Safeguarding Research Integrity and Security in the Global Academic Environment

Prepared for Sandia National Laboratories

by:

Blanca Applewhite
Josh Bruegger
Emily Carlisle
Tommy Clark
David Gifford
Bradley Kozisek
Philip Carl Nunn

Texas A&M University

Bush School of Government and Public Service

PSAA 675-700 Executive Master of Public Service and Administration Capstone

Dr. Kevin R. Gamache

April 27, 2025

Abstract

Sandia National Laboratories commissioned this Capstone research project to assist US partners in developing a research security framework, easily implemented and tailored for higher education institutions (HEIs) and research-producing organizations (RPOs) in economically developing countries. The resulting deliverables will benefit the US government, its international partners, policymakers, and research officers across various economic landscapes. This paper addresses the critical overarching research question: How can research institutions in developing countries implement a research security program that safeguards their intellectual property (IP) from malign foreign influence and enhances their country's economic and national security?

The objectives include identifying emerging technologies and research areas targeted by malign foreign actors, revealing core principles of research security adopted by developed countries, and determining the best practices for HEIs and RPOs in developing countries. This research also illustrates the benefits of implementing a robust research security program and the risks of neglecting such protocols.

The research methodology includes an extensive literature review to pinpoint critical and emerging technologies specifically vulnerable to malicious actors, leveraging established research security and integrity programs in countries such as Australia, Canada, Japan, and the US. Real-world case studies will highlight potential pitfalls and justify the recommended best practices while examining export controls and categorizing protective measures for critical research data. The Capstone research project stands to significantly contribute to protecting IP and promoting economic security for research institutions in developing countries, fostering global collaboration and resilience in research security practices.

Table of Contents

Executive Summary

Purpose

This Capstone research project, commissioned by Sandia National Laboratories, assists US partners in developing a research security framework that is easily implemented and tailored for higher education institutions (HEIs) and research-producing organizations (RPOs) in economically developing nations. The central research question guiding this study is: *How can research institutions in developing countries implement a research security program that safeguards their intellectual property (IP) from malign foreign influence and enhances national economic and security outcomes?*

The study explores three sub-questions:

1. What core principles from developed countries are most compatible with effective research security frameworks?
2. What best practices should HEIs and RPOs follow?
3. What are the benefits of implementing research security protocols and the risks associated with neglecting such protocols?

Research Methodology

The research methodology included in-residency team discussions in Washington, D.C., a thorough literature review, case study analysis, participation in the Academic Security and Counter-Exploitation seminar at Texas A&M University, and consultations with experts across academia, government, and industry. The literature review identified critical technologies vulnerable to malicious actors, leveraging established research security and integrity programs in countries such as Australia, Canada, Japan, and the US. Case studies highlight potential pitfalls and justify recommended best practices while examining export controls and protective measures

for critical research data. The analysis examines successful multilateral efforts and consortia among countries like Canada, Japan, Australia, and Brazil, which provide scalable models for developing nations. These comparative frameworks offer valuable insights into striking a balance between openness and security while maintaining research integrity.

Key Findings

The core principles of research are academic freedom and scientific openness, research integrity and ethical conduct, and compliance with national interest and export control regulations. There is ample opportunity for malign actors to access an institution's prized intellectual property, which Brown and Singh describe as "crown jewels," through non-state actors. This is because the research industry's culture values openness, international collaboration, digitalization, sharing, and international travel as norms of conduct. HEI stakeholders may not be aware of how their activities align with strategic state interests to expand their influence on the world stage, nor how they contribute to dual-use research and state-sponsored interference. As Capstone instructor, Dr. Kevin R. Gamache explained during the in-residency discussion, understanding the benefits and risks of research security and identifying which crown jewels an institution wants to protect are integral for developing a balance.

Implementing research security frameworks in developing countries presents distinct structural, financial, and political challenges. One of the most frequently cited obstacles is resource limitation. Despite these challenges, several authors recommend positive ways forward, suggesting that international frameworks should be adaptable and modular. They should also allow developing nations to build capacity without being excluded from global research

networks. Moreover, partnerships that emphasize equity and mutual benefit, rather than one-sided compliance, are more likely to foster sustainable security cultures.

Multilateral collaborations between nations, as well as the individual achievements of Australia, Brazil, Canada, the EU, and Japan, have become fundamental in constructing robust research security structures. For underdeveloped entities, consortia create alliances that pool efforts. They have dedicated themselves to proactive dialogue on export controls to develop a harmonized approach to sensitive technologies, including artificial intelligence (AI) and biotechnologies, which are considered dual-use technologies, as well as quantum computing, which has both commercial and defense applications. Securing exports is imperative to the non-proliferation of information and technology that could be used in a military capacity.

Developing countries must be made aware of the benefits they can expect from academic research programs, as well as the risks associated with failing to implement academic research security.

Benefits of Academic Research Security Programs

- Protection of Intellectual Property and Sensitive Information
- Maintenance of Academic Honesty and Trust
- Compliance with Legal and Regulatory Requirements
- Mitigation of National Security Threats
- Enhanced Competitiveness and Reputation

Risks Associated with Failure to Implement Academic Research Security

- Loss of Intellectual Property
- Reputational Damage
- Threats to National Security
- Legal and Financial Consequences
- Erosion of Academic Freedom

Recommendations

Develop modular research security programs rooted in five core pillars:

Pillar I: Organizational Culture

- Fostering a security culture, successful research security schemes entail technical controls and a security-conscious culture among researchers and staff, since researchers are the first line of defense.
- When senior faculty and administrators lead by example, the security culture will likely positively impact the organization.
- To safeguard international travel, it must be preapproved and subject to disclosure. In addition, short-term loaner device programs for cell phones, laptops, and USB drives should be implemented to reduce the risk of seizure, loss, or infection by malware during researchers' international travel.

Pillar II: Process

Processes are key to creating a foundation for research security. Furthermore, institutions involved in international research security consortia gain access to a pool of expertise, which enables them to enhance their security posture.

- Institutions should implement research security programs tailored to their unique needs and risk profiles.
- Research Security Offices (RSOs) provide the necessary expertise to execute research security while preserving institutional autonomy and achieving buy-in from researchers.
- For international collaboration with clear security guidelines, institutions should be aware of sanctions by performing open-source research to comply with regulations within their country or when collaborating with other countries.
- Due diligence must be conducted thoroughly before entering research partnerships, such as reviewing financial stability and ethical standards, and doing so continuously throughout the project. Investigative service tools are available to assist with due diligence.
- Mandatory disclosures and reporting offer transparency.
- Continuous and comprehensive risk assessments must be made throughout the life cycle of any research project.
- Regular security audits and reviews will improve the effectiveness of security protocols and identify potential weaknesses.
- Institutions must comply with national export control regulations to prevent the unauthorized transfer of sensitive technologies or information.
- Institutions should establish anonymous reporting tools and whistleblower protections that allow staff to report potential security threats without fear of retaliation and with transparency.
- Case study scenario-based training can include cyber risks, talent and recruitment program risks, insider threats, failure to follow procedures, and travel risks.

- Having a strong cyber security process is essential to protect sensitive research data.

Pillar III: Policy

Implementing an effective security program for research begins with developing an institution-specific security framework to address individualized vulnerabilities and needs. Key research areas, including AI, quantum computing, biotechnology, and research related to sensitive data, must be prioritized for national security. The following actions support effective policies:

- Instituting tiered research security capabilities at the national and institutional levels allows the research ecosystem to maintain open data exchange.
- A practical framework for international travel and collaboration demands that international sanctions be continually monitored to understand who is facing the consequences of malign foreign influence.
- Faculty disclosures must be mandated, and training modules developed to assist researchers and safeguard them from exploitation.

Pillar IV: Awareness and Training

Developing effective awareness and training programs promotes a security-conscious culture within academic and research institutions. Effective instruments that drive awareness include:

- Training materials
- Training completion tracking
- Tailored security training programs
- Consistency by RSOs
- Understanding of international collaboration standards
- Export control compliance training

- Scenario-based training
- Cyber security training.

Pillar V: Cyber Security and Technology

Cyber security includes installing system updates as issued by software developers, using complex passwords and multi-factor authentication, fostering a culture of vigilance through awareness and training, implementing effective cyber security frameworks, utilizing real-time threat detection, and having a plan for containment and response to cyber threats.

Technology options from governmental and commercial entities help manage security frameworks, enabling the secure management of research and innovation. Innovations for performing due diligence include artificial intelligence and machine learning, which Susie Spencer describes as "force multipliers" that can quickly investigate potential research partners on a large scale.

Conclusion

Research security is no longer an issue that impacts research institutions peripherally but is a central component of national security, economic advancement, and academic credibility. Building sustainable, adaptable, and values-driven research security programs for developing countries is a strategic imperative and an opportunity to lead responsibly in the global research ecosystem. Implementing the best practices identified in this paper will help institutions protect their research and reputation.

Introduction

Research security denotes the best practices and policies to safeguard research information, patented and proprietary materials, and research data in academic, government, and commercial research settings. With research activities deeply connected across the global environment, they are vulnerable to cybercriminals, patent infringements, and intellectual property (IP) theft. These vulnerabilities have significant financial implications for institutions and organizations, as they can damage their operational functionality and reputation. In the academic field, research security is crucial when gathering key information, adhering to established policies, and safeguarding national security. Academic research security programs are vital in academia, where the competitive advantage today depends on the security of ideas, patents, products, or research.

This paper answers the overarching question: *How can research institutions in developing countries implement a research security program that safeguards their intellectual property from malign foreign influence and enhances their country's economic and national security?* Through an in-depth literature study and attendance at the Academic Security and Counter Exploitation (ASCE) seminar, this research project further considers three sub-questions: (1) What core research principles from developed countries are most compatible with effective research security frameworks? (2) What best practices should HEIs and RPOs follow? (3) What are the benefits of implementing research security protocols and the risks associated with neglecting such protocols?

This literature review identifies the benefits of adopting research security programs, which should always lead the conversation with partners, as well as the threats associated with

not adopting research security programs and protocols. The approach of reviewing both aspects of the issue will enable the authors to demonstrate to stakeholders the necessity of conducting research with a specialization in security concerns. Moreover, case studies demonstrate both successful examples of implementing sound research security protocols and instances of failures resulting from complacency in this area. Both approaches emphasize that research security is essential for academic integrity, research security, and national security.

The National Academies of Sciences, Engineering, and Medicine's National Science, Technology, and Security Roundtable highlighted an important characteristic of research security and integrity. Remembering to protect it, from "fundamental research" to "applied research," is essential. (Hagan 2025, p. 37). Fundamental research includes researchers' ideas. The funding sources and clear understanding of international collaborators who may pose a threat must be assessed through due diligence at the fundamental research stage. Applied research encompasses the stage at which research has become IP. The sources of venture capital and investment must be assessed to determine if the applications have a potentially harmful end use, and international transactions must be vetted. (Hagan)

By studying the benefits achieved through the protocols proposed in this research, and clearly understanding the risks when the recommendations are unheeded, partnering nations with less developed academic research security structures will have a guide to follow as they broaden their participation in the global research community.

Literature Review

The obligation to safeguard academic research from malign foreign influence has garnered international attention with the increasing interconnection of the global scientific and technological research landscape. Other names for the phenomenon may include external influence, geopolitical interference, or international leverage, yet the outcome remains the same. Sovereign nations and independent academic institutions resist attempts by hostile actors, whether state-affiliated or non-state, to exploit their technological innovations and intellectual property (IP). Research institutions in developing countries face unique challenges in protecting their IP while fostering innovation and collaboration. This literature review addresses the overarching question: *How can research institutions in developing countries implement a research security program that safeguards their intellectual property from malign foreign influence and enhances their country's economic and national security?* Through an in-depth study of key themes in the literature, this review explores three sub-questions: (1) What core research principles from developed countries are most compatible with effective research security frameworks? (2) What best practices should HEIs and RPOs follow? (3) What are the benefits of implementing research security protocols and the risks associated with neglecting such protocols?

