RAND

EXPERT INSIGHTS
Perspective on a Timely Policy Issue

March 2026

Research Security in **Science and Technology**

CHRISTOPHER G. PERNIN, CORTNEY WEINBAUM, FIONA QUIMBRE, SHANSHAN MEI, SHAY HERSHKOVITZ, LIBBY WEAVER, CATHERINE KISH

Introduction

Collaboration, including international collaboration, is a cornerstone of modern scientific research. International scientific collaborations are more frequent now than in the past, and growing evidence of cases of problematic activities has led to increasing scrutiny of how collaborations can be misused. This paper describes early indicators or warning signs that a collaboration might have risks that warrant mitigation to help readers identify when research security may be jeopardized.

This paper also describes a framework, structured around three pillars, to aid researchers, research institutions, and research funders in identifying, assessing, and managing risks associated with global scientific collaborations. This framework can be applied to research collaborations within the same country (when all researchers work under the same legal structure and societal expectations), though it is particularly useful when collaborators are in different countries (and do not necessarily work under the same legal structure and societal expectations). The framework can support reciprocity in scientific research so that researchers and institutions in different countries can share in the process and results of scientific research, particularly when economic inequalities and other elements of power and influence may be unevenly distributed across the research collaboration. The framework provides a list of indicators for researchers and research institutions to consider when assessing the risk of a new or ongoing collaboration. Research institutions can include this framework in their research security processes as a tool or checklist.

What Is Research Security?

Research security is a collection of efforts, processes, and tools that goes by different names depending on the country, reflecting different national agendas and ministerial responsibilities. In the United Kingdom (UK), it is more commonly known as *trusted research*; in the Netherlands, *knowledge security*; and in Sweden, *responsible internationalization* (see Table 1).

Despite the use of different terms, the underlying goal remains largely the same: to protect the inputs, processes, and outputs of research from being misappropriated and misused by others, whether at home or abroad, while upholding and bolstering the open and collaborative nature of science.

In practice, research security means implementing a set of safeguards to protect critical knowledge, data, equipment, and technologies generated from the work of researchers from often legal but unauthorized exploitation or illegitimate transfer to other parties. These safeguards might include cybersecurity measures, disclosure forms, due-diligence and risk assessment processes, visa screenings, export controls, and restrictions on physical access to sensitive research facilities, particularly for science that is not as protected as intellectual property (IP).

Striking the right balance is crucial, as working with untrustworthy partners can jeopardize a country, institution, or individual's economic and security interests. Research partners who have been unwittingly compromised, such

as by allowing another research partner into their data networks, create invisible vulnerabilities. Avoiding valuable collaborations entirely can be equally damaging; therefore, this paper provides guidance on how to collaborate safely.

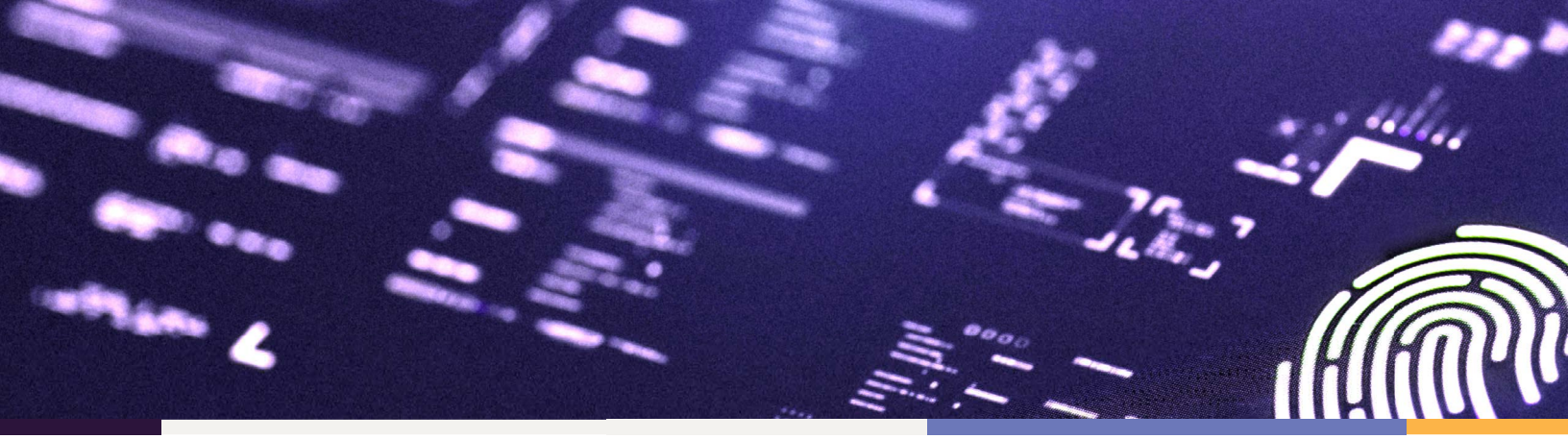
Table 1 | Research Security–Related Terms

