June 1, 2026

EXPERTS TAKE

"Are Research Security Policies in the U.S. Working?"

A Case Study on Research Collaborations with PRC Defense Laboratories and U.S. Federally Sponsored Research

An Interview with Jeffrey Stoff

In this Experts' Take, conducted by Mathilde Huard and Bastian Szepanski from ISDP's Stockholm Center for Research and Innovation Security (SCRIS), Jeffrey Stoff discusses the critical vulnerabilities in U.S. and European research security. Mr. Stoff, a non-resident Senior Research Fellow at ISDP, argues that current policies fail to prevent the People's Republic of China (PRC) from exploiting fundamental research to advance its military capabilities. To address this, he advocates a "paradigmatic shift," including the creation of a centralized National Research Security, Integrity, and Compliance Center (NRSICC) and a unified framework of "redlines" for allied nations.

Jeffrey Stoff is the founder and president of the Center for Research Security & Integrity, a U.S. non-profit organization dedicated to the protection of research and innovation from harmful foreign influence and interference. He previously spent over 18 years in the U.S. government as a China analyst and linguist. He advised the U.S. White House, senior Department of Defense leaders; the departments of Commerce, Energy, and State; the National Science Foundation; and the National Institute of Health. Mr. Stoff has presented at dozens of conferences and seminars for U.S. and foreign government, academic, and private sector leaders on research security and technology protection issues.

Mr. Stoff is a contributing author of China's Quest for Foreign Technology: Beyond Espionage (Routledge, 2020), coauthor of "Global Engagement: Rethinking Risk in the Research Enterprise" (Hoover Institution, 2020), coauthor of "Eyes Wide Open: Ethical Risks in Research Collaboration with China" (Hoover Institution, 2021), author of Should Democracies Draw Redlines around Research Collaboration with China? A Case Study of Germany (Center for Research Security & Integrity, 2023), and coauthor of "Transparency and Integrity Risks in China's Research Ecosystem: A Primer and Call to Action" (Center for Research Security & Integrity, 2024).

This discussion is based on his latest study, "Are Research Security Policies in the U.S. working? A Case Study on Research Collaborations with PRC Defense Laboratories and U.S. Federally Sponsored Research", co-authored with John Sava and L.J. Eads.

We are currently witnessing a seismic shift in the transatlantic relationship, with several European nations reorienting their foreign policies to include closer cooperation with China. Given your analysis of the research collaboration between U.S. federally sponsored programs and PRC defense laboratories, what is the single most critical lesson that European policymakers should take away from this? Specifically, how can they navigate this reorientation without falling into the same vulnerabilities of technology transfer and unintended military enablement that have characterized past U.S.-China engagements?

Jeffrey Stoff: China has been exploiting European S&T and innovation for decades; the EU has faced the same risks, vulnerabilities, and predations from China as the U.S. It is naïve for the EU to think it can somehow manage a closer relationship with China that is built on trust more safely. Much of the PRC party-state system, including its research ecosystem, does not adhere to the core values and norms of scientific research that the G7 countries espouse as critically important in international collaborations. China's military development has benefited tremendously from largely unrestricted (fundamental) research collaborations with European nations. The EU must create more effective, concrete, and consistent policies that specifically address knowledge and technology transfers that have hitherto gone largely unnoticed or unmitigated.

While research security policies have intensified in recent years, particularly following the measures introduced during the Trump administration, there are growing concerns regarding their actual effectiveness. In your new publication, you argue that these

frameworks have failed to close critical gaps, leaving the defense sector exposed. From your perspective, which specific branches of security and defense remain most susceptible to exploitation, and what fundamental flaws in current policy prevent them from effectively mitigating these risks?

Jeffrey Stoff: While U.S. research security policies have evolved over the past several years, there is a common misconception among allied nations that the U.S. has greatly increased restrictions on collaborations with China. That is simply not the case. The most important policy change is the implementation of National Security Presidential Memorandum 33 (NSPM-33), but that policy primarily focuses on clarifying and standardizing disclosure rules on federal grant applications and periodic reviews. The policy is mostly intended to safeguard research dollars from conflicts of commitment and interest – ensuring that recipients of federal funding are not receiving resources elsewhere to do the same research. It does not place restrictions on which entities an institution can partner with. NSPM-33 has, however, placed new restrictions on participation in foreign malign talent programs whereby selectees of certain foreign talent programs are no longer eligible to receive federal research funding. However, based on my previous experience in the U.S. government and current research, it appears that there is little monitoring for compliance and enforcement of such rules, suggesting they have had little effect to date.