1. Putting Research Security in a Global Context

The literature identifies a growing international concern about the vulnerability of academic institutions to foreign exploitation. D'Hooghe and Lammertink (2023), Antoni (2020), and Tiffert (2020) highlight the risks that may accompany open scientific collaboration. Bochorodycz (2023) adds a strategic perspective by showing how alliances and national

interests intersect in academic diplomacy. However, while these sources agree on the rising threat level, they differ in their proposed countermeasures. Antoni (2020) focuses on systemic frameworks, whereas Bochorodycz (2023) emphasizes the use of soft power engagement. This contrast underscores a gap in the literature around the coordination of diplomatic and institutional responses.

Giumelli and Onderco (2021) offer insight into how private and public actors uphold knowledge security in the Netherlands, suggesting that shared management may be more sustainable than state-led mandates. Ross (2024) criticizes excessive institutional secrecy, warning that it may deter collaborative innovation. In contrast, Shih (2024) highlights the overextension of national security concerns in academic settings, which can result in a chilling effect on research.

Meanwhile, the OECD (2022) and Smith and Walsh (2023) advocate for a unified approach to research integrity and security, aligning with frameworks such as Canada's "Safeguarding Your Research" and Australia's Code for the Responsible Conduct of Research (NHMRC 2018). These models serve as functional templates, but their success depends heavily on domestic institutional capacity, which may be limited in developing countries. Notably, the U.K. Foreign Affairs Committee (2019) and German BMBF (2024) go further, advocating the framing of research security as a national strategic objective and treating intellectual capital as critical infrastructure. Mazarr (2015) and Milevski (2024) support this by identifying gray zone competition as a growing sphere where academia serves both soft and overt power objectives. The result is that the literature agrees on the urgency of action, but disagrees on the balance between openness and control.

2. Core Principles of Research in Developed Countries

Academic Freedom and Scientific Openness

Academic freedom is a cornerstone of research environments in developed nations, but its accordance with security policies is complex. Baylis, Smith, and Owens (2022) advocate for maintaining open inquiry as essential to scientific progress, while the International Science Council (2024) frames openness as a global standard necessary for collaborative knowledge production. However, Van Der Molen (2023) critiques how national security imperatives in countries like the Netherlands can inadvertently limit legitimate international engagement. Briffa (2023) likewise warns that policies focused on fear of foreign interference may foster prejudice and hinder partnerships, especially with researchers from non-Western countries.

Shih (2024) expands this critique by highlighting the lack of clarity in security policies, which can lead to self-censorship in academia. In contrast, the OECD (2021) advocates for balance through open-access mandates and transparency, suggesting that clear and publicly accessible policies can mitigate this tension. The European Commission (2023) and Pannier (2023) endorse a standardized approach that prioritizes open science while utilizing focused protections for critical technologies. The emerging view suggests that squaring freedom and security requires more than a compliance framework; it requires cultural alignment across institutions, funders, and governments.

Research Integrity and Ethical Conduct

Integrity frameworks ensure responsible research practices, but their effectiveness varies across environments. Armond and Kakuk (2021) analyze Brazil's evolving approach to institutional ethics, revealing gaps in enforcement despite policy adoption. Resnik (2020) argues for standardized ethics training as a universal safeguard but acknowledges that institutional

unwillingness can hamper its impact. The Singapore Statement (2010) and World Conferences on Research Integrity offer global norms, but their acceptance has been irregular, especially in countries lacking regulatory infrastructure.

Cerdà-Navarro *et al*. (2022) highlight academic fraud as a growing threat to research trust, especially in underregulated digital publishing environments. Hossain, Çelik, and Hertel (2024) expand the discussion by linking research ethics to copyright and information literacy, which are often overlooked in traditional integrity training. Ordoñez de Pablos (2024) and Gardner *et al*. (2021) connect ethical conduct to larger frameworks of responsible innovation and artificial intelligence (AI) governance, indicating a shift toward a more integrated view of research responsibility. These connections suggest that integrity is not merely about avoiding misconduct but also about fostering resilience, credibility, and societal application in research institutions.

National Interest and Export Control Compliance

Export control programs are prominent in research security in developed countries, but their design and implementation vary widely. The US Export Administration Regulations (EAR), International Traffic in Arms Regulations (ITAR), and Bureau of Industry and Security (BIS) guidelines (2024) offer detailed classifications and control lists of dual-use technologies. Although these are comprehensive, the systems are often criticized for their bureaucratic complexity, which can delay research and discourage international collaboration (GAO 2023).

Kimball (2022) examines the Wassenaar Arrangement and finds that countries implement its principles inconsistently despite its multilateral intent. The German DFG (2022) and the Japanese CSTI (2021) embrace more targeted, science-specific guidelines that balance

protection and innovation. Ollongren (2020) presents the Dutch case, where enforcement focused heavily on Chinese partnerships, triggering a backlash from academic institutions.

A critical contrast emerges between the US and EU models. While the US prioritizes national defense through rigid regulation and guidance, such as NIST's *Safeguarding International Science, Research Security Framework* (Strouse *et al.* 2023), EU countries often employ risk-based approaches, allowing for institutional decision-making. This difference has profound implications for the autonomy of research. For instance, Cornell University (2024) and Imperial College London (2023) have developed internal risk-screening procedures to comply with national and international obligations, highlighting the burden shifted onto institutions.

Critically, many scholars argue that these frameworks must change along with emerging technologies such as AI, quantum computing, and biotechnology, where rigid export control lists quickly become outdated. This challenge is confirmed by Paulsen (2024), who advocates for more adaptable, collaborative compliance models. While export controls are essential to research security, their overly restrictive application can undermine scientific progress and global cooperation.

3. Best Practices for Research Security Programs

Due Diligence and Risk Assessment

Adequate research security begins with robust due diligence protocols. Institutions such as Aston University (2022), Lancaster University (2024), and UKRI (2022) have adopted systematic processes to evaluate international partnerships, intellectual property vulnerabilities, and reputational risks. These models rely heavily on structured vetting, red flag indicators, and

data-driven assessments. However, Enkhtur, Li, and Zhang (2021) point out that these frameworks often assume a high level of institutional development, which can be unrealistic in under-resourced or developing institutions.

In contrast, the Netherlands' "Capability Maturity Model" (Netherlands 2023) offers a tiered framework that accommodates different institutional capacities. This is especially useful for global adaptation, allowing developing countries to scale up into more comprehensive security programs gradually. Meanwhile, critics like Claeys-Kulik *et al*. (2020) argue that institutional risk tools are insufficiently used without national coordination. The GAO (2022; 2023) echoes this critique in its audits of US universities, revealing that even well-resourced institutions often lack centralized data on international collaboration. This results in fragmented oversight and increased vulnerability.

Thus, while due diligence practices exist in robust forms, their effectiveness is often hindered by capacity constraints, decentralized implementation, and insufficient alignment with national risk intelligence. The literature collectively suggests that due diligence cannot be a checklist exercise. It must be implemented in an institution's strategic culture and supported by national infrastructure.

Governance Structures and Training Programs

Governance structures are foundational to embedding research security within institutional operations. Clark (2024) and Crandall (2023) argue that research security initiatives struggle to take root without executive-level support and cross-departmental coordination. This is particularly true for institutions where research governance is not effectively managed or security is not viewed as a shared responsibility.

Training programs have become a popular strategy for institutionalizing best practices. Examples from Cornell University (2021), Virginia Tech (2024), and the University of Maryland, Baltimore (2025) demonstrate how workshops, onboarding protocols, and ongoing compliance education help institutional actors understand regulatory obligations and emerging threats. However, the literature also highlights variations in the quality, scope, and funding of these programs across countries.

The Japanese government's dual approach, where they issue both a "Checklist for Internationalization" (2023) and a "Guideline on Integrity" (2021b), represents a coordinated national model that ties training directly to funding eligibility. This contrasts with more decentralized models in the US Federal guidelines (e.g. NSF 2024), which recommend training but leave the implementation to individual institutions.

However, critics like Christiansen (2021) and Gardner *et al*. (2021) warn that training can lose its value if not grounded in institutional culture and supported by audits and enforcement efforts. Researchers can race through online training. Merely checking the box on compliance modules does not ensure behavioral change. Moreover, cultural resistance and faculty skepticism can undermine participation, especially in the academic realm where autonomy has been institutionalized. Researchers like their freedom.

The consensus across the literature is that governance and training must work hand in hand. Strong governance connects resources, incentives, and expectations, while training ensures widespread awareness and consistent application. Institutions that neglect either one risk having fragmented or ineffective research security programs.

Collaboration and Transparency with Government Agencies

Collaboration between research institutions and government agencies is a critical but often underdeveloped component of research security. The guidance emphasizes the importance of real-time intelligence sharing, standardized reporting protocols, and early detection of foreign interference (ODNI *et al.* 2024). This detection advice includes reporting security threats and is similar to the "see something, say something" approach commonly used in counter-terrorism efforts. These mechanisms can provide institutions with valuable foresight into emerging threats and help them tailor their internal controls accordingly.

However, several sources critique the disparity of this collaboration. Christiansen (2021) and the German Rectors' Conference (2020) argue that vague mandates or overly aggressive interventions may erode trust between academia and the state. Who wants the government in academia? A Canadian Parliamentary report (Parliament of Canada, 2024c) echoes these concerns, noting that poorly defined roles and inconsistent interagency coordination can deter universities from fully participating.

CAPES (2023) in Brazil and the BMBF (2024) in Germany represent more structured government-led models where ministries actively guide security efforts while respecting institutional autonomy. The correct explanation might make a difference. Similarly, Japan's CSTI promotes partnership through national integrity policies that communicate expectations without excessive intrusion.

Transparency also helps engender trust. Gaviao, Dutra, and Kostin (2021) advocate for clear, publicly accessible risk guidelines to help academic institutions proactively manage

compliance. In contrast, Job (2022) warns that excessive transparency can backfire, making institutions vulnerable to geopolitical backlash or cyber exploitation.

The literature suggests that collaboration and transparency are most effective when government engagement is framed as supportive rather than punitive and when universities are treated as partners in safeguarding national interests rather than passive enforcement nodes. This shows a positive collaboration.

Digital Infrastructure and Cyber Security Measures

Cyber security is now a cornerstone of research security policy as academic institutions increasingly store sensitive data and collaborate internationally using digital platforms. Scholars such as He, Frost, and Pinsker (2020) and Farid, Warraich, and Iftikhar (2023) emphasize that vulnerabilities in digital infrastructure threaten institutional operations. They can also erode national competitiveness by facilitating IP theft and espionage. The 2018 Australian National University (ANU) breach (Sarraf 2019; Stilgherrian 2019) remains a high-profile case that illustrates how sophisticated state-sponsored cyberattacks can penetrate advanced academic environments.

Geer, Jardine, and Leverett (2020) argue that firewalls, encrypted storage, and two-factor authentication are insufficient without an integrated strategy that includes personnel training, vendor vetting, and policy alignment. This is despite many institutions' best efforts to do so. Thakur (2024) adds that fragmented systems across departments often create weak points, especially when cyber security is seen as the sole responsibility of IT staff.

Comparative models from Japan, Germany, and the US illustrate different national strategies. Japan's METI has integrated cyber security assessments into research funding eligibility. US agencies, such as the Cybersecurity and Infrastructure Security Agency (CISA) and the Office of the Director of National Intelligence (ODNI), produce guidance tailored explicitly to higher education. Studies by Olweny (2024) and Ige, Kupa, and Ilori (2024) show that awareness is growing in Brazil and Nigeria. Nonetheless, there is still chronic underfunding and a lack of expertise.

Most importantly, digital infrastructure must also address data governance and cross-border transfers. Kianpour, Kowalski, and Øverby (2021) highlight how regulatory misalignment between national systems, such as GDPR in Europe versus looser regimes in other regions, creates compliance dilemmas for international consortia. This complexity suggests the need for harmonized standards or mutual recognition agreements.

Overall, cyber security is not merely a technical issue but an organizational and geopolitical one. Institutions must view it holistically, embedding it in governance, budgeting, and training. Thus, they can effectively protect research integrity and national interests.

4. Implementation Challenges for Developing Countries

Implementing research security frameworks in developing countries presents distinct structural, financial, and political challenges. Differences in research capacity, regulatory infrastructure, and access to technical expertise compound these challenges.