Country or Organization	Definition
Australia Countering foreign interference in the Australian university sector	"Foreign interference occurs when activities are carried out by, or on behalf of a foreign actor, which are coercive, clandestine, deceptive or corrupting and are contrary to Australia's sovereignty, values and national interests."[a]
France Protection du potentiel scientifique et technique de la nation [protection of the nation's scientific and technological potential]	Protecting the nation's scientific and technological potential means "protecting the most 'sensitive' knowledge, expertise, and technologies produced by public and private institutions (research laboratories, companies, etc.) located on the national territory. The misappropriation or acquisition of which could: 1) harm the economic and scientific interests of the nation; 2) strengthen foreign military capabilities or weaken French defense capabilities; 3) contribute to the proliferation of weapons of mass destruction and their means of delivery; 4) be used for terrorist purposes on national territory or abroad."[b]
G7 Research security	"Research security involves the actions that protect our research communities from actors and behaviours that pose economic, strategic, and/or national and international security risks. Particularly relevant are the risks of undue influence, interference, or misappropriation of research; the outright theft of ideas, research outcomes, and intellectual property by states, militaries, and their proxies, as well as by non-state actors and organized criminal activity; and other activities and behaviours that have adverse economic, strategic, and/or national security implications."[c]
Germany Research security	"Research security refers to measures that protect our research community from actors and behaviors that pose an economic, strategic, and/or national and international security risk."[d]
Japan Research security	"Research freedom, transparency, and openness are essential for the pursuit of knowledge and the development of society, and this is the virtue of research. Still, there are concerns that the improper use of an open research system may damage the integrity and fairness of the research system, increase the risks of misuse of research outcomes, and lead to technological leakages. The importance of openness of research does not change, but it is necessary to protect academia from such improper movements. Though there must be no discrimination based on race or nationality."[e]
Netherlands Kennisveiligheid [Knowledge security]	"Knowledge security refers primarily to preventing the undesirable transfer of sensitive knowledge and technology with negative implications for our national security and ability to innovate. It also involves covert activities aimed at influence and interference activities on the part of state actors within the context of higher education and science. Such foreign interference can lead to forms of censorship (including self-censorship), thereby resulting in the impairment of academic freedom. Finally, knowledge security concerns ethical issues relating to collaboration with individuals and institutions from countries in which fundamental rights are not respected."[f]

Table 1.—Continued

Country or Organization	Definition
OECD (Organisation for Economic Co-operation and Development) Research security	"In a globalised research ecosystem, ensuring research security means preventing undesirable foreign state or non-state interference with research. The main goal of research security is to protect the research ecosystem and thus protect legitimate national and economic interests."[g]
 **Republic of Korea** National core technology	"The term 'national core technology' refers to technologies designated under Article 9 that may have a significant adverse effect on national security and the development of the national economy if divulged abroad, due to their high technological and economic value in domestic and foreign markets or the high growth potential of related industries."[h]
 **Sweden** Responsible internationalization	"Being responsible involves the consideration of ethical, legal, financial and security aspects. Frequently different goals, such as quality, transparency and security, must be balanced. Making these trade-offs requires extensive knowledge of the international landscape, beyond the area of cooperation itself."[i]
 **United Kingdom** Trusted research	"'Trusted research' is a research and innovation sector term for protecting the UK's intellectual property, sensitive research, people and infrastructure from potential theft, manipulation and exploitation, including as a result of interference by hostile actors."[j]
 **United States** Research security	Research security refers to "[s]afeguarding the research enterprise against the misappropriation of research and development to the detriment of national or economic security, related violations of research integrity, and foreign government interference."[k]

[a] Australian Government, *Guidelines to Counter Foreign Interference in the Australian University Sector*, p. 5.
[b] Secrétariat Général de la Défense et de la Sécurité Nationale [General Secretariat for Defense and National Security], French Government, "Protéger le potentiel scientifique et technique de la nation."
[c] G7 Working Group on the Security and Integrity of the Global Research Ecosystem, G7 *Common Values and Principles on Research Security and Research Integrity*, p. 2.
[d] Federal Ministry of Research, Technology, and Space, German Government, "Research Security."
[e] Japan Science and Technology Agency, "Efforts to Ensure Research Security to Protect Freedom of Research."
[f] Loket Kennisveiligheid [Knowledge Security Desk], Dutch Government, *National Knowledge Security Guidelines*.
[g] Organisation for Economic Co-operation and Development, *Integrity and Security in the Global Research Ecosystem*, p. 19.
[h] South Korean Ministry of Trade, Industry, and Energy (Technology Security Division) [산업통상자원부[기술안보과], Act on Prevention of Divulgence and Protection of Industrial Technology (Abbreviated: Act on Protection of Industrial Technology) [산업기술의 유출방지 및 보호에 관한 법률 (약칭: 산업기술보호법)].
[i] Swedish Foundation for International Cooperation in Research and Higher Education, "Responsible Internationalisation."
[j] UK Research and Innovation, "Trusted Research and Innovation."
[k] Subcommittee on Research Security, Joint Committee on the Research Environment, *Guidance for Implementing National Security Presidential Memorandum* 33 (NSPM-33) *on National Security Strategy for United States Government–Supported Research and Development*, p. 24.



Research security is not a new area of interest. It builds on established practices, such as research integrity guidelines, export controls, classified research protocols,[1] and counterintelligence and anti-espionage efforts, to name a few. The specific term *research security* gained traction in the United States in the 2010s, as China's science and technology capabilities grew relative to those of the United States. Although the Chinese government has long pursued efforts to acquire foreign scientific knowledge and technologies, U.S. concerns and responses only intensified as the technological gap between the two nations began to close and Chinese state-driven technology transfer efforts directly threatened the United States' competitive edge.

But research collaborations can have risks from around the world, not only from China, and research security is being formulated to help address those risks. Among European Union (EU) member states, priorities vary in terms of specific countries on which they focus: Some countries are primarily concerned with Russia,[2] others with China, and still others with the United States, Iran, Turkey, or Saudi Arabia.[3] More often, however, countries prefer to adopt a country-agnostic approach—meaning that they avoid singling out specific nations or specific incidents for violations of research security—and instead refer broadly to "countries of concern," "foreign actors," and recurring activities or behaviors.