As I pointed out in my latest study, only NASA and the Department of Defense (DoD) or War as it is called now have actual restrictions on funding they provide to academia. DoD restrictions are very new (late 2025 / early 2026), so it is too soon to determine the effectiveness of those policies. A key finding of my study is that the majority (over 70 percent) of funding susceptible to PRC exploitation—where PRC defense laboratories are collaborating with U.S. institutions in defense and security domains—come from the National Science Foundation (NSF). This is a key vulnerability: NSF is not equipped to address potential national security concerns related to the basic/fundamental research grants it awards to institutions, and the sheer scope and scale of NSF funding make such a task nearly impossible without a radical shift in

A key finding of my study is that the majority (over 70 percent) of funding susceptible to PRC exploitation—where PRC defense laboratories are collaborating with U.S. institutions in defense and security domains—come from the National Science Foundation (NSF). This is a key vulnerability: NSF is not equipped to address potential national security concerns related to the basic/fundamental research grants it awards to institutions, and the sheer scope and scale of NSF funding make such a task nearly impossible without a radical shift in resources and capabilities. Consequently, I believe most critical technology fields remain vulnerable to China's predations.

resources and capabilities. Consequently, I believe most critical technology fields remain vulnerable to China's predations.

While scientific communities emphasize the risk of driving away global talent, your research suggests that open collaboration has functioned as a primary conduit for advancing the PRC's military capabilities. How can the U.S. move beyond this binary talent vs. security debate to create a framework that welcomes the best minds while strictly prohibiting their technical contributions from flowing into the PRC's defense system?

Jeffrey Stoff: This debate on driving away global talent is largely polemical: academia often equates restricting *some* collaborations with PRC entities with completely cutting off access to the global supply of talent. Some go so far as to assert that no one outside of the PRC can do cutting-edge research and populate our graduate STEM programs. Is it really true that there are so few talented scientists and engineers in Europe, for example? Or perhaps that the incentives, programs, and structures to encourage greater talent mobility are insufficient? It seems incongruous that the PRC has a near monopoly on global talent while at the same time the PRC itself continues to actively seek partnerships and exchanges with advanced nations; it sends PhD students and postdocs in very large numbers abroad, precisely because so much innovation and talent reside in Europe, North America, and East Asia.

We need to shift the paradigm to focus on creating trusted ecosystems that have free exchanges of talent and mutually share any benefits that result from research efforts—where integrity, reciprocity, transparency, and a merit-based hiring system are *core requirements* for participation.

Moving beyond the criticism of the U.S. administration's framework, what does your analysis reveal about the role of academia itself? In what ways are universities and research institutions—either knowingly or unknowingly—failing to safeguard sensitive information? Furthermore, what systemic or cultural factors within the academic environment have led to these persistent vulnerabilities?

Jeffrey Stoff: I need to caveat that my observations are broad generalizations, not absolute truths as academic institutions are naturally not monolithic: Academia has had a mindset that science is a borderless endeavor and that geopolitical concerns or realities are irrelevant or transitory when it comes to conducting research. Additionally, individual scientists, for good reasons, are focused on very specific research problems and tasks; they focus on science. It is understandable why many academics do not have a nuanced understanding of specific threats, risks, or challenges associated with specific countries, especially China. This, combined with the openness of our system, provides ample opportunity for actors to exploit the lack of awareness of an adversarial nation's true intentions. And while many PRC academics may share the same values, goals, and intentions as their Western counterparts, they work in a system vastly different from ours that is anathema to academic freedom and autonomy.

However, an uncomfortable truth is that academia is not always the innocent victim of exploitation; many are active enablers and participants in the diversion of intellectual capital for the direct benefit of the PRC, where those benefits are not mutual in any meaningful way. Yes, some are unwitting, but others understand the implications of their activities or are directly tasked by PRC entities to facilitate know-how transfers that are clearly asymmetric in nature.

U.S. scientific agencies that fund research have to date largely left the responsibility of safeguarding research to the individual institutions receiving funding. That will never be a recipe for success. Even research institutions that genuinely want to protect research investment dollars lack the capabilities, subject matter expertise, and resources to do so effectively. There must be a partnership where the federal (and possibly state) government provides resources and support in much more concrete ways than the current model.