One of the most frequently cited obstacles is resource limitation. Bui, Bui, and Pham (2024) highlight that institutions in Vietnam often lack the funding and personnel to fully

implement SDG-aligned research governance. They also cannot add complex security protocols. Cross *et al*. (2017) reach a similar conclusion in their analysis of Brazilian institutions. They find that internationalization efforts are frequently prioritized over security investments due to external funding incentives.

Capacity gaps extend beyond funding to include human capital and institutional maturity. Campoli *et al*. (2025) emphasize that without stable governance structures, research security frameworks risk becoming "paper policies" that are not enforced. Tapay-Cueva and Dong (2023) point out that efforts to increase scientific autonomy in Brazil are undermined by weak enforcement and bureaucratic fragmentation. This prevents a coordinated response to foreign influence.

Legal and regulatory frameworks also pose a barrier. While some countries have adopted high-level strategies (e.g., Brazil's CAPES policies or Japan's integrity checklist), these often lack the enforcement mechanisms and institutional support necessary for consistent application. Antoni (2020) argues that many developing countries attempt to adopt external best practices without tailoring them to local contexts, leading to a mismatch between design and implementation.

Furthermore, scholars such as Job (2022) and Efstathopoulos (2021) stress that developing countries face unique geopolitical vulnerabilities. Their academic institutions often operate in environments that depend on international funding. This primarily stems from the actions of great powers, which can create both opportunities and risks. Gabriel (2020) highlights Latin America's strategic entanglement with Chinese investment. Komljenovic and Williamson (2024) warn that higher education exposes institutions to surveillance and exploitation.

Despite these challenges, several authors recommend positive ways forward. The OECD (2022) and Paulsen (2024) suggest that international frameworks should be adaptable and modular. They should also allow developing nations to build capacity without being excluded from global research networks. Moreover, partnerships that emphasize equity and mutual benefit, rather than one-sided compliance, are more likely to foster sustainable security cultures.

In summary, implementing research security in developing contexts requires more than replicating models from developed countries. It demands a nuanced, context-sensitive strategy that addresses capacity constraints, political realities, and institutional ecosystems.

5. Benefits of Research Security Programs

The literature overwhelmingly affirms that research security programs substantially benefit institutions and nations, particularly in protecting intellectual property, sustaining innovation ecosystems, and enhancing global reputation. These programs focus on defensive mechanisms and strategic investments in resilience, trust, and long-term competitiveness.

One of the most widely cited benefits is the protection of national interests and the enhancement of innovation capacity. Atlamazoglou (2024) provides a compelling estimate of the economic losses associated with IP theft. This is especially true in the high-tech and defense sectors. Meanwhile, Mervis (2024), Hagan (2025), and Flagg, Toney, and Harris (2021) show how government investments in secure R&D environments yield dividends in innovation and economic security. Research security mechanisms act as safeguards for these public investments. This is especially so when taxpayer-funded discoveries carry dual-use or commercial potential.

Another significant advantage is the enhancement of institutional trust and global reputation. Resnik (2020), Gardner *et al*. (2021), and the OECD (2019) suggest that institutions with strong ethical and compliance records are better positioned to attract funding, form global partnerships, and withstand political scrutiny. These sources argue that security and ethics are mutually reinforcing. Well-governed research is also more likely to be trustworthy and socially beneficial. Gabriel (2020) and Efstathopoulos (2021) extend this argument to a geopolitical level, showing that countries with secure and ethical research environments gain leverage in international science diplomacy.

Research security also contributes directly to national economic and technological development. Paulsen (2024), Xu (2024), and Milevski (2024) draw a straight line between protected knowledge systems and sovereign industrial capacity. This is echoed in frameworks published by BIS (2024c), ODNI (2021), and Pannier (2023). They argue that secure research systems are essential for successfully deploying emerging technologies like AI, quantum computing, and biotechnology. These capabilities are increasingly seen not just as academic pursuits but as strategic assets that shape global power structures.

Notably, the literature suggests that the benefits of research security are cumulative and synergistic. Programs that integrate cyber security, governance, integrity, and transparency do more than protect against threats. They build an institutional culture of responsibility and resilience. Zhang *et al*. (2022) support this view by demonstrating how AI collaboration in secure environments fosters innovation without compromising national interests.

While critics sometimes argue that security policies may hinder openness or collaboration, the emerging consensus is that well-calibrated frameworks can enable more

sustainable, equitable, and productive research partnerships. Institutions that proactively implement research security measures are not merely shielding themselves. They are creating conditions for ethical, strategic, and globally competitive science.

6. Risks of Inaction

The risks associated with failing to implement research security measures are profound. They are also wide-ranging, touching on national security, public trust, and the strategic autonomy of academic institutions. The literature shows what can go wrong when vulnerabilities are left unaddressed.

One of the most pressing risks is exposure to espionage and IP theft. A series of reports from the US Government Accountability Office (2005, 2008, 2011, 2020, 2023) document gaps in the enforcement of export controls, collaboration oversight, and institutional awareness. The Charles Lieber case, detailed by El-Bawab (2023), illustrates how poorly monitored research relationships enable external governments to access sensitive knowledge. Similarly, ODNI (2021) and the Canadian government platform (2024) provide case studies where the absence of clear institutional protocols contributed to the misappropriation of research outcomes.

Inadequate research security can also undermine public trust in science and higher education. Christiansen (2021). The German Rectors' Conference (2020) cautions that failure to prevent unethical collaborations or cyber breaches erodes the credibility of research institutions. Van Der Molen (2023) ties this erosion to broader skepticism about the political neutrality of universities, particularly when foreign influence is perceived as affecting the integrity of scientific outcomes. Olweny (2024) links these concerns to financial technologies, highlighting how compromised research can have a ripple effect on economic systems.

Another significant risk is the loss of national policy autonomy. Scholars such as Job (2022), Tapay-Cueva and Dong (2023), and Efstathopoulos (2021) demonstrate how dependence on international research funding, platforms, or partnerships can limit domestic decision-making. Gabriel (2020) provides examples from Latin America, where entanglements with Chinese scientific infrastructure have created diplomatic tensions. Mazarr (2015) and Milevski (2024) argue that knowledge systems are increasingly weaponized in an era of gray zone conflict. Countries that do not control their research pipelines risk becoming pawns in geopolitical rivalries.

In short, the cost of inaction is not merely theoretical. It is observable in real-world breaches, scandals, and strategic setbacks. Institutions that lack comprehensive research security measures risk losing their credibility, discoveries, and autonomy in scientific and political spheres.

Future Direction

The literature reviewed demonstrates that research security is not only a technical or compliance concern. It is a strategic necessity embedded in international collaboration, national competitiveness, and institutional trust. While developed countries offer robust frameworks and established models, these cannot be replicated in developing contexts. Instead, developing institutions must adopt context-sensitive approaches that reflect their capacity, governance culture, and geopolitical position.

Key themes emerge across the literature: the tension between openness and control, the need for scalable due diligence, the central role of cyber security, and the importance of cross-

sector collaboration. Policies that strike a balance between preserving academic freedom and protecting national interests are more likely to be effective and sustainable.

The risks of inaction are considerable, ranging from espionage to reputational damage to diminished sovereignty. However, as the literature also shows, the benefits of thoughtful, well-integrated research security policies include stronger institutions, better international partnerships, and long-term economic and technological resilience.

Future research should explore case studies from institutions in the Global South that have implemented innovative or locally adapted security strategies. Comparative analysis could help identify best practices that are both globally informed and locally grounded. Additionally, interdisciplinary collaboration among security experts, ethicists, technologists, and policymakers will be critical in designing next-generation research security frameworks that are both ethical and effective. Ultimately, safeguarding research integrity is about more than compliance. It is about preserving the integrity, sovereignty, and societal value of knowledge.

Methodology

Core Principles of Research

Several key considerations emerged during the research on core principles in developed countries that are essential to research security programs. Identifying the specific areas of research that are most vulnerable is a prerequisite for any research security program. Internet tools are available to stay abreast of sensitive technology areas. (Canada 2024b) All research is susceptible to being pilfered. Therefore, organizations need to understand the risks and take action to minimize intellectual and technology theft (European Commission 2023; ODNI 2021).

Geopolitical factors should also be considered when determining vulnerability. Relationships between nations provide a framework to recognize areas of concern. Due to research theft worldwide, organizations must remain diligent in their dealings and associations with countries or groups that could potentially expose their research to security risks (Aston University 2022; HRK 2020).

Suppose organizations work with national security programs or receive government grants or funding. In that case, their research security program should account for measures to protect their research and the programs of the organizations with which they work, as mandated by the *Presidential Memorandum on US Government-Supported Research and Development National Security Policy* (Trump 2021). Understanding their role in the research security process can help mitigate potential security threats in the context of the open exchange of information common in academia and research. It is further aligned with the *Memorandum for the Heads of Federal Research Agencies.* (Prabhakar 2024) Additionally, awareness of evolving threats should be enhanced by utilizing available open-source tools. (Canada 2024)

Organizations should work with government agencies to be aware of potential research security risks and programs that can assist in preventing security issues, particularly in sensitive areas (Prabhakar 2024; BMBF 2024). Many universities are implementing research security measures to reduce their exposure to security breaches (Smith and Walsh 2023). Policies and procedures incorporating research security measures are the first steps in mitigating security threats (Bochorodycz 2023). Moreover, policies and procedures implemented across the organization help coordinate efforts to minimize risks (NPSA 2024; OECD 2023). Many universities are developing policies and procedures to enhance their security measures.

Universities are evaluating their international collaboration efforts in a manner that helps identify foreign influences in their research and those individuals involved in the research studies (NPSA 2024). While it is imperative to continue collaborative research, measures must be taken to reduce threats from menacing sources (DFG 2022; Claeys-Kulik, Jorgensen, Stober *et al*. 2020).

Training in implemented policies and procedures is imperative when implementing a research security program (Prabhakar 2024). Highlighting researchers' legal and ethical obligations is a critical exercise that organizations must address in their policies and training. Training is typically beneficial if it is clear, detailed, accessible, and practical (D'Hooghe and Lammertink 2023). Training should include best practices, case studies, and checklists, highlighting areas and opportunities for improvement (Imperial College London 2023; Crandall 2023). The implementation and training of research security policies and procedures should also emphasize self-monitoring, awareness of potential security risks, and building relationships with government agencies and best practice organizations (BMBF 2024).

While security risks should be addressed, academic freedom, open research, and IP are key areas researchers believe are essential (BMBF 2024). All researchers should be trained in academic integrity and ethics, especially if they participate in collaborative research with potentially foreign-influenced institutions or personnel (Smith and Walsh 2023).

Best practices, including security protocols, risk assessments, research awareness, risk management, policies, procedures, and international relationship reviews, are key to an organization's research security (BMBF 2024). Organizations should have a means of cross-referencing personnel to establish connections with foreign influence. Open communication with government agencies and partners can help expand connections (Ross 2024). Thorough interviews should be conducted with potential personnel to establish connections with foreign influence. Putting these strategies into practice allows HEIs and RPOs to initiate the foundations of a research security program.

Overview of Research Security Programs

Security programs have emerged as critical reference models in various settings and fields, including universities, companies, and research facilities that support guarding information assets, patents, and original research results. Such programs are aimed at the emerging security risks of preserving data consistency, safeguarding ideas and income, and critical compliance with regulations. A well-rounded research security program generally includes documenting, classifying, and securing IP. The trend is apparent in data protection measures, protection of IP rights, and compliance checks (Kianpour, Kowalski, and Overby 2021). In turn, each component plays its part in the reliable protection of research processes and

in minimizing threats such as unauthorized data access, piracy of research and other materials, or violation of legal requirements.

The fundamental principle of data protection underpins the research security programs, mainly protecting research data from unauthorized access, accidental damage, or threats from hackers. Security shields cover a broad spectrum, including encryption, protection of stored information, and firewalls to deny access and leakage. The final security policies include access control policies, which restrict the data by employees and fellow researchers and limit the scope and access rights of their positions. Data is sensitive and necessary for research institutions to protect research credibility and participant confidentiality, as well as for security reasons with national security implications.