How Can Research at Risk of Undue Influence Be Identified?

International research partnerships—especially in fields in which countries and companies are competing for new advancements, such as quantum computing, artificial intelligence (AI), and aerospace—bring both benefits and security challenges. Assessing the net costs and benefits may prove to be difficult without a fuller understanding of the various ways in which those collaborations benefit all sides, as well as the broader research community. For the purposes of this discussion, we use three fundamental "pillars" of research security to help unpack problematic activities and categorize incidents and activities.

The pillars below are drawn from sources listed at the end of this document (universities, government agencies, and research organizations) and provide a framework for understanding, discussing, and mitigating risks in international collaborations. The global frameworks we examined consisted of Canada's Tri-Agency Framework and Safeguarding Your Research portal;[4] the UK Research and Innovation trusted research and innovation principles;[5] frameworks from the Organisation for Economic Co-operation and Development and the League of European Research Universities;[6] Canada's National Security Guidelines for Research Partnerships;[7] the Five Eyes Secure Innovation Initiative;[8] Australia's University Foreign Interference Taskforce guidelines;[9] the EU's 2022 toolkit;[10] and Japan's JST-TRUST.[11]

These pillars are universally applicable, no matter which country is involved in the collaboration. Researchers and their institutions can use these pillars when assessing the risks of collaborations.

PILLAR 1

Protection of Data, Knowledge, Results, and Products of Research

Do you control who gets access to prepublication data, findings, and discoveries? Do you know who is using prepublication research and products?

The first pillar focuses on safeguarding the products of research—the ideas, data, prototypes, and other items that result from the research—from theft, manipulation, or unauthorized use. Research security entails protecting proprietary knowledge, technologies, and materials so that they are not misappropriated to the detriment of the researcher's work and reputation or of economic or national security. This pillar accounts for the fact that cutting-edge research (e.g., in AI and quantum) is often targeted by actors seeking illicit advantage.

One key concern is the potential for theft or illicit transfer of data, technology, equipment, or know-how. In research collaborations, a problematic partner is one who siphons off confidential data or duplicates research materials without permission.

China's legal and regulatory framework creates a challenging environment for the protection of results and products of research. Chinese national security–related laws stipulate that Chinese nationals and entities must comply with the state, even when operating abroad or in collaboration with foreign partners. For example, the 2017 National Intelligence Law requires Chinese organizations and individuals to "support, assist, and cooperate with state intelligence work," effectively mandating compliance with government demands, including the transfer of sensitive data or research outcomes.[12] Similarly, the 2023 Counter-Espionage Law and the 2017 Cybersecurity Law grant the Chinese government broad authority to access data and IP, even from private companies and academic institutions, under the pretext of national security.[13]

> "Research security entails protecting proprietary knowledge, technologies, and materials so that they are not misappropriated to the detriment of the researcher's work and reputation or of economic or national security."

These laws create significant risks for foreign researchers collaborating with Chinese institutions. For instance, joint projects may result in IP being appropriated by the Chinese state without proper acknowledgment or compensation. This regulatory framework undermines trust in research collaborations and raises concerns about the misuse of scientific discoveries for strategic or military purposes.

The following box shows several additional tactics that undermine this pillar.

Tactics Undermining the Protection of Results and Products of Research

- Unpublished data are copied or exported without permission.
- Findings are transferred to third-party actors abroad prior to publication, and peer review or institutional oversight is bypassed.
- Covert parallel research takes place in a partner institution using jointly developed data with no acknowledgment or IP sharing.
- Collaborators, institutions, or governments gain unauthorized remote access to research systems or cloud-based datasets.
- Prototypes shared in good faith during collaboration are reverse engineered for national gain or competitive use.
- Coauthorship or credit is required as a condition for collaboration, despite minimal or nontransparent contributions by coauthors.
- Key methods or data are withheld by a stronger collaborator to create dependence while extracting knowledge.
- A stronger collaborator uses coercive tactics to manipulate junior collaborators into agreeing to undesirable terms.
- Data hosting on foreign servers is mandated, increasing the risk of state access, manipulation, or surveillance.
- Prior agreements are circumvented through publishing or patenting abroad before joint ownership is finalized.
- Joint research outputs are used for unapproved dual-use applications (e.g., surveillance technology is derived from AI-related health tools).

PILLAR 2

Transparency and Disclosure

Are your research partners who they claim to be? Are they working on what they should—and for whom they say they do? Transparency within the research collaboration—between and among research partners—is the second pillar of research security. Transparency reveals potential export control breaches and conflicts of interest or commitment and mitigates the opportunity for hidden agendas. When partners provide false information or fail to fully disclose information to each other, such actions raise serious questions about motives.

Research security often begins to falter when transparency is compromised. At this point, research institutions, funders, and individuals must step in to monitor and address the risks.

One warning sign that this pillar has been compromised is failure to disclose foreign sources of funding. Such nondisclosure violates this pillar and can lead to serious consequences, including the jeopardization of other sources of funding or even legal action. For researchers collaborating with the U.S. government, failing to abide by disclosure rules or lying on grant applications, and then later being found out, could result in their research grants being terminated, for example.