You advocate for a new, centralized federal research security and integrity center, which would be referred to as the National Research Security, Integrity, and Compliance Center (NRSICC). How do you foresee the establishment of this centralized institution, and what potential impacts could it have on the viability and functions of existing organizations?

Jeffrey Stoff: It is not clear to me (yet) how or when a NRSICC would be established; i.e., what government organ would be responsible for running it, where its funding will come from, etc. My recommendations outlined in my latest publication and in Congressional testimony I provided in 2025 are centered more on a "concept of operations"—proposed key tasks, responsibilities, and goals of the NRSICC.

A key goal of the proposed NRSICC is to assist **both** research institutions **and** federal agencies with the daunting task of safeguarding research and to address the shortcomings of the current system. Right now, each funding agency has its own policies on research security and integrity (if any), as well as its own methods for assessing risk (if done at all). Centralizing such an entity allows for a uniform standard across the government which would make life easier for both academic institutions (uniform / standardized grant applications, disclosure requirements, etc.) and federal agencies (uniform methodologies for assessing risk and monitoring for compliance). It would provide much needed resources for agencies that lack such capabilities or whose capabilities are insufficient, such as the National Institutes of Health, the National Science Foundation, NASA, and the Departments of Commerce, Agriculture, and Transportation that

Academia has had a mindset that science is a borderless endeavor and that geopolitical concerns or realities are irrelevant or transitory when it comes to conducting research. Additionally, individual scientists, for good reasons, are focused on very specific research problems and tasks; they focus on science. It is understandable why many academics do not have a nuanced understanding of specific threats, risks, or challenges associated with specific countries, especially China. This, combined with the openness of our system, provides ample opportunity for actors to exploit the lack of awareness of an adversarial nation's true intentions.

provide research funding.

Another important task of the NRSICC should mirror what some of our key allies like Canada, the UK, and the Netherlands have already put in place: serve as a central (national) point of contact where research institutions can seek assistance in assessing risks associated with ongoing or future projects, partnerships, exchanges, etc. The NRSICC can also assist institutions in ensuring compliance with federal grant rules and work to address identified deficiencies in ways that help institutions avoid civil or criminal litigation or penalties.

Given that the American scientific ecosystem has historically been characterized by openness and freedom as foundational principles, how do you assess the challenges and potential trade-offs involved in introducing more stringent research security policies and practices, and to what extent might these changes risk undermining the collaborative and transparent nature that has driven scientific progress?

Jeffrey Stoff: Another uncomfortable truth is that academic freedom is often viewed as the freedom to work with any entity on any project, without any conditions or limitations. But academic freedom should not mean freedom from responsibility, especially when federal funding is involved. I disagree with the notion that placing some restrictions undermines or limits scientific progress. Safeguarding innovation is critical to driving future progress and should not be viewed as a zero-sum endeavor, but rather as an essential component of scientific advancement.

It is equally important to understand the context and purpose of most federal research dollars: those are taxpayer-funded investments with the goals of promoting *domestic* economic development and national defense, not simply advancing the frontiers of knowledge. Recipients of federal funding are stewards of taxpayer money and should be accountable to the public, just as civil servants and politicians should. Thus, it would be irresponsible to allow the PRC to siphon off technology developed from taxpayer investments. Research security policies must prevent such exploitation, theft, diversion of investment, etc., by our adversaries.

Research security policies must also address research integrity concerns—an area I believe lacks the policy attention it deserves, both at the government level and at individual institutions. An unknown portion of scientific research is **not** based on honest or transparent practices, undermining trust, corrupting the validity of some science, and often intertwining with research security issues. For example, flows of PRC talent to foreign research institutions oftentimes are not based on merit, i.e., open opportunities or competition, but rather from malign influence activities at the individual or institutional level.

Your analysis shows that the PRC specifically targets Fundamental Research—which is often exempt from security controls—as a primary way to harvest dual-use technology. Should the U.S. move away from the fundamental research exception in specific fields like AI or quantum?

Jeffrey Stoff: Yes, but I do not think it is necessary to list specific technology fields. Research security policies and controls should be harmonized with our export control and sanctions regimes, where restrictions are based on the risks and threats posed by specific entities similar to end-user control in export control realms. The U.S. government already maintains lists of foreign entities that pose serious national security, ethical (and sometimes economic security) risks. Yet research institutions

can freely take taxpayer funding and collaborate on fundamental research with those same organizations, even ones sanctioned by the U.S. Treasury Department or those that have a presumption of denial on any export license. This bifurcation makes no sense, especially as technology development accelerates and timelines from the inception of a research project to a deployed technology or capability shrink.