Security programs exist in different research institutions and have unique reasons and purposes for implementing research security. For example, universities often research interdisciplinary fields, including medical research, engineering, and social sciences. The targets of these institutions are frequent sites of academic hospitality where assumptions about openness may constitute risks (Fedele and Roner 2022). The issues of confidential information and IP protection arose at the universities as many began interacting with business and government organizations. Many university boards have established separate offices for research compliance and technology transfer, coordinating with trademarks and patents, and managing data to safeguard research work.

Research security programs are critically important for the corporate world, particularly for companies operating in technology, pharmaceuticals, and biotechnology, where research and development define the company's competitive strategy. Many companies respond by adopting

corporate research security programs that focus on IP safeguarding and data defense, including using AI for threat identification and the blockchain for data authentication and surveillance systems. Corporate strategies are used to safely manage research security because any breach or leak can lead to significant loss of funds and damage to reputation. Different companies have their divisions for security or hire the services of third-party security companies to help them put up and enforce sound research security measures.

Research laboratories have specific security needs, especially those focused on governmental or defense activity. Information involving chemistry, genetics, military weapons, and AI is filtered through these labs, which often concern national security. Consequently, they implement high-security measures that may be considered above the industry average of many controlled access facilities, and confidentiality agreements are tightly regulated. Labs that governmental organizations subcontract must comply with the Federal Information Security Modernization Act (FISMA) and export control policies. Still, they frequently add more security measures to protect their work (Geer, Jardine, and Leverett 2020). This institution must have a broad security program to protect data, key funding sources, and government grants. It also helps institutions that are interested in reports sent by the laboratory.

Capstone Group Research Methodology

The research methodology employed by the Capstone authors of this study of Academic Research Security began with one week in residency at the Bush School of Government and Public Service on the Texas A&M University campus in Washington, D.C. The residency included initial introductions to the team, the Capstone instructor, and the client. Dr. Kevin R. Gamache, Associate Vice Chancellor and Chief Security Officer for the Texas A&M University System, ensures that Texas A&M's 11 universities and eight state agencies comply with the US government requirements to protect sensitive federal information. The students' professional backgrounds vary across the public and nonprofit sectors, incorporating local and federal service experience. The sponsoring agency for this Capstone project is Sandia National Laboratories. All parties collaborated during the residency week to design the research questions, project goals, and milestones.

Following the residency week, the students divided the research questions and began the weekly review of current publications related to academic research security and integrity. Each team member shared publications and exchanged feedback throughout the fall semester, meeting weekly for study discourse and planning discussions. Monthly meetings included the course instructor and the client. By the end of the fall semester, the Research Plan and Literature Review were completed and submitted to the client. In the spring semester, the second half of the Capstone project continued, with the team's attendance at the Academic Security and Counter Exploitation seminar at Texas A&M University in College Station. During this week, the Capstone team attended lectures presented by academic and governmental security officials from around the world, alongside approximately 600 research security practitioners. It facilitated informative conversations that contributed to a deeper understanding of this deliverable.

Discussion

Theory and Values

Digitalization and non-state actors have changed the art of war to include gray zone tactics, irregular warfare, and interference from competing nations (Mazarr 2015). Driven by a fear of the reigning conventional military superiority of the US (Mullins 2024), authoritarian governments in pursuit of supremacy have exploited the world's rapid expansion of digital technology to fuel their culture of military innovation and statecraft. By employing technology and non-state actors, government entities have capitalized on the opportunity to exist in a gray zone between outright conventional warfare and peace in international relations (Mazarr 2015; State 2017). In this context, they have focused on a strategy of external malign influence through deliberate, nonviolent hybrid conflict strategies using nonmilitary instruments of power such as economic, political, social, and informational pressures (Jordan 2020). Authoritarian nations also take advantage of the "limitations and dilemmas involved in employing such strategies" within the gray zone (Mazarr, p. 126). The gray zone allows continuous innovation through subversion and infiltration of Western society while disregarding conventional warfare objectives, such as victory, shock and awe, and immediate dominance (Milevski 2024).

Non-state actors are entities that, while not directly representing governments, nevertheless wield consequential influence in international affairs (NIC 2007). These actors may operate autonomously, semi-autonomously, or under state direction, motivated by self-interest, coercion, or the benefits of executing malign state-influence operations (Mullins 2024). Regarding research security in HEIs, non-state actors can be identified and activated to execute malign foreign influence or state-directed exploitation through gray zone tactics. Through the development of talent programs designed to engage researchers, the establishment of quid-pro-

quo relationships, or outright coercion (ODNI n.d.), external governments can source, acquire, and relay valuable innovation back to their sovereign borders for employment in their military and economic statecraft.

The research industry is rich with IP and state-of-the-art development in all sectors. There is ample opportunity for malign actors to access an institution's prized intellectual property, which are described as "crown jewels" (Brown and Singh 2018), through non-state actors since the research industry's culture values openness, international collaboration, digitalization, sharing, and international travel as norms of conduct (Resnik 2020, OECD 2021). Academics see this as central to the operation of science (OECD 2022). With the apolitical nature of international collaboration, it is common for HEIs to diminish the importance of nationality and promote collaboration across national borders, making it routine to see "researchers from different countries working together regardless of the geopolitical and ideological positions of governments" (OECD 2022). Furthermore, the research industry's frameworks enable and advance international scientific exchange and collaboration.

HEI stakeholders, such as administrators, faculty, and students, may not be aware of how their activities align with strategic state interests to expand their influence on the world stage. Additionally, these stakeholders are typically non-participants in national defense. They may not realize they are infringing on national security or contributing to dual-use research and state-sponsored interference. Given their proximity to international participants in the research industry, it is in this gray zone of opportunity for malign foreign influence that it becomes "important for researchers to learn how to interpret, assess, and apply various research rules and how to make decisions and act ethically in various situations" (Resnik 2020). This includes being aware of research security, employing best practices, and mitigating risk. It can be

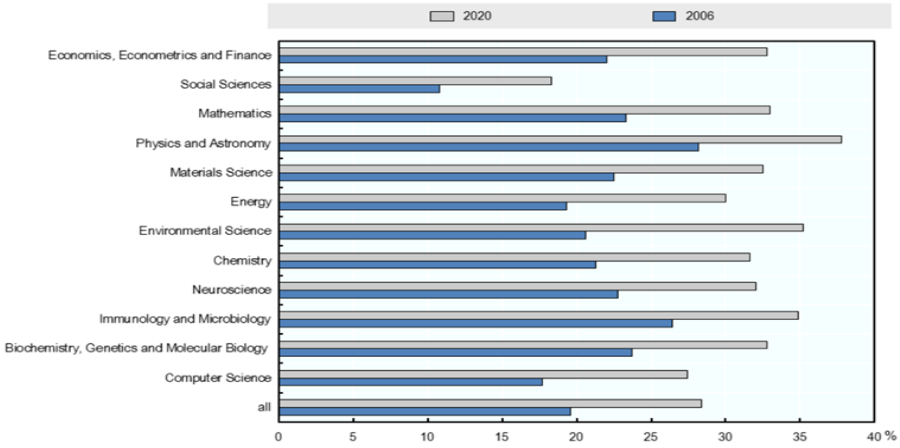
challenging for HEI stakeholders to distinguish between international governments pursuing a legitimate interest in education and those interested in subversive, undeclared, coercive, or criminal activities.

International councils have developed statutes, rules of procedure, and recommendations to promote fair use through various documents (ISC 2024). Multiple efforts and declarations boost international research collaboration and develop international access, ironically limiting nations' ability to deter malign influence. These recommendations and declarations include the *Statutes and Rules of Procedure* (ISC 2024); the *International Covenant on Economic, Social, and Cultural Rights* (U.N. 1966); the *Recommendation of the Council Concerning Access to Research Data from Public Funding* (OECD 2021); the *Marseille Declaration on International Cooperation in Research and Innovation* (French Presidency of the Council of the European Union 2022); the Recommendation of the Council on AI (OECD 2019); and Singapore's Statement on Research Integrity (World Conferences on Research Integrity 2010). Despite the international frameworks promoting scientific collaboration, they pressure organizations that want to protect their research. Institutions worldwide face this same pressure.

In an environment inherently willing to collaborate, share, and exchange research information internationally, the risk is high for research misappropriation to result in the "detriment of national or economic security, related to violations of research integrity, and foreign government interference" (NSTC 2022). Through direct infringement of the research industry's core values and disrespect of international regulations, state actors have found considerable opportunities in their ability to exert cross-border influence operations through non-state actors successfully. By targeting HEIs, hostile states can access tightly restricted pools

of research and information subject to export controls, encryption, and national security policies. Acknowledging the challenge for "countries to maintain the balance between open and trust-based scientific collaboration and protective but potentially restrictive regulations" (Organization for Economic Cooperation and Development 2022), HEIs must be proactive in developing research security programs that take a structured and methodical approach to risk management as international collaboration continues to expand. The Organization for Economic Cooperation and Development released a comparative analysis of internationally co-authored research collaborations from 2006 to 2020 (OECD 2022, 20), demonstrating the continued expansion of multinational research.

Figure 1. Percentage of scientific publications involving international co-authorships, OECD 2006 and 2020



Note: The figure shows the percentage of scientific publications co-authored among institutions in different countries.
Source: OECD calculations based on Scopus Custom Data, Elsevier, Version 5.2021, September 2021 (OECD, 2021[19]; n.d.[20]).

StatLink https://stat.link/7o0p25k/

The core research principles in developed countries that remain compatible with adequate research security include transparent international collaboration, responsible data sharing, academic integrity, and ethical research conduct. Developing countries can protect their research enterprise while honoring these principles through balanced security frameworks that safeguard intellectual assets without stifling innovation. Understanding how these principles can be

preserved while implementing security measures requires examining the benefits of research security programs and the risks of neglecting such protections. Meanwhile, the increasing interconnection of global research, shown in Figure 1, creates opportunities for innovation and vulnerabilities for exploitation. Institutions must develop research security protocols that protect IP without undermining the core values of academic freedom and open exchange of information. Understanding the benefits and risks of research security and identifying which crown jewels an institution wants to protect (Gamache 2024) are integral for developing a balance.

Comparative Analysis of Benefits v Risks

Research security programs establish indispensable protection for intangible institutional assets, personnel data, and an organization's reputation. These measures benefit high-tech firms and research institutes, where research results are under the most appreciable threat of theft. Prudent security initiatives safeguard an organization's IP and innovation from outside invasion and internal threats and assist the organization in following legal regulations, thus saving organizations from the iron hand of the law (Ige, Kupa, and Ilori 2024). These programs also enhance the environment's reliability, with collaborators, investors, and other stakeholders looking for safe institutional partners. In addition, a comprehensive security blueprint is a strategic asset that can protect advanced inventions from falling into the wrong hands and ensure an organization's authority to regulate the flow of its inventions into the market.

The lack of research security opens an institution’s door to consequential threats such as IP theft, data leakage, and reputational damage. Examples of cyber espionage have shown that some institutions lacked sufficient security programs, such that competitors or external entities used stolen data to duplicate similar technologies (He, Frost, and Pinsker 2020). Such losses are not only limited to diminished revenues but also include a loss of reputation that may reduce

future funding and partnerships. For example, some institutions have been criticized for compromising their research standards (Grimaldi, Greco, and Cricelli 2021). Thus, institutions with a tarnished reputation will need support and guidance to meet compliance requirements from grant-making institutions and the public. Academic and research institutions must avoid falling prey to hostile intrusions that will disrupt and delay their research operations. The high recovery costs resulting from external interference will stifle the ability to advance innovation and potentially hamper future research funding.

While the potential impact of research security programs differs across the variety of economic development worldwide, examining the benefits these programs offer HEIs provides a clearer understanding of their value. The following benefits demonstrate the advantages of well-designed research security programs and should always lead the conversation.

Benefits of Academic Research Security Programs

1. Protection of Intellectual Property and Sensitive Information

Protecting IP and sensitive data is one of the most prominent benefits of academic research security. Educational communities are at the forefront of breakthroughs and technological advancement, making them ideal targets for abuse and theft. Protecting such advances is paramount for a nation's security and competitiveness, as well as an institution's success (Komljenovic and Williamson 2024). When sensitive data and patented technologies such as renewable energy and aerospace are compromised, unfair access and covert exploitation can deliver undue benefit to enemies and competitors. Research institutions have a responsibility to secure their innovations.