A subtle warning sign—often only clear after the fact—is when a collaborator misrepresents the intended end use of the work. The mismatch may emerge only once the research is complete or after due diligence uncovers undisclosed affiliations or funding. An example might be participating in a research project under the pretense of conducting benign civilian research but secretly intending to use the results for military, illicit, or undesirable purposes. One documented example is the proposed Imperial College London Data Science Institute (DSI) partnership with China's Jiangsu Automation Research Institute (JARI) (the "Future Digital Ocean Innovation Centre"). Imperial described the planned work as civilian-focused (i.e., involving ocean modeling and forecasting, logistics, and data tools), but a November 2018 Chinese-language email from JARI's head of research stated that JARI wanted DSI's help developing data-visualization tools, including for military purposes, explicitly referencing "smart military base(s)"—a purpose that was not translated into English in the email chains provided through a freedom of information request.[14]

"Research security often begins to falter when transparency is compromised. At this point, research institutions, funders, and individuals must step in to monitor and address the risks."

Ensuring robust disclosure from all collaborators is vital so that partners know with whom they are working. Recent evidence reveals collaborations between Western researchers and Chinese AI labs on technologies for urban applications, including traffic management and environmental monitoring. A December 2025 investigation found that leading universities, including the Massachusetts Institute of Technology, Stanford, and Oxford, collaborated with two Chinese state-backed AI laboratories—the Shanghai Artificial Intelligence Research Institute and Zhejiang Lab—that have deep ties to China's surveillance apparatus and Ministry of Public Security.[15] These collaborations, which received U.S. and UK government funding, developed technologies that included gait recognition, multi-object tracking, and facial recognition systems. While many of these technologies have legitimate civilian applications,[16] the same Chinese partner institutions have deployed similar technologies for mass surveillance, including in Xinjiang, where members of the ethnic Uyghur Muslim minority have been subject to large-scale detention and imprisonment policies. The extent to which Western researchers were aware of their collaborators' connections to surveillance operations or adequately disclosed these relationships to their institutions and funders remains unclear and represents a potential failure of due diligence and transparency in international research partnerships.

The following box shows several other tactics that undermine transparency and disclosure in research. Researchers and institutions should watch for these signs to identify when their work might be targeted for foreign exploitation or misuse.

Tactics Undermining Transparency and Disclosure

- Researchers or institutions provide or have a historical track record of providing incomplete or inconsistent disclosure of affiliations, including those of research collaborators, funding sources, obligations, and other relevant relationships.
- Researchers refuse to provide information about end users or end use, or researchers use delay tactics to avoid answering questions.
- Researchers use historical institutional names, acronyms, or aliases that omit defense ties to evade due-diligence and compliance efforts.
- Public-facing materials (such as websites, publications, and curricula vitae [CVs]) contain inconsistent affiliations or omit known partnerships, making it difficult to verify a collaborator's true institutional alignment or obligations.
- A collaborator is asked to sign a secrecy agreement or a nondisclosure agreement before affiliations, roles, research goals, and funding sources are revealed. Although this may appear to be an IP protection measure, it can sometimes be used to conceal the true nature or intent of the research.
- There are discrepancies between public-facing and internal representations (e.g., multiple versions of websites), including discrepancies between native-language information and given information.
- Overly scripted or evasive messaging about research goals, particularly when all collaborators repeat identical talking points or avoid discussing potential applications.
- A collaborator's CV indicates either overqualifications or underqualifications for the project, or their skills do not align with their stated qualifications.
- A third party finances the research to avoid end-user identification.
- Requests are made to bypass or avoid institutional compliance, ethics, or export control reviews.
- A partner's website is purposely not accessible in your jurisdiction, complicating due-diligence efforts.

PILLAR 3

Governance

Are you aware of the applicable governance regulations, structures, processes, and policies? Are you aware of the laws, norms, and requirements of your partners' host countries? The third pillar involves the establishment of and adherence to laws, policies, management structures, and norms that govern research and international collaboration in research. Collaborations that bypass safeguards, centralize control with one research partner, or operate under vague or shifting terms may create exploitative dynamics, restrict scientific reciprocity, undermine academic standards, and compromise academic freedom. This pillar includes complying with export control regulations, following security protocols for sensitive technologies, and establishing clear governance for collaborating.

High-tech research that is protected under export control laws cannot be shared with foreign entities without authorization. Accordingly, export control governance and compliance are listed as main focuses of research security programs.

Beyond legal compliance, this pillar includes the establishment and socialization of formal oversight structures (e.g., review committees, due-diligence processes) to ensure that collaborations are conducted on equitable and secure terms. Some universities have created dedicated review committees to vet high-risk international projects, evaluating such factors as the backgrounds of research partners, potential dual use of research, and other potential red flags. These bodies provide guidance to researchers on maintaining security and integrity in their research collaborations and allow that expectation to be shared among collaborators.

One risk to securing research is the circumvention of export controls or regulations. A collaboration might involve access to sensitive information (say, satellite capability information or AI algorithms), and, without shared governance structures or with unclear expectations on either side, that information can find its way to team members who are not authorized to receive

> "Collaborations that bypass safeguards, centralize control with one research partner, or operate under vague or shifting terms may create exploitative dynamics, restrict scientific reciprocity, undermine academic standards, and compromise academic freedom."

it. Such transfers can occur either intentionally or because of insufficient oversight. Strong research security puts in place rules and processes for clear and shared protocols and expectations for information, knowledge, and technology transfer that are enforceable through known mechanisms. For example, this may include export-control compliance processes, institutional conflict of interest and disclosure systems, and formal cybersecurity controls. Each may have clear ramifications if not followed and help codify the overall intent of the focus on research security.

