype suddenly works. A new material becomes essential to missile production. A fusion company achieves a breakthrough. A quantum device crosses a meaningful capability threshold. A space startup becomes central to military communications. Suddenly, a company that few national-security officials had reason to know six months earlier possesses technology that Chinese intelligence has every reason to acquire.

At that moment the company has crossed what we might call a counterintelligence threshold.

The problem is that Washington has no systematic mechanism for recognizing when that happens. Too often, we depend on a company winning a defense contract, stumbling into the right government relationship, suffering an intrusion, or discovering an insider problem before the national-security apparatus understands what is at stake.

Meanwhile, Beijing's technology-acquisition system is actively looking for precisely these companies – through cyber operations, talent recruitment, investors, research partnerships, suppliers, customers, and insiders.

The United States needs a graduated private-sector counterintelligence partnership. We should not turn every promising startup into a classified defense contractor. But when companies developing strategically significant technologies cross identifiable thresholds, government should be able to offer them better threat intelligence, designated counterintelligence contacts, voluntary security assessments, cyber assistance, insider-threat guidance, and help navigating foreign investment and partnerships. Stronger obligations can attach later where companies receive classified information, sensitive contracts, or other government access.

And the government has to make that relationship valuable. A founder facing a sophisticated intrusion or suspicious foreign approach should know whom to call – and should receive useful assistance when he does.

The organizing question is simple: How do we ensure that the United States recognizes when an American company becomes "actually important" before Beijing does?

Our counterintelligence perimeter must follow strategically important technology wherever it is created – not wait for that technology to migrate inside the traditional national-security perimeter.

7. RECOMMENDATIONS: BUILDING A TECHNOLOGY COUNTERINTELLIGENCE STRATEGY

These threats require more than a collection of defensive measures. They require a counterintelligence strategy designed for an economy in which much of America's most important national-security technology is privately owned, digitally connected, and globally distributed. I would emphasize five priorities.

a. **Build a Technology CI Mission.** The Intelligence Community should lead a formal effort – with the FBI, Commerce, Defense, Energy, Homeland Security, and others – to identify private companies and infrastructure crossing the counterintelligence threshold and understand the Chinese tactics used to target them. What has become strategically important here, and how is Beijing trying to acquire or compromise it?

b. **Protect Frontier AI.** Frontier labs require a durable government-industry security compact covering nation-state cyber threats, insider risks, model

security, and industrial-scale distillation. Government should provide classified threat intelligence, investigative and vetting support, and rapid incident coordination; labs should meet serious standards for privileged access, monitoring, third-party security, and incident response. Counterintelligence should be built into any emerging federal framework for frontier AI.

c. **Harden the Homeland Perimeter.** The Spiderweb lesson requires stronger protection of sensitive geography, while the data-center revolution requires us to treat large data centers as critical grid infrastructure. CFIUS, land-security, base-defense, counter-drone, grid, and hardware-security authorities should reflect a world in which nearby commercial property can become a drone-launch site and remotely accessible equipment inside a gigawatt data center can become a grid vulnerability.

d. **Protect the U.S. Compute Lead.** Technology controls should protect capabilities, not merely individual exports. Beijing should not be able to buy advanced chips directly, rent equivalent compute remotely, smuggle it through third countries, steal the underlying technology, distill frontier capabilities, or acquire the manufacturing equipment needed to reproduce it. Export enforcement, counterintelligence, and allied technology controls increasingly constitute one mission.

e. **Reindustrialize What Matters.** We cannot counterintelligence our way out of industrial dependence. Restrictions on Chinese drones, inverters, transformers, and other critical hardware will fail if American and allied alternatives do not exist at scale. The strategic logic behind CHIPS should extend to other indispensable national-security supply chains.

The objective is not to wall off America's technology economy. It is to make sure that the technologies making America stronger do not simultaneously create new avenues for an adversary to weaken us.

8. CONCLUSION

More than a decade into our new Cold War with China, the United States does not lack warnings. We have seen Spiderweb attacks from inside an adversary's territory, unidentified drones over our own military bases, gigawatts of data-center load move in seconds, Chinese theft of advanced AI secrets, industrial-scale model distillation, and continued efforts to evade our semiconductor controls.

Sputnik became a Sputnik moment because America responded. We have strengths and advantages. Will we mobilize to preserve them?

I will end where our adversaries begin – with America's extraordinary strengths. I don’t want my message today to be read as negative, let alone fatalistic. Our frontier AI labs lead the world and may unlock breakthroughs from military capability to drug discovery. The United States and its allies possess commanding advantages across advanced compute, semiconductor design, and the technologies required to manufacture the world's best chips. Our companies, capital markets, allies, and ability to attract extraordinary talent remain enormous strategic assets.

Counterintelligence is urgent precisely because we have so much to protect. Thank you. I look forward to your questions.