A research security program also instills academic integrity by properly managing sensitive information and IP. In an era of increased data theft and IP misuse, universities have a

role in anticipating interference, securing their research, and upholding high ethical standards. Universities can safeguard their research and demonstrate responsible governance through security audits, access controls, and data encryption. Misusing this sensitive information in biotechnology, AI, and healthcare could have disastrous ethical and social repercussions (Hossain, Celik, and Hertel 2024).

Additionally, research security programs ensure an institution's compliance with laws and regulations. Many countries have rules and regulations protecting sensitive research, especially in countries with national security concerns. Institutions that violate such requirements can suffer severe consequences, including penalties, lawsuits, and loss of government funding. Research security programs guide institutions through complicated laws to ensure compliance and avoid penalties (Ali *et al*. 2021). They also help mitigate national security risks since AI, quantum computing, and biotechnology studies can involve national security (Pawlikowski 2024). Such research may be a weapon in the hands of competitors, stripping a nation of its technological ability to preserve its sovereignty. A research security program finds and fixes such flaws and can help it become a responsible partner in research and national security.

2. Maintenance of Academic Honesty and Trust

Another principal advantage of a research security program is establishing and maintaining academic integrity and trust. Honesty forms the backbone of successful collaborations, both institutionally and globally. Institutions and researchers gain the confidence of funding agencies, collaborators, and society by demonstrating a commitment to ethical practice and responsible information stewardship. Research security programs that responsibly secure sensitive information and IP (Cerda-Navarro, Touza, Morey-Lopez, and Curiel 2022). Trust is paramount in maintaining productive relations and driving scientific development.

For researchers and institutions to work effectively across borders and disciplines, trust is also at the root of successful academic collaboration. In an age of hyper-connectivity, when research involves increasingly complex relationships, honesty and trust must be preserved to promote innovation and build innovative ideas. Successful academic research security is integral to creating and maintaining such trust. It reflects an institution's commitment to ethical conduct and responsible preservation of sensitive information (Ibuken *et al*. 2023). With the assurance that its information and IP will not go astray, researchers and institutions will become increasingly willing to collaborate, combine assets, and make breakthroughs.

Moreover, a research security scheme empowers an institution to navigate the complex ethical and legal landscape of modern research. By adhering to best practices and satisfying requirements, an institution can avoid ethical issues and legal disputes that can erode trust and damage its reputation (Olweny 2024).

3. Compliance with Legal and Regulatory Requirements

Compliance with laws and legislation is obligatory for academic research security, enabling an institution to function under the cover of legality and protecting sensitive information. National governments have crafted a range of legislation and laws to safeguard work, such as in regions with national security concerns or sensitive information at issue, including laws governing control over specific technology and information exported to an external entity, such as under export controls, and laws over information, such as under European Union's General Data Protection Regulation (GDPR), governing the use of individual information. In the US, federally sponsored institutions must comply with legislation and laws, such as National Institutes of Health (NIH) guidance on foreign influence and requirements under the Department of Defense for protecting defense-related work. All such legislation and

laws function to prevent the misuse of work, preserve national security, and enable ethical behavior. However, they can become a challenge in compliance, such as for an institution with international collaborations and new work. An effective security program keeps an institution compliant through guidance, training, and oversight, minimizing opportunities for legal and financial consequences.

Failure to adhere to laws governing research security can result in financial penalties and lawsuits, loss of funding, and damage to reputation (Thakur 2024). Institutions that violate laws governing exports, for example, can suffer hefty penalties, including supplemental restrictions and financial penalties for future research. Similarly, not adhering to rules governing the protection of information can yield costly lawsuits and damage to an institution's reputation. In extreme scenarios, failure to adhere can result in a loss of funding at the national level, which can hinder an institution's ability to conduct research.

4. Mitigation of National Security Threats

Academic research in transformative fields such as AI, quantum computing, and biotechnology has decisive consequences for national security. Most emerging technologies have dual-use capabilities, serving both civilian and military ends. In hostile hands, such research can become an attack weapon, a tool for undermining a nation's technological edge, and a threat to national security (Priyanka *et al*. 2024). Securing such research is a matter of protection at an institution and a national imperative.

A robust security scheme for dual-use research is pivotal in countering such vulnerabilities. It entails having access controls, security audits, and background checks for workers in sensitive studies in place. Besides, an institution can have proper protocols for the dissemination of study information, such that sensitive information is not inadvertently shared

with unauthorized persons. By actively countering such vulnerabilities, a security scheme keeps critical technology secure from theft and misuse, safeguarding national security and an institution's studies. A notable achievement in successful risk avoidance is a university that kept dual-use technology, such as drones and encryption software, out of thieves' hands by imposing stringent export controls. University research in such technology had a high potential for use in military applications. It, therefore, represented a target for a country interested in acquiring the technology for use in a national security issue. By having a security program with high compliance with export controls, a university can ensure that its research in such technology is shared with approved entities (Giumelli and Onderco 2021). Not only did such a proactive action protect an institution's assets, but it also helped protect national security by preventing the misuse of sensitive technology. The case highlights the worth of a security program for research in closing gaps and minimizing vulnerabilities, allowing academic work to drive innovation without jeopardizing national security.

5. Enhanced Competitiveness and Reputation

A strong commitment to research security fortifies an institution's reputation and competitiveness, attracting funding agencies, top talent, and industry partners. In an era in which information breaches and IP theft have become widespread, responsible and proactive institutions with a high regard for research security have strong reputations (Mai, Bui, and Thai Pham 2024). Integrity and trust can attract top talent in terms of researchers who seek a secure environment to work, as well as funding agencies and industry partners who value ethical behavior and risk management. Research institutions prioritizing security have a better chance of being awarded grants, building international collaborations, and attracting private and public

investments. Such an edge is evident in competitive fields such as renewable energy, AI, and biotechnology, with high potential for misuse and high stakes.

Failing to protect research security can expose institutions to substantial risks despite these noteworthy benefits. When adequate security measures are overlooked, the following consequences can be expected.

Risks Associated with Failure to Implement Academic Research Security

1. Loss of Intellectual Property

Failure to have an academic research security program in an institution makes it susceptible to hijacking its IP by competing nations, corporate espionage, or malicious insider threats. Academic research involves cutting-edge breakthroughs and proprietary technology that is of high value to private and public entities. Without strong security measures, such as data encryption, access controls, and audits, an institution must sacrifice its competitive edge and financial gain from its breakthroughs (von Uexkull and Buhaug 2021). The long-term impact of hijacked IP can be even more profound, for it destroys an institution's ability to innovate and compete in a worldwide research and development environment. By not protecting its IP, the university not only stood to sacrifice its proprietary technology but also its position at the cutting edge of biotechnology research.

2. Reputational Damage

A security incident can have catastrophic consequences for an institution's reputation, eroding stakeholder trust and compromising its academic position. With sensitive information revealed or IP compromised, an institution is publicly criticized and questioned. For example, a research institution that experiences a data incident compromising sensitive patient information could see its reputation suffer immensely. An incident in which medical records in a clinical

study are accessed without authorization could cause a loss of trust between participants, collaborating groups, and funding agencies. As a result, it could fail to recruit participants for future studies and struggle with grant procurement. Consequences include loss of funding, collaborations, and academic standing for a long time, with stakeholders perceiving the institution as careless and untrustworthy (Komljenovic and Williamson 2024). The reputational loss jeopardizes an institution's ability to attract talent and resources, eroding its purpose in driving knowledge and innovation. In a competitive academic environment, a strong reputation is paramount, and failure to prioritize research security can have long-term consequences.

3. Threats to National Security

Academic research in critical fields such as AI, quantum computer technology, and defense technology can have significant national security implications. In the wrong hands, such research can become an attack weapon, a weapon for undermining a nation's technological edge, or both. Academic institutions have a requisite role in averting such a scenario through effective security programs that detect and counter vulnerabilities. By not assuming such a role, an institution can contribute to global instability and undermine its country's security. Academic institutions play a prominent role in safeguarding national security, and failure to secure a study can have disastrous consequences for both the institution and the nation (Ibrahim Halill and Abdel-Rahman 2023).

4. Legal and Financial Consequences

Failing to maintain a security program for research can have severe financial and legal consequences, including lawsuits, penalties, and the loss of government grants. Institutions that fail to comply with research security regulations, such as controls and laws safeguarding information and export controls, can face severe penalties. Such penalties can be disastrous,

specifically for universities whose work is supported almost wholly through government funding. Besides penalties, institutions may face lawsuits filed by dissatisfied individuals, adding additional financial burdens (Ibrahim Halill and Abdel-Rahman 2023). The long-term financial repercussions of compromised research security extend far beyond. They can jeopardize an institution's future funding and collaborations. Institutions that do not prioritize security in their research activity can undermine their financial viability and ability to conduct effective research.

5. Academic Freedom Erosion

Research security is important, but not at the expense of academic freedom and collaboration. An improperly executed security research program can cause overreactions, such as excessive restrictions or bans on international cooperation. For instance, an institution with a security incident involving sensitive research information could overreact and curtail international cooperation. The subsequent policy following the incident could hinder researchers' innovation and access to international counterparts to prevent future complications. Research is obstructed by undermining academic freedom, suppressing new work, limiting free thought, and encumbering information exchange (Cerda-Navarro, Touza, Morey-Lopez, and Curiel 2022). Academic freedom is fundamental to scientific progress. By not having a balanced mechanism for research security, institutes can jeopardize their role in creating new knowledge and innovation.

Due to the benefits of research security programs and the risks of failing to implement them, many countries have recognized that collaboration can enhance the effectiveness of these programs. Multilateral efforts have emerged as a powerful strategy to address research security challenges that transcend national boundaries.

Multilateral Efforts and Export Controls

Introduction to Multilateral Efforts

Developing standards and partnerships is imperative in the evolving world of fast-growing technology, with the introduction of AI and the urgent need to protect research and IP. Multilateral collaborations between nations and the individual achievements of Canada, Japan, Australia, and Brazil have become fundamental in the construction of robust structures for research security. Collaborating countries face common external threats, such as cyberattacks and IP theft. Collaborative efforts in research security emerge as a central response to a rapidly changing geopolitical landscape, justifying a thorough examination.

The need for improved research safety is underlined by the dynamics in the evolution of international relations (Gabriel 2020; Baylis, Smith, and Owens 2022). Gabriel discusses Japan's strategic involvement in South America, noting the increasing significance of South American countries in the context of global trade and technological development. The engagement between these countries shows the recognition and belief that research and technology security collaboration is beneficial to protecting national interests from collective threats (Gabriel). Japan, Canada, Australia, and Brazil have committed proactively to promoting research security networks that transcend bilateral agreements. It is a comprehensive strategy that recognizes the delicate issues of security risks and their transnational nature (Gabriel). The need for cooperation assumes multifaceted dimensions. For example, Canada has positioned itself as a leader in promoting multilateral initiatives focused on cyber security, sharing best practices, and fostering resilience in research environments (Canada 2024). Australia recognized the importance of information sharing on collaborative innovation and research platforms and put in place protocols that fortify national security while boosting technological advancement (Ross 2024).

With its diversified research landscape, Brazil uses its partnerships to promote its research agenda and contribute to a collective safety ethos that benefits all stakeholders (Armond and Kakuk 2021; Cross, Thomson, and Sinclair 2017). The strategies these partnering nations adopt in their collaborative efforts provide a plan for adequate research security. Steps that create shared standards, structures, and protocols can be promoted by developing countries as future operating procedures. The results of these collaborations create a fortified research environment where information and resources are exchanged more securely, thereby increasing the overall resilience of national research ecosystems.

The potential impact of multilateral efforts extends beyond the most immediate and basic concerns of research security. The more nations begin to collaborate, the more trust will grow. Increased efforts to maintain research security standards will become a mutual understanding, and joint research initiatives will become fluid. Global challenges can be met head-on in a collaborative effort. This synergy increases research skills and cultivates a diplomatic landscape anchored by shared goals and collaborative success. The results and implications for multilateral research collaborations in research security between the US, Canada, Japan, Australia, Brazil, and other developing countries become crucial to evaluate how these partnerships can adapt to the unpredictable nature of global threats and capitalize on emerging opportunities (Kundu and Gupta 2024). The exploitation of these dimensions not only informs practices in partnering nations but also offers information to the global community that faces a time when collaboration is integral to protecting intellectual activities against a constantly evolving risk scenario. (Gaviao, Dutra, and Kostin, 2021).