The CRSI report identifies structural irresponsibility where institutions failed to flag ties to PRC military organs. Is this a lack of technical capability for due diligence, or is there a cultural resistance within academia to acting as an extension of national security vetting?

Jeffrey Stoff: First, it is important to understand (and again I am speaking in generalities) that U.S. academia takes strictly legalistic approaches. In other words, policies and decisions on research partnerships/collaborations are often based solely on whether such activity is legal, not whether it is in the best interests of the U.S. And given my previous comment that there are so few restrictions on collaborations, there is little incentive for institutions to set policies or restrictions that do not violate U.S. law or federal grant terms or conditions.

On the other hand, current policies place the burden of performing risk assessments almost entirely on individual universities. Universities' missions are to educate and conduct research – it is unreasonable and unrealistic for *every* institution to fully understand current geopolitical and strategic issues; have a nuanced understanding of the PRC's technology dominance strategies, security structures, party-state influence apparatus, etc. I have argued in my publications and testimony to the U.S. Congress and the Canadian Parliament that *even the U.S. government* lacks the resources, priorities, and subject matter expertise to effectively conduct robust due diligence, threat and risk assessments, and risk mitigation efforts. If the government is unable to do this effectively, how can institutions possibly be equipped to handle this? Anecdotally, my experience is that there are not that many people in the U.S. that have the level of in-depth expertise required, and the vast majority of those individuals have left the U.S. government.

Your report recommends a common framework for all liberal democracies

Research security policies must also address research integrity concerns—an area I believe lacks the policy attention it deserves, both at the government level and at individual institutions. An unknown portion of scientific research is not based on honest or transparent practices, undermining trust, corrupting the validity of some science, and often intertwining with research security issues. For example, flows of PRC talent to foreign research institutions oftentimes are not based on merit, i.e., open opportunities or competition, but rather from malign influence activities at the individual or institutional level.

regarding research security. What specific red lines should European and U.S. partners agree upon to ensure that a researcher banned in the U.S. for security reasons cannot simply restart the same high-risk collaboration at a German or French university?

Jeffrey Stoff: Some countries like Canada, the Netherlands, and Denmark have already implemented internal policies that have drawn consistent redlines, notably restrictions on research collaborations with PRC military organs (associated with the PLA and its oversight entity the Central Military Commission) and the Seven Sons of National Defense universities. This is a good place to start, and all allied nations should set this same standard. While some exceptions could be made, there should be general redlines that restrict collaborations with PRC entities that are part of or primarily or extensively support the military and China's defense industry. Given that the U.S. still does not have such a policy in place, there is more work to be done.

A common framework requires a common (and robust) understanding of the risks and challenges. I continue to call for paradigmatic shifts in how we can address the shortcomings and knowledge gaps, and a key element is to build consortia of organizations in the public and private sectors, including government and non-government organizations, to collaborate so that different capabilities and knowledge are pooled together to form common standards for assessing risk and align research security policies. The NRSICC is one piece of this; my non-profit organization is another example. ISDP is a third. This must entail a coalition of allies and key partners, as no single country can or should take this by itself.

Conclusion

Jeffrey Stoff's observations are grounded in extensive research conducted through his non-profit organization, as well as his prior experience within the U.S. government, where he supported agencies responsible for funding and safeguarding U.S. research and innovation.

His analyses have highlighted current systemic issues in research security: Mr. Stoff pointed out that the U.S. government currently lacks the resources, priorities, and specialized expertise needed to conduct thorough due diligence, threat assessments, and risk mitigation measures. He advocates for a unified framework that fosters a common understanding of risks and challenges, calling for paradigmatic shifts in research security. The goal is not to do without talent that may exist abroad, but rather to create and strengthen protective mechanisms. This includes establishing consortia that bring together the public and private sectors, as well as governmental and non-governmental organizations, to pool capabilities and establish common standards for risk assessment and the harmonization of research security policies.

Mr. Stoff also noted that the EU faces similar risks, vulnerabilities, and predatory practices from China, particularly regarding knowledge and technology transfers, which have historically gone unnoticed or unaddressed. He emphasizes the urgent need for the EU to develop more effective, concrete, and coherent policies to mitigate these threats.