Another issue could be a lack of governance or enforceable agreements, which can enable unethical partners to dominate or exploit collaborative relationships. Power imbalances and language barriers may undermine trust and academic freedom, causing junior collaborators to share science with stronger partners without reciprocity. This is why some organizations stress that global engagements must be "reciprocal, transparent and aligned with research terms and conditions, which promote broad dissemination of information."[17] Proper governance can help enforce reciprocity and transparency and reduce the risk of undisclosed objectives. By setting clear collaboration terms (e.g., disclosure of funding and affiliations, publication and data-sharing rules, export-control and dual-use screening), providing role-based compliance training, and applying proportionate oversight (e.g., review checkpoints and auditability), research organizations can better ensure that collaborative projects follow both legal requirements and institutional expectations for fair collaboration.[18]

The following box highlights several tactics of concern that undermine standards of governance.

Problematic Tactics in Governance

- Partnerships between institutions of unequal size and influence or partnerships across international borders lack formal ethics, legal, or IP review processes; or, in these partnerships, there is pressure to relocate oversight to jurisdictions with weaker standards that benefit one party over another.
- There are restrictions that allow one partner exclusive or disproportionate access to shared data, access to research facilities, or control over publication rights.
- There are vague or frequently changing partnership terms that lack formal documentation or mutual review.
- There is a lack of documented policies governing international collaboration, such as procedures for partner due diligence, disclosure requirements for foreign affiliations and funding, or protocols for data-sharing and IP management.
- There is no designated point of contact for research security or compliance oversight.
- There is a lack of shared standards or transparency around data provenance, audit logging, platform security, or compliance with export control and privacy regulations.
- Requests are made to adopt weak or asymmetrical data protection practices that grant one party disproportionate access to data and information systems. These requests could include the use of unverified information platforms or informal methods for data transfer.
- There is a lack of signed data-handling agreements, and/or there is reliance on verbal agreements in lieu of written agreements.
- There is a lack of awareness of or disregard for applicable export controls, data protection laws, data privacy laws, and other national rules for handling data collected from human subjects.

Summary

Research security is critical in enabling scientific progress and international collaboration while mitigating risks to national security, economic competitiveness, and standards. Effective research security practices recognize the growing interconnectedness of global research along with the heightened vulnerabilities of such research, especially in high-tech fields, such as AI, quantum computing, biotechnology, and aerospace. State actors can exploit open academic systems, leverage dual-use technologies, siphon off IP through nondisclosure agreements that are unknown to researchers' employers, or employ covert tactics. Failing to address these risks may result in stolen innovations, compromised data, and unethical research applications and may degrade national security. Institutions and nations must establish robust governance mechanisms to prevent exploitation while maintaining the openness essential to scientific advancement.

The framework we present in this paper provides a list of indicators that researchers and research institutions can consider when assessing the risk of a new or ongoing collaboration. Research institutions can include this framework in their research security processes as a tool or checklist. If any indicators from this framework appear in research collaborations, the collaborators and their institutions should consider the context for the risk and whether the risk should be mitigated.

At the core of safeguarding research security is the challenge of balancing transparency and collaboration with the protection of intellectual assets. Without proper safeguards—such as export controls, cybersecurity protocols, disclosure requirements, and due-diligence mechanisms—international partnerships may serve as avenues for espionage, economic exploitation, or unethical applications of research. As demonstrated by the examples in this paper, the stakes are not limited to hypothetical risks but extend to real consequences for economic development, scientific credibility, and global power. Research security is therefore more than just an administrative or procedural concern; it is a cornerstone of sustaining trust, equity, and safety within the global research enterprise. Research security offers a preventative strategy to manage risk before detrimental effects occur. The challenge is to do so without compromising the collaborative ethos that drives scientific discovery and while minimizing extra burdens on researchers.

Notes

[1] Examples include specific post–World War II systems, such as International Traffic in Arms Regulations and other export control regulations.

[2] European Commission, "Statement on the Need to Protect EU Research and Innovation from Foreign Interference."

[3] Gattolin, *Notice Rapport*.

[4] Government of Canada, *Tri-Agency Framework*; Government of Canada, "Safeguarding Your Research."

[5] UK Research and Innovation, "Trusted Research and Innovation."

[6] Overlaet, *A Pathway Towards Multidimensional Academic Careers*.

[7] Government of Canada, *National Security Guidelines for Research Partnerships*.

[8] Office of the Director of National Intelligence, "Secure Innovation."

[9] Australian Government, *Guidelines to Counter Foreign Interference in the Australian University Sector*.

[10] Directorate-General for Research and Innovation, European Commission, *Tackling R&I Foreign Interference*.

[11] Japan Science and Technology Agency, "Efforts to Ensure Research Security to Protect Freedom of Research."

[12] National People's Congress of the People's Republic of China, National Intelligence Law of the People's Republic of China.

[13] In a companion paper to this one, our colleagues explain these laws and their implications for research with Chinese researchers and research institutions; see Mei and Huismans, *China's Science and Technology Strategy in Perspective*. For a translation of the Counter-Espionage Law, see China Law Translate, "Counter-Espionage Law of the P.R.C. (2023 ed.)." For a description of the 2017 Cybersecurity Law and 2025 amendments, see National People's Congress of the People's Republic of China, Cybersecurity Law of the People's Republic of China; and Nie and Zhang, "China."

[14] For UK-China Transparency reporting on this incident, see Huang, Guo, and Imperial College London's Data Science Institute, "Imperial College London & the Chinese Military." For subsequent reporting on this incident, see Devlin, "Chinese Firm Sought to Use UK University Links to Access AI for Possible Military Use."