Development of Standards and Strategies

Multilateral efforts in the form of collaborations and consortia have been developed between Canada, Japan, Australia, and Brazil. This resulted in developing and implementing standard strategies to improve research security. At the center of these strategies are several agreements and protocols specifically adapted to reinforce the protection of sensitive innovations (Gaviao, Dutra, and Kostin, 2021; Canada 2024d). Collaborative frameworks facilitate the exchange of information regarding best practices and intelligence on entities that represent potential risks to research integrity (Gaviao, Dutra, and Kostin 2021). In the domain of export controls, these four nations have dedicated themselves to proactive dialogue to create a harmonized approach to regulate sensitive technologies. This includes the consultation and implementation of specific guidelines on AI and biotechnologies, which are considered dual-use technologies (Zhang *et al*. 2022; Antoni 2020). Canada, for example, has refined its export control laws to align with the initiatives of Japan and Australia about sensitive technologies, such as quantum computing, which may have commercial and defense applications (Canada 2024f). Brazil has adopted a complementary position by developing its regulatory frameworks in consultation with these partners, emphasizing the need for consistency in global standards to avoid the unauthorized transfer of such technologies (Zhang *et al*. 2022).

In addition, collective efforts to address the regulations surrounding the digital economy illustrate a commitment to strengthening research integrity (Larionva and Shelepov 2021). Japan has taken the lead in discussions about digital governance, focusing on the ethical use of IP data. Australia has contributed its experience in developing cyber resilience, aiming to equip researchers with the necessary tools to protect their work from cyber threats. The established digital research security protocols highlight this bilateral approach, ensuring that all member

nations are aligned in preserving the integrity of research data while continuing to encourage innovation (Larionva and Shelepov 2021). The strategic alliances forged among Canada, Japan, Australia, and Brazil provide a compelling multilateral collaboration model to enhance research security. Each associated nation contributes its strengths and innovations toward creating standards and policies that can help mitigate the evolving complexities of research in a globalized society. The results of this collaboration have impactful implications for the future of research security and broader global international scientific cooperation. The results of multilateral collaborations between Canada, Japan, Australia, and Brazil to advance research security reveal remarkable, measurable impacts on innovation, security, and knowledge sharing. Each nation has leveraged its resources to enrich its research programs while maintaining a robust security framework.

Impacts and Outcomes of Collaborations

Brazil, alongside its counterparts, has developed its unique position as a standard power to facilitate a platform for collaborative research initiatives. Efstathopoulos (2021) illustrates that Brazil has exploited its various research capacities to form partnerships that are focused on innovation by having improved security, which has led to the development of advanced technologies in fields such as cyber security and biomedicine, where collaborative projects not only prioritize security but also promote a joint spirit of innovation. The overall impact of these partnerships has created a trust that allows for the pooling of resources and expertise and the enhancement of their collective capacity (Efstathopoulos). This has led to policies and practices that facilitate the rapid dissemination of research results. This has been particularly relevant in security, as countries have shared best practices and lessons learned from their individual experiences. The transfer of knowledge inherent in these efforts plans to benefit from future

research initiatives, while nations are based on a multitude of shared intellectual capital. In addition, the importance of these collaboration efforts becomes particularly obvious in international peace operations. Christiansen (2021) notes that enhancing research security strengthens peacekeeping missions through improved operational efficiency and enhanced information sharing. Canada, Japan, Australia, and Brazil have collectively developed executives that allow a more coordinated response to world security challenges, ultimately contributing to international stability (Christiansen 2021).

Furthermore, the COVID-19 pandemic underlined the need for and the effectiveness of such collaborations in strengthening resilience to global crises. Briffa (2023) stresses that collaborative research responses to the pandemic presented the advantages of multilateral approaches. By pooling data, sharing research results, and coordinating research efforts on vaccines, these nations have had an overview of the attenuation of crisis impacts. There is a modern paradigm of scientific development where rapid innovation is ever-present, and security measures are needed to protect collaborative efforts from threats such as disinformation and economic espionage (Briffa 2023).

Multilateral collaborations in research security have progressed in innovation and knowledge sharing and demonstrated an increased capacity to manage global security challenges. By integrating their forces and effectively collaborating, Canada, Japan, Australia, and Brazil have established a model for future research cooperation that reinforces the idea that security and innovation are complementary forces that stimulate progress on several fronts. Future implications for research security best practices cultivated through multilateral collaborations among Canada, Japan, Australia, and Brazil hold considerable promise in addressing existing and emerging global challenges. As these nations continue to forge alliances and develop

sustainable objectives, it is imperative to continually evaluate the effectiveness of current practices and the potential expansion of these collaborations to cover broader safety, sustainability, and shared success (Campoli *et al*. 2025).

As countries navigate the complexities of economic insecurity, collaborating countries can achieve long-term security objectives through the standard protocols tied to funding for research initiatives. This is the common ground for maintaining and expanding their collaborative research agendas (Job 2022). Paulsen (2024) notes that breaking free from rigid political mindsets in international relations benefits global working partnerships. Populism and nationalism in partnering countries can block cooperation and lead to policies that prioritize individual countries' national interests at the expense of sharing knowledge and fostering innovation (Paulsen 2024). In the context of Canada, Japan, Australia, and Brazil, these countries should proactively promote a narrative centered on shared mutual benefits by promoting the value of research collaboration as a mechanism for addressing global crises. Future collaborations can be optimized using the latest digital technologies and platforms to improve communication and cooperation across various disciplines. The proliferation of digital platforms offers real-time information sharing, intercultural dialogue, and collaborative problem-solving opportunities.

In short, the continuous evolution of multilateral research collaborations among Canada, Japan, Australia, and Brazil can significantly impact future research security ventures. These collaborative nations can reinforce their partnerships and increase their collective resilience by strategically aligning their collaborative efforts and global sustainability initiatives and facing the newest challenges represented by economic insecurity and ideological structures. The examination of multilateral collaborations in research safety between Canada, Japan, Australia,

and Brazil reveals an intricate tapestry of strategies and results, highlighting the need for supported international cooperation. The collaborative initiatives established by these nations have produced better practices that can serve as exemplary models for future partnerships (Ordoñez de Pablos 2024). By sharing skills, resources, and methodologies, these countries have forged paths to improve safety protocols, encourage innovation, and cultivate resilience in the face of emerging threats (Ordoñez de Pablos).

The strategies identified in this analysis underscore the importance of adapting and responding to each nation's unique geopolitical and environmental contexts (Ordoñez de Pablos). An example of bringing Canada's attention to computer security aligns with Australia’s progress in protecting emerging digital infrastructures. At the same time, Japan's initiatives in disaster resilience contribute to the joint efforts in addressing challenges (Ordoñez de Pablos). Brazil has committed to a sustainable research security model, allowing for a bigger picture with localized knowledge. Integrating these strategies solidifies the multifaceted nature of research security and the need for an integrated approach across countries and sectoral institutions (Ordoñez de Pablos). The outcomes of these collaborations exemplify the tangible benefits of working together towards common objectives. In particular, joint research companies led to innovations in climate adaptation technologies, advanced the securitization of data-sharing processes, and facilitated initiatives that strengthened research capacity and security measures (Ordoñez de Pablos). These results exemplify effective multilateral partnerships and contribute to a collective competence that improves the global response to transnational challenges.

Supporting and expanding these multilateral collaborations cannot be overstated. The need for a unified approach to research safety becomes primary in these times of rapid technological progress and interconnection. The foundations laid by Canada, Japan, Australia,

and Brazil must evolve to continue confronting current issues and future vulnerabilities. Through collaboration, these nations can collectively navigate the complex and constant evolution of research security, ensuring that resilience remains in the face of emerging global challenges (Baylis, Smith, and Owens 2022). The path must be followed through a continuous dialogue, cooperation, and an unshakable commitment to advance the safety objectives of collective research (Hall 2020; Ordoñez de Pablos). Export controls represent one of the most well-defined and legally binding mechanisms among the various multilateral efforts to implement research security. They play a crucial role in research security by regulating sensitive technologies and innovation transfer.

Export Controls

Export controls are a regulatory mandate necessary to oversee the transfer of goods, information, and technology. Some of these exports are considered to be sensitive or dual-use materials. "A 'dual-use' material has civil applications as well as terrorism and military or weapons of mass destruction (WMD)-related applications" (BIS 2025). Securing exports is imperative to the non-proliferation of information and technology that could be used in a military capacity. Securing exports also protects nations economically. Many countries also seek to grow their international relations through agreements and trade partnerships, doing their part to protect the world from malicious actors. "The US government must limit the possibility of sensitive items falling into the wrong hands while allowing legitimate trade. Achieving this balance, however, has become increasingly difficult due to redefined security threats and an increasingly globalized economy. The export control system is a key government program to balance US interests" (GAO 2005). The US has dramatically invested in research and security over the last decade. This growing investment in sensitive research must be protected with proper export

controls and mandatory reporting. The US seeks to improve collaboration with its partner nations and is aiming to strengthen its research security strategies to ensure economic and national security (Flagg, Toney, and Harris 2021). Export control has several key agencies and regulations that seek to guide and protect national interests. These agencies have various compliance agreements and responsibilities outlined in federal oversight reports (GAO 2008). However, audits have shown that the US export control system still suffers from vulnerabilities and inefficiencies in the context of national security after 9/11 (GAO 2005).

While there is no perfect system of export controls, this will continue to be an elemental tool in research security that developing countries must include in their toolbox. Regulatory frameworks assist with the basic structure to formulate a system of operative export controls.

Agencies and Regulations

The export control ecosystem is subject to many regulations and reports to several agencies that monitor US exports, including the Departments of State and Commerce. While the State regulates arms exports, the Commerce Department regulates dual-use exports that can provide military and civilian functions (GAO 2005) through the BIS. These agencies focus on risk profiling and screening exports (Van Der Molen 2023). The BIS regulates export, re-export, and domestic transfer of commercial use with dual-use capabilities through the Export Administration Regulations (EAR). Some of these dual-use capabilities include conventional arms, WMD, terrorist activities, human rights abuses, and other military materials (BIS n.d.). BIS strives to advance national security, foreign policy, and economic objectives by ensuring effective export control, treaty compliance system, and technology guidance. (ITA 2025). It also oversees US laws, regulations, and policies that control the export and re-export of commodities, software, and technology under the jurisdiction of the EAR (ITA 2025). The EAR creates the

Commerce Control List (CCL) and ensures that materials meet the export licensing requirements, including Export Control Classification Numbers (ECCNs) required by the Department of Commerce (BIS 2024).

By coordinating various legislative and executive actions, such as the International Traffic in Arms Regulations, the Directorate of Defense Trade Controls (DDTC) secures commercial exports of defense materials and services to ensure they advance US national security and international relations (State n.d.-b). The DDTC works with the Defense Trade Advisory Group (DTAG) to coordinate across the defense and private sectors and offers communication channels between US private sector defense exporters and specialists in defense trade (State n.d.-a). Further structure is provided by the Office of Foreign Assets Control (OFAC) under the US Department of the Treasury, which administers and enforces economic and trade sanctions to comply with foreign policy. OFAC pays attention to countries, regimes, and terrorists engaged in the proliferation of weapons of mass destruction and other threats to the US (OFAC n.d.) International efforts are becoming increasingly consequential as dual-use technology advances rapidly. For example, the Missile Technology Control Regime (MTCR) is an informal agreement to apply authorization requirements when exporting products on its list (State n.d.-c). Another multilateral group that plays a prominent role in preventing proliferation is the Nuclear Suppliers Group (NSG), which controls nuclear-related exports to ensure they are not used for weapons development (Nuclear Suppliers Group n.d.). In addition, there is a voluntary export control group called the Wassenaar Arrangement that seeks to provide transparency for exports by exchanging information which offers "greater responsibility" to prevent "destabilizing accumulations" (Kimball 2022, para. 1). These collaborations and

agreements support transparency and responsible use to assist with international security and stability.

Compliance Requirements and Enforcement

Adhering to and enforcing compliance requirements is central to maintaining a successful export control program. Following the CCL for end-use materials, production equipment, materials, software, and technology is mandatory (BIS 2024). These products are categorized and given specific designations on the CCL to identify the materials based on their type and technical use (BIS 2024b). These categories focus on dual-use technology that can be applied in military and civilian organizations. An effective export control by the US Department of Commerce is the use of deemed export licenses that are required to transfer dual-use technologies to citizens from countries outside the US, as well as the Department of State's requirement for foreign nationals to have special visas when working in engineering, computer science, and biotechnology (GAO 2011). There are also restrictions on specific countries and sanctions for certain materials. OFAC restricts the export of dual-use materials to Russia, Iran, North Korea, Cuba, China, Venezuela, and others in efforts to mitigate the proliferation of sensitive data and technologies. The US Munitions List (USML) has export restrictions. The BIS has a division that enforces the EAR called Export Enforcement (EE), which partners with US embassies, external governments, industry, and trade associations to keep exports secure, conduct site visits known as end-use checks, and verify compliance with regulations (ITA 2025). These brief descriptions demonstrate the importance of nations in securing vulnerable materials and technologies.

Export Control Best Practices and Challenges

Export control regarding research security has many challenges to overcome, and following best practices helps mitigate some of these challenges to protect sensitive research. Utilizing strict research security protocols is rewarded. The US NIST grants funding to those institutions that implement cooperative agreements and disclosures in programs related to bioscience, manufacturing, and other technologies, which are increasingly at risk of exploitation by approaching quantum computing advancements (GAO 2023). Data analysis, such as that provided by the Office of Technology Evaluation, can guide educators in understanding what is at risk of being exploited through a review of license application data and data trends of global trade (ITA 2025). Recent advancements in research security have occurred, such as the development of the SECURE Center, which stands for Safeguarding the Entire Community in the US Research Ecosystem. The NSF invested $67 million to protect technology like semiconductors from malicious actors. It is expected to help organizations establish research security practices more easily (Mervis 2024). This program also hopes to standardize how universities handle research security. The NSF will award Texas A&M University $17 million for SECURE Analytics over the next five years. "TAMU had submitted its proposal to lead the SECURE program," says Dr. Kevin Gamache, chief research security officer for the TAMU system. "But after the selection [of UW] was made, NSF approached us and offered us the chance to use our strength in data analysis and tools," says Gamache, who will direct the analytics center (Mervis 2024).

Failure to comply with regulatory export controls can lead to severe consequences. Organizations must adhere to guidance, mandatory reporting, and licensing to ensure compliance, mitigate risk, and help preserve their economy and national defense. Research

security is growing and needs to be prioritized when exporting or collaborating with other institutions and organizations. The goal is to maintain collaboration and access while also implementing sufficient restrictions to prevent sensitive data from falling into the hands of those with malicious intent.

While understanding the theoretical frameworks and regulatory structures of research security is essential, analyzing real-world examples gives insight into practical implementation strategies. The following case studies illustrate how various institutions and countries have addressed research security challenges, highlighting both successes and failures.

Case Studies of Academic Research Security Incidents

Researching security approaches across different countries provides valuable insights into practical implementation strategies. These examples highlight both successes and challenges in balancing security with academic freedom. The following case studies examine both positive examples where institutions successfully implemented research security measures and negative examples where security failures led to compromised research integrity, IP theft, or other adverse outcomes.

Building Institutional Capacity

Academic Research Security Success

The UK university case study demonstrates the successful implementation of robust due diligence processes when evaluating research partnerships. When a faculty member was invited to collaborate on a project backed by a UK-registered company with considerable research funding, the university's due diligence revealed that the company's overseas owner was a state-owned manufacturer with ties to military shipbuilding. Recognizing the security implications, the university made the prudent decision to withdraw from the partnership (UUKI 2024).

The university's approach to managing such risks included conducting in-depth background checks and sharing findings with faculty to heighten awareness. This proactive approach illustrates how effective due diligence processes, proper training procedures, and strict partnership evaluations can safeguard research integrity before security breaches occur (UUKI 2024).

Australia's response to the ANU cyberattack provides another positive example of building institutional capacity after a security breach. Following the attack, ANU responded by overhauling its cyber security protocols, enhancing encryption, expanding staff training,

strengthening multi-factor authentication, and releasing a public report outlining lessons learned, contributing to sector-wide awareness about cyber security risks (ANU 2019). This transparent approach to addressing security failures represents a constructive model for institutional responses to security incidents.

Academic Research Security Failure

The ANU cyberattack itself represents a negative example that exposed institutional vulnerabilities. In 2019, ANU's central systems were breached, allowing hackers to access personal and academic data from 200,000 students, staff, and researchers (Sarraf 2019). The breach was likely initiated through a phishing attack, exposed sensitive information, and raised serious privacy and security concerns (ZDNet 2019). This incident revealed inadequate preventive security measures and highlighted the vulnerabilities that many research institutions face without proper cyber security infrastructure.

In the UK, another negative example emerges from cases where universities unknowingly partnered with Chinese institutions whose collaboration could benefit China's military (Hayward 2021). These collaborations initially appeared to support academic advancement but eventually sparked national security concerns (UK FAC 2019). This situation revealed insufficient screening processes for international partnerships and inadequate awareness of the potential security implications of specific research collaborations.

Managing Foreign Influence

Academic Research Security Success

The Dutch government's response to foreign influence provides a positive example of managing security risks. After identifying concerning influence patterns, the Dutch government took decisive action by reassessing externally funded academic programs, which led some

universities to cut ties with Confucius Institutes. Additionally, the government introduced national security measures to monitor foreign influence in higher education (d'Hooghe and Decker 2020). This systematic approach to addressing foreign influence demonstrates how government oversight can support institutional security efforts.

Another positive example comes from Dutch intelligence successfully disrupting a Russian espionage operation. In 2020, Dutch intelligence identified and countered an operation in which Russian officers, working under diplomatic cover, attempted to steal sensitive research in AI, semiconductors, and nanotechnology (Ollongren 2020). Once discovered, the Dutch government expelled the officers and tightened counterintelligence efforts (Ollongren). This case demonstrates effective collaboration between intelligence services and the academic sector to protect sensitive research.

Developing comprehensive disclosure requirements in the US is a constructive response to concerns about foreign influence. Following several high-profile cases, universities began working with the federal government to devise systems and guidance to identify, analyze, and mitigate threats to research security (GAO 2020). These efforts include implementing conflict of interest policies and requiring disclosure of external affiliations, associations, activities, and research support (GAO 2020). These systematic approaches to transparency help protect research integrity while allowing beneficial international collaboration to continue.

Academic Research Security Failure

The Netherlands' experience with Confucius Institutes illustrates the negative impacts of unchecked foreign influence. Reports revealed that some Dutch academics avoided politically sensitive topics, such as human rights issues in Xinjiang and Tibet, to preserve access to Chinese partnerships and funding (d'Hooghe and Decker 2020). Other researchers faced travel restrictions

or visa denials when pursuing critical research involving China if they had worked on politically sensitive topics (d'Hooghe and Decker). This case demonstrates how external funding can compromise academic freedom and research integrity when safeguards are not in place.

The Harvard Professor Dr. Charles Lieber case represents one of the most prominent negative examples of undisclosed external influence. Dr. Lieber, former Chair of Harvard's Chemical Biology Department, concealed his connection with the Wuhan University of Technology, his participation in China's Thousand Talents Program, and his substantial income from these affiliations (VT 2024). As part of his arrangement, Dr. Lieber reportedly received a salary of up to $50,000 per month, living expenses of up to $150,000, and more than $1.5 million to create a research lab at the Wuhan University of Technology (El-Bawab 2023). His failure to disclose these relationships violated university and federal policies, resulting in criminal charges and damaging institutional trust.

Balancing Collaboration and Protection

Academic Research Security Success

Japan's comprehensive guidelines for international research exchange provide a model for maintaining productive collaboration while protecting sensitive information. The Japanese government has developed detailed policies addressing research integrity concerns, including guidelines and checklists highlighting the elimination of irrational overlap or excess concentration and strict responses to illegal receipt and use of research funds (Japan 2021).

Japan has also established practical support systems, including a help desk for consultation, risk education and training, risk monitoring systems, risk comparison reports, research transparency reports, and risk assessment processes when an external organization's risk

level changes (Japan 2023). These approaches allow Japanese institutions to collaborate with international partners while maintaining appropriate security measures.

A US research institution successfully adhered to government laws and regulations for sensitive research and, in so doing, continued to enjoy access to grants from the federal government (Gardner *et al*. 2022). In its defense-related study, the institution embraced a comprehensive security program with regular compliance audits, personnel training, and access controls. The institution avoided penalties by proactively addressing its weaknesses and compliance with laws for controls over exporting, and its access to federal funding continued unimpeded. Not only did its proactive compliance protect its research, but it also consolidated its position as a responsible and reliable collaborator. The case study reaffirms compliance with a security program for research in managing a complex legal and regulatory environment. It enables an institution to preserve its key purpose of driving innovation and expanding knowledge.

Canada's response to the case involving virologists at the National Microbiology Laboratory demonstrates a positive example of balancing security with scientific collaboration. After identifying security concerns related to the transfer of virus samples to the Wuhan Institute of Virology, Canadian authorities implemented enhanced physical security, cyber security, and staff awareness training and reinforced international collaboration policies (Canada 2024c). The government also developed recommendations for expedited security clearance vetting, establishing a list of trusted countries for research sharing, and updating national security policy (Canada 2024c). These measures show how countries can maintain valuable scientific collaboration while implementing appropriate security protocols.

Academic Research Security Failure

Brazil's approach to research integrity reveals sizable gaps in security infrastructure despite extensive international collaboration. Results from a study of Brazilian research institutions indicate that only twenty-eight percent of the sixty institutions surveyed had developed guidelines or adopted documents regarding research integrity, while thirty-six percent were either working to implement or lacked official guidance on research integrity (Armond and Kakuk 2021). Only nine research organizations had established research integrity offices or committees (Armond and Kakuk). This lack of formal security infrastructure creates vulnerability despite Brazil's increasing international research profile.

The case of Canadian researchers collaborating with Iranian institutions on drone technology highlights the risks of insufficient oversight of dual-use research. This collaboration raised concerns about potential violations of international sanctions, as the research, though framed as civilian, had clear military implications. Investigations revealed that some partnerships had bypassed proper oversight, prompting the Canadian government to tighten guidelines on international collaborations (Fife and Chase 2022). This case demonstrates how inadequate scrutiny of research partnerships can lead to serious security and compliance issues, particularly in fields with dual-use applications.

The case studies demonstrate that research security is not just a theoretical concern but a real-life challenge that requires real solutions. The juxtaposition of positive and negative examples helps identify lessons and best practices.