[15] For example, see Strategy Risks, "Global AI Research Partnerships and China's Rights Abuses."

[16] IEEE Digital Privacy, "Are Smart Cities a Threat to Personal Privacy?"

[17] As an example, see Ohio State University, "International Research Engagements."

[18] For example, both U.S. and UK guidance focus on clear institutional policy for transparency and disclosure, oversight, and compliance. See Subcommittee on Research Security, Joint Committee on the Research Environment, *Guidance for Implementing National Security Presidential Memorandum 33 (NSPM-33) on National Security Strategy for United States Government–Supported Research and Development*; and UK Research and Innovation, "Trusted Research and Innovation."

Bibliography

The entries in this section are organized by category in order to distinguish laws and governance from commentary, reports and studies, and other resources.

News, Commentary, and Challenges

"China Exploits US-Funded Research to Advance Its Military Technology: Report," *Colombo Gazette*, October 10, 2024.

Christou, Andrea, and Chad Damro, "Research Security and the European Union," *EU-RENEW* blog, June 13, 2025.

Devlin, Hannah, "Chinese Firm Sought to Use UK University Links to Access AI for Possible Military Use," *The Guardian*, June 16, 2024.

Saballa, Joe, "Russian Military Suppliers Exploit Loophole in US Microchip Embargo," *Defense Post*, December 10, 2024.

Shih, Tommy, "Challenges to Research Security," SSRN, 2025.

Talley, Ian, and Brett Forrest, "Russia Doubled Imports of an Explosives Ingredient—With Western Help," *Wall Street Journal*, March 29, 2024.

Tsvetkova, Maria, Polina Nikolskaya, Anton Zverev, and Ryan McNeill, "Russia Building Major New Explosives Facility as Ukraine War Drags On," Reuters, last updated May 9, 2025.

Wang, Yaqiu, "Can the U.S. Find a Balance Between Scientific Openness and Security?" *ChinaFile*, January 22, 2025.

Frameworks and Guidelines

Australian Government, "Resources," webpage, undated. As of March 20, 2026: https://www.education.gov.au/resources/countering-foreign-interference-australian-university-sector

Australian Government, *Guidelines to Counter Foreign Interference in the Australian University Sector*, 2021.

Bitzinger, Richard A., Yoram Evron, and Zi Yang, "Roundtable: China's Military-Civil Fusion Strategy: Development, Procurement, and Secrecy," *Asia Policy*, Vol. 16, No. 1, January 2021.

Directorate-General for Research and Innovation, European Commission, *Tackling R&I Foreign Interference: Staff Working Document*, Publications Office of the European Union, 2022.

European Commission, "Statement on the Need to Protect EU Research and Innovation from Foreign Interference," press release, May 18, 2022.

G7 Working Group on the Security and Integrity of the Global Research Ecosystem, *G7 Common Values and Principles on Research Security and Research Integrity*, June 2022.

Gattolin, André, *Notice Rapport: Protéger le potentiel scientifique et technique de la France,* Sénat Français [French Senate], No. 873, 2021. As of August 13, 2025: https://www.senat.fr/notice-rapport/2020/r20-873-notice.html

Government of Canada, *Tri-Agency Framework: Responsible Conduct of Research*, 2021.

Government of Canada, "Safeguarding Your Research," webpage, last modified October 6, 2022. As of June 18, 2025:
https://science.gc.ca/site/science/en/safeguarding-your-research

Government of Canada, *National Security Guidelines for Research Partnerships*, 2023.

Japan Science and Technology Agency, "Efforts to Ensure Research Security to Protect Freedom of Research: Appropriate Balance Between Openness and Security for Scientific Research," webpage, undated. As of August 13, 2025:
https://www.jst.go.jp/osirase/research_security/index_e.html

Loket Kennisveiligheid [Knowledge Security Desk], Dutch Government, *National Knowledge Security Guidelines: Secure International Collaboration*, January 2022.

Organisation for Economic Co-operation and Development, *Integrity and Security in the Global Research Ecosystem*, June 2022.

Overlaet, Bert, *A Pathway Towards Multidimensional Academic Careers: A LERU Framework for the Assessment of Researchers*, League of European Research Universities, January 2022.

South Korean Ministry of Trade, Industry, and Energy (Technology Security Division) [산업통상자원부 [기술안보과], Act on Prevention of Divulgence and Protection of Industrial Technology (Abbreviated: Act on Protection of Industrial Technology) [산업기술의 유출방지 및 보호에 관한 법률 (약칭: 산업기술보호법)], trans. by Georgetown Center for Security and Emerging Technology, 2023. As of August 13, 2025:
https://cset.georgetown.edu/wp-content/uploads/t0521_industry_protection_EN.pdf

Swedish Foundation for International Cooperation in Research and Higher Education, "Responsible Internationalisation," webpage, undated. As of June 26, 2025:
https://www.stint.se/en/responsible-internationalisation/

UK Research and Innovation, "Trusted Research and Innovation," webpage, last updated April 30, 2025. As of June 18, 2025:
https://www.ukri.org/manage-your-award/good-research-resource-hub/trusted-research-and-innovation/

Institutional Resources

Chapman University, "Research Security," webpage, undated. As of June 18, 2025:
https://www.chapman.edu/research/integrity/research-security/index.aspx

Federal Bureau of Investigation, "The China Threat," webpage, undated. As of June 26, 2025:
https://www.fbi.gov/investigate/counterintelligence/the-china-threat/chinese-talent-plans

Federal Ministry of Research, Technology, and Space, German Government, "Research Security," webpage, undated. As of June 26, 2025:
https://www.bmbf.de/EN/Research/InternationalAffairs/ResearchSecurity/researchsecurity_node.html

Harvard Medical School, "Research Security," webpage, undated. As of June 18, 2025:
https://ari.hms.harvard.edu/research-compliance/research-security

National Institute of Standards and Technology, "Research Security Office," webpage, undated. As of June 18, 2025:
https://www.nist.gov/adlp/research-security-office

National Science Foundation, "Research Security at the National Science Foundation," webpage, undated. As of June 18, 2025:
https://www.nsf.gov/research-security

National Science Foundation, "The Research on Research Security Program (RoRS)," webpage, April 11, 2025. As of June 18, 2025:
https://www.nsf.gov/funding/opportunities/rors-research-research-security-program

Office of the Director of National Intelligence, "Secure Innovation," webpage, undated. As of June 18, 2025:
https://www.dni.gov/index.php/ncsc-what-we-do/secure-innovation

Ohio State University, "International Research Engagements," webpage, undated. As of June 18, 2025:
https://research.osu.edu/research-responsibilities-and-compliance/export-controls/international-research-engagements

Organisation for Economic Co-operation and Development, "International Collaboration in Science," webpage, undated. As of June 27, 2025:
https://www.oecd.org/en/topics/sub-issues/international-collaboration-in-science.html

Secrétariat Général de la Défense et de la Sécurité Nationale [General Secretariat for Defense and National Security], French Government, "Protéger le potentiel scientifique et technique de la nation," webpage, January 1, 2025. As of June 26, 2025:
https://www.sgdsn.gouv.fr/nos-missions/proteger/proteger-le-potentiel-scientifique-et-technique-de-la-nation

University of California, Santa Barbara, "Research Security," webpage, undated. As of June 18, 2025:
https://www.research.ucsb.edu/research-security

University of Maryland, Baltimore County, "Export Control Overview," webpage, undated. As of June 18, 2025:
https://research.umbc.edu/export-control-overview/

University of Michigan, "Research Safety First, Safety Everyday," webpage, undated. As of June 18, 2025:
https://research.umich.edu/research-safety/

University of Texas, "International Collaborations and Research Security," webpage, undated. As of June 18, 2025:
https://research.utexas.edu/resources/research-integrity-and-compliance/international-collaborations

U.S. Department of State, "Military-Civil Fusion and the People's Republic of China," one-pager, May 2020. As of August 13, 2025:
https://www.state.gov/wp-content/uploads/2020/05/What-is-MCF-One-Pager.pdf

Policies and Legislation

China Law Translate, "Counter-Espionage Law of the P.R.C. (2023 ed.)," webpage, April 26, 2023. As of March 2, 2026:
https://www.chinalawtranslate.com/en/counter-espionage-law-2023/#gsc.tab=0

Lander, Eric, "Guidance for U.S. Scientific Research Security That Preserves International Collaboration," White House, January 4, 2022.

National Counterintelligence and Security Center, Office of the Director of National Intelligence, "Research Security," undated. As of June 18, 2025:
https://www.dni.gov/index.php/safeguarding-science/research-security

National People's Congress of the People's Republic of China, Cybersecurity Law of the People's Republic of China, June 1, 2017.

National People's Congress of the People's Republic of China, National Intelligence Law of the People's Republic of China, June 27, 2017.

Public Law 117-167, CHIPS and Science Act, August 9, 2022.

Subcommittee on Research Security, Joint Committee on the Research Environment, *Guidance for Implementing National Security Presidential Memorandum 33 (NSPM-33) on National Security Strategy for United States Government–Supported Research and Development*, Executive Office of the President of the United States, January 2022.

U.S. Code, Title 42, The Public Health and Welfare; Chapter 163, Research and Development, Competition, and Innovation; Subchapter VI, Miscellaneous Science and Technology Provisions; Section 19232, Malign Foreign Talent Recruitment Program Prohibition.

Reports and Studies

Blevins, Emily G., *Federal Research Security Policies: Background and Issues for Congress*, Congressional Research Service, R48541, May 20, 2025.

Brown, Michael, and Pavneet Singh, *China's Technology Transfer Strategy: How Chinese Investments in Emerging Technology Enable a Strategic Competitor to Access the Crown Jewels of U.S. Innovation*, Defense Innovation Unit Experimental, January 2018.

Diamond, Larry, and Orville Schell, eds., "Technology and Research," in *China's Influence & American Interests: Promoting Constructive Vigilance*, Hoover Institution Press, 2019.

European University Association, "Enhancing Research Security in Europe: European University Association Input to the European Commission's Call for Evidence on 'Boosting Research Security in the EU,'" December 2023.

Héau, Lauriane, "The EU Research Security Initiative: Implications for the Application of Export Controls in Academia and Research Institutes," Stockholm International Peace Research Institute, March 2025. As of June 18, 2025: https://www.sipri.org/sites/default/files/2025-03/eunpdc_94.pdf

Huang Ping, Guo Yike, and Imperial College London's Data Science Institute, "Imperial College London & the Chinese Military," UK-China Transparency, June 16, 2024. As of March 2, 2026: https://ukctransparency.org/wp-content/uploads/2024/06/Imperial-College-London-the-Chinese-military.pdf

IEEE Digital Privacy, "Are Smart Cities a Threat to Personal Privacy?" webpage, undated. As of August 13, 2025: https://digitalprivacy.ieee.org/publications/topics/are-smart-cities-a-threat-to-personal-privacy/

Lauer, Michael, "Foreign Interference in National Institutes of Health Funding and Grant Making Processes: A Summary of Findings from 2016 to 2021," National Institutes of Health, July 30, 2021.

Mei, Shanshan, and Judith Huismans, *China's Science and Technology Strategy in Perspective: Historical Evolution, Political Drivers, and Global Implications*, RAND Corporation, RR-A4104-3, forthcoming.

Nie, Yuechao, and Laney Zhang, "China: Counterespionage Law Revised," Library of Congress, September 22, 2023.

Select Committee on the CCP, "How American Taxpayers and Universities Fund the CCP's Advanced Military and Technological Research: Moolenaar, Foxx Uncover That American University Research Aids Chinese Military," press release, September 23, 2024.

Strategic Partnership Unit, Federal Bureau of Investigation, "Preventing Loss of Academic Research," Counterintelligence Strategic Partnership Intelligence Note 15-006, June 2015.

Strategy Risks, "Global AI Research Partnerships and China's Rights Abuses," press release, December 8, 2025.

U.S. Department of Justice, "Information About the Department of Justice's China Initiative and a Compilation of China-Related Prosecutions Since 2018," webpage, last updated February 23, 2022. As of June 18, 2025: https://www.justice.gov/archives/nsd/information-about-department-justice-s-china-initiative-and-compilation-china-related

U.S. Government Accountability Office, *Research Security: Strengthening Interagency Collaboration Could Help Agencies Safeguard Federal Funding from Foreign Threats*, GAO-24-106227, January 2024.

U.S. Senate, *Threats to the U.S. Research Enterprise: China's Talent Recruitment Plans*, November 19, 2019.

Wagner, Caroline S., *The Collaborative Era in Science: Governing the Network*, Palgrave Macmillan, 2018.

About the Authors

Christopher G. Pernin is the vice president of the RAND Army Research Division and director of the RAND Arroyo Center. He brings over two decades of experience analyzing international technology development and security implications and has led numerous assessments of foreign research capabilities, technology transfer risks, strategic technology development, and decisionmaking processes in research organizations. Pernin serves on several North Atlantic Treaty Organization expert committees focused on emerging technology risks. He holds a Ph.D. in chemistry.

Cortney Weinbaum is a senior management scientist at RAND. She specializes in national security topics, and she brings more than two decades of experience assessing the implications of and possible uses for emerging technologies. She has examined opportunities and risks for emerging technologies in space architectures, special operations, countering weapons of mass destruction, and cybersecurity. Weinbaum holds a B.S. in physics.

Fiona Quimbre is a senior analyst at RAND Europe, where she examines the nonmilitary dimensions of competition with China, focusing on threats to Europe's economic, infrastructure, and scientific assets. Her recent research has focused on the security implications of a power grid developed and governed by China. Quimbre holds an M.A. in China studies and an M.A. in international relations.

Shanshan Mei is a political scientist at RAND. She is the author of numerous reports and research essays on the organization and culture of the People's Liberation Army (PLA) and Chinese defense modernization priorities, and her recent research has focused on U.S. competition and relations with China and the PLA's approach to manned-unmanned teaming. Mei holds a Ph.D. in international relations.

Shay Hershkovitz is an expert in strategy, national security, intelligence, climate change, and emerging technologies, with a rich professional background in the public, private, and academic sectors. He has engaged in consulting in strategic and competitive intelligence and has published work on how emerging technologies reshape intelligence communities. Hershkovitz holds a Ph.D. in political science.

Libby Weaver is a Chinese-language research assistant at RAND. She is interested in such topics as Chinese military-civil fusion, Chinese state-owned enterprises, Indo-Pacific security, Taiwan's defense, and Chinese intelligence. Weaver holds a B.A. in international law and institutions and a B.A. in East Asian languages and cultures.

Catherine Kish is a Chinese-language specialist research assistant at RAND. Her research interests include Indo-Pacific security, forced labor practices in China, U.S.-China relations, U.S.-China military competition and deterrence in the Taiwan Strait, human rights, and far-right extremism and terrorism. Kish holds a B.A. in political science and Chinese.

About This Paper

Research security is critical for ensuring scientific progress during international collaboration while mitigating risks to national security, economic competitiveness, and standards. The growing ease and interconnectedness of global research—especially in high-tech fields, such as artificial intelligence, quantum computing, biotechnology, and aerospace—has both increased the pace of discovery and heightened vulnerabilities in this space. This paper describes research security and provides a framework structured around three pillars (protection of vulnerable results and products, transparency and disclosure, and governance) to aid researchers, research institutions, and research funders in identifying, assessing, and managing risks associated with global scientific collaborations. This framework can be applied broadly to international research collaborations.

RAND National Security Research Division

This work was conducted within the International Security and Defense Policy Program of the RAND National Security Research Division, which conducts research and analysis for the Office of the Secretary of War, the U.S. Intelligence Community, the U.S. State Department, allied foreign governments, and foundations.

For more information on the RAND International Security and Defense Policy Program, see www.rand.org/nsrd/isdp or contact the director (contact information is provided on the webpage).

Funding

This effort was sponsored by the U.S. government.

Acknowledgments

We thank Sale Lilly and Jeff Stoff for providing critical inputs to early versions of this paper, and we thank Sale and Jon Schmid for providing thoughtful peer reviews.

For more information on this publication, visit www.rand.org/t/PEA4104-1.

Cover image: Adapted from images by metamorworks/Getty Images and dem10/Getty Images

PE-A4104-1

www.rand.org