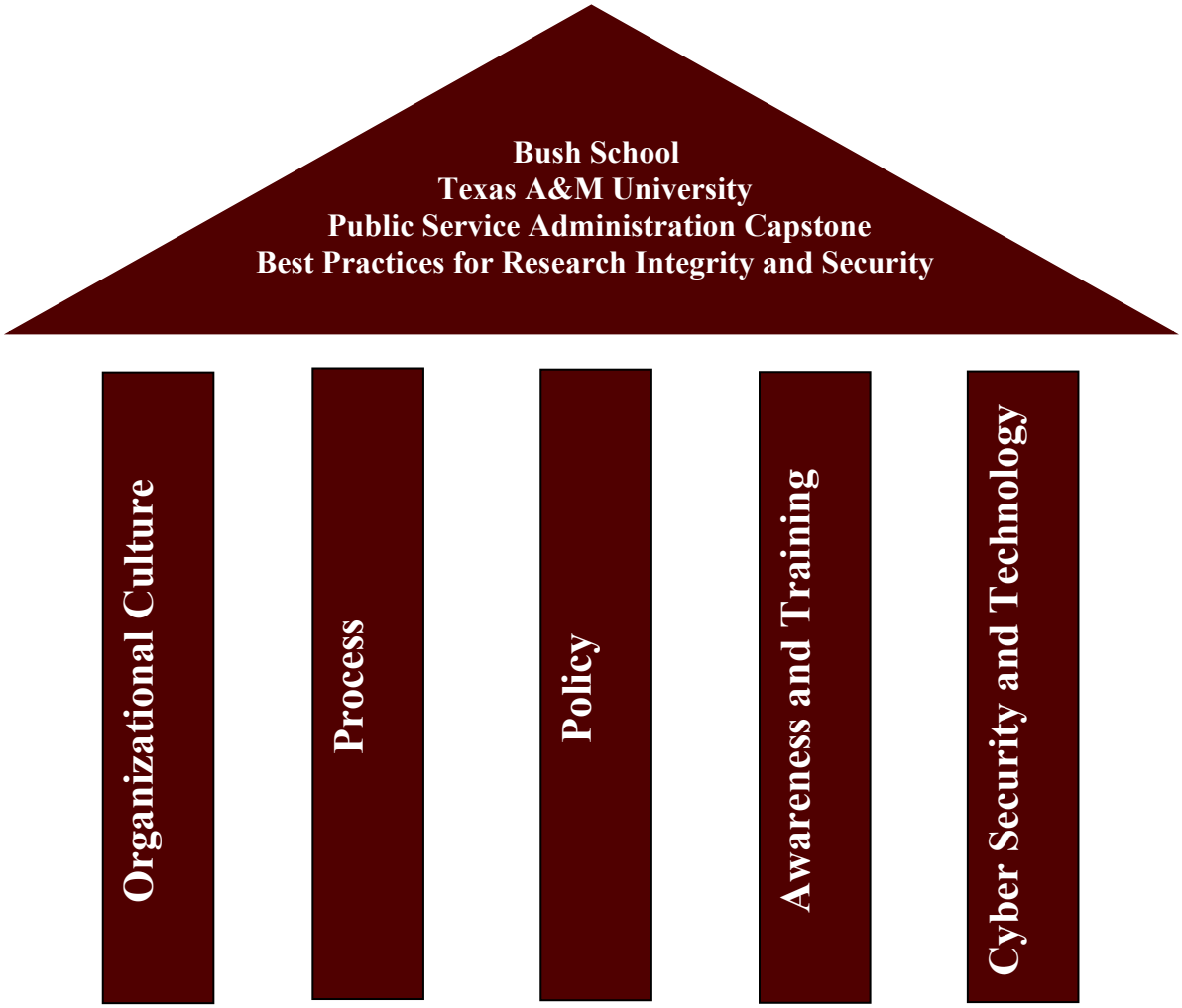
Lessons Learned from Case Studies for Best Practices and Recommendations

The case studies examined in the previous section, both positive and negative, reveal several valuable lessons for research security implementation:

1. **Proactive due diligence**: The UK university example shows the value of thorough background checks on potential research partners before collaboration begins.
2. **Robust cyber security infrastructure**: Australia's response to the ANU breach demonstrates the importance of comprehensive cyber security protocols, encryption, and multi-factor authentication.
3. **Transparent disclosure requirements**: Dr. Lieber's negative example highlights the necessity of clear disclosure policies for external affiliations and funding.
4. **Collaboration between governments and universities**: The Dutch and Canadian examples show how cooperation between government agencies and academic institutions strengthens research security.
5. **Dedicated security resources**: Japan's help desk and risk assessment systems illustrate the benefits of dedicated infrastructure for research security.
6. **Ongoing security training**: Multiple examples emphasize the importance of security awareness training for researchers and staff.
7. **Balanced approach to international collaboration**: Japan's framework demonstrates how countries can maintain productive international relationships while implementing appropriate security measures.

The negative examples in these case studies often led to positive reforms, showing that adequate research security can emerge from learning from mistakes. However, as seen in Japan's comprehensive approach, proactive measures can prevent security breaches before they occur.

Best Practices Guide - Embracing the Benefits of Research Security



Recommended Best Practices

Protecting IP and sensitive data is a significant benefit of an academic research security program. Educational communities are at the forefront of breakthroughs and technological advancement, making them ideal targets for abuse and theft. The protection of such advances is vital for national security, competitiveness, and the success of academic institutions (Komljenovic and Williamson 2024).

The foundations of any research security program are academic integrity and trust. The literal definition of integrity may vary slightly, but the generally accepted meaning is rooted in

six fundamental values: honesty, trust, fairness, respect, responsibility, and courage (ICAI n.d.). Trust leads to successful collaborations. Institutions and researchers lay the groundwork for trust alongside funding agencies, collaborators, and society by demonstrating a commitment to ethical practice and responsible information management. Academic integrity is the cornerstone for building productive relationships and advancing scientific development.

The reinforcement of an institutional research security program is compliance with laws and regulations. Most countries have rules and regulations protecting sensitive research, especially in countries with national security concerns. Institutions that fail to adhere to such requirements can suffer severe consequences, including penalties, lawsuits, and the collapse of government funding support. While research security plans and programs may vary across organizations, this paper's best practices will fortify cyber security, physical security, personnel security, data management and sharing, export controls, conflict of interest and commitment disclosure, travel disclosures, and foreign influence mitigation.

The best practice areas are organized into five pillars. These pillars outline "countermeasures" that every institution should strive for and are based on published academic security research "solutions" (Tiffert 2020, p. 118). The best practice pillars build upon each other, contingent on the program's maturity and institutions' financial limitations. A comprehensive research security program will include all five pillars. The pillars represent the foundation upon which any Academic Research Security Program must anchor itself, extending the structural perimeter of the program.

I	II	III	IV	V
Organizational Culture	Process	Policy	Awareness and Training	Cyber Security and Technology

Pillar I – Organizational Culture

Foster a Culture of Security

A successful research security scheme entails technical controls and a security-conscious culture among researchers and staff. Since researchers are the first line of defense, it is beneficial to encourage the researchers to own security controls. Institutions can make them owners through training and tools that enable them to detect and respond to security vulnerabilities (Olweny 2024). Promoting transparency and sharing security threats develops a security awareness culture. Institutions must promote open discussions about emerging security concerns and periodically issue updated security policies and best practices. Institutional forums, newsletters, and web portals can inform researchers about emerging security concerns and offer methods to respond to them effectively. Institutional reporting channels for security concerns must be in place, and researchers must be assured of whistleblower protections. Transparency and communication build confidence and stimulate collaboration to develop a secure environment for research.

Implementation

Implementing an academic research security plan requires careful consideration of the institution's organizational culture. The culture will significantly impact how security countermeasures are received, adopted, and maintained. Many organizations must undergo organizational paradigm shifts to execute successful research security programs. They need a culture of shared responsibility at all levels of the organization. While there are several fundamental areas, each organization's research security program should be customized to the institution’s needs, focusing on the type of research being conducted.

Balancing open research with security can be challenging, particularly when seeking buy-in from academics who value autonomy. Successful research security programs must have acceptance from the entire research ecosystem, including managers, researchers, staff, and administrators. Research security policies should not be overly burdensome, but must protect sensitive research areas. Researchers often prefer to spend time conducting research rather than being obligated to perform additional administrative tasks and responsibilities, such as research security protocols. It is imperative to convey the need to follow research security practices by describing the risk of IP theft, which researchers aim to avoid.

Leadership

One of the first examples of the necessary culture shift is having organizational leadership demonstrate a strong commitment to research security by investing in training, resources, and technology. Stakeholders at HEIs, including administrative leadership, faculty, staff, and students, may not be aware of how their activities align with strategic state interests to expand their influence on the global stage.

A distinct disparity exists between external governments pursuing legitimate, declared educational interests and those pursuing subversive, undeclared, coercive, or criminal activities. It can be challenging for educational stakeholders to distinguish between them. Additionally, this group of stakeholders is typically not involved in national defense and may not realize their role aligns with national security, dual-use research, and malign foreign influence. When senior faculty and administrators lead by example, the security culture is likely to positively impact the organization. Security policies should be consistently communicated and reinforced through internal memos, meetings, and academic forums to maintain high levels of awareness and compliance.

Safeguarding International Travel

While international research collaboration is vital, research institutions must be vigilant about the risk of foreign interference when traveling outside their national borders. As this paper has described, the threat to an institution's IP is higher when its personnel carry the information during normal travel activities (Resnik 2020). International travel should be preapproved and subject to disclosure (Cornell 2024). By instituting disclosure protocols, institutional leadership can guide researchers when areas of concern flag a potential threat.

In addition, institutions should consider utilizing a short-term loaner device program for cell phones, laptops, and USB drives for any personnel traveling internationally. Doing so ensures that only the minimum institutional data is carried, which reduces the risk should the device be seized by immigration officials or stolen (Calgary 2025). Implementing a loaner laptop program also helps protect the researcher and the institution should malware be introduced surreptitiously while accessing public wireless networks, computer workstations, or charging stations during international travel (Calgary).

By creating a culture that prioritizes transparency in international travel, an institution demonstrates its trustworthiness and holds its researchers to high standards. This includes reporting all international travel and ensuring that only cleared and dedicated technological devices are used during international travel.

Pillar II – Process

Best practices for research security include processes that minimize risk by broadcasting the presence of security programs, assessments, audits and reviews, training, and diligence in international collaborations. Most guidelines agree that defined processes are necessary to protect the organization's and individuals' research. The level and intensity of security vary from organization to organization and project to project, shielding sensitive research while promoting collaboration between trustworthy researchers. Research security processes are essential when protecting susceptible programs, products, patents, and academic exploration. Working with industry partners and government agencies while implementing organizational policies and procedures minimizes risk (NPSA 2024; OECD 2023).

Processes are key to creating a foundation for research security. Training and implementation are at the forefront of an organization's ability to protect its research. A security program should include training on risk analysis for the ethical responsibility of research, risk minimization with an emphasis on secure data collection, and the moral responsibilities of researchers, promoting research self-regulation (Leopoldina 2022). Training and policies should highlight researchers' legal and ethical obligations while promoting open, transparent, and ethical research practices. Balancing open research with research security processes is a fundamental best practice observed by many organizations.

Collaboration with private and government sector partners gives an institution access to external expertise and assets. Government agencies may issue guidance, funding, and tools to enable institutions to secure their research, particularly in regions with national security implications. Industry partners can contribute to research security where academic and commercial use overlap. Industry collaboration can provide institutions access to state-of-the-art

security technology and intelligence on emerging threats and best practices (Thakur 2024). Furthermore, institutions involved in international research security consortia gain access to a pool of expertise to improve their security posture.

Tailored Security Process

Tailored programs create non-intrusive processes that align with the individual risks and requirements of institutions and research projects (OECD 2022). Institutions should implement research security programs tailored to their unique needs and risk profiles. Willoughby (2024) demonstrates how research institutions benefit from customized security programs. These include sponsoring security clearances and meeting specific compliance requirements of defense-related research. The OECD (2022) also recommends creating non-intrusive protocols that align with the particular risks and requirements of individual institutions.

Research Security Offices (RSOs)

RSOs provide the necessary expertise to execute research security while preserving institutional autonomy and achieving buy-in from researchers (OECD 2022). Establishing dedicated research security offices at the national and institutional levels is an effective way to ensure acceptance. Countries that develop national offices can assist research institutions in navigating security risks and provide expertise to obtain concurrence from researchers (OECD 2022).

Pannier also notes that France has centralized its research security and the prime minister's office, managing sensitive sectors like engineering and biotechnology (2023). The University of Adelaide also highlights the importance of a research security office that oversees compliance with foreign influence reporting and security clearance requirements (Willoughby

2024). In addition to these responsibilities, research security offices are responsible for managing awareness, training, policies, and procedures for research security (UTHealth Houston 2024).

Whether a given research security office comprises a team of people or a single individual dedicated to the research security framework, having an RSO takes the burden off the researcher when undertaking training, due diligence, and governmental compliance. RSOs are not implemented to stifle international collaboration, yet they allow researchers to enter with their eyes wide open.

International Collaboration with Clear Security Guidelines

Although international collaborations are fundamental for research, it is clear that security guidelines must be implemented to mitigate risks. Pannier points out that the EU has moved toward a more security-conscious approach, focusing on collaborations with trusted allies while maintaining safeguards to protect sensitive research (2023). The OECD also advises that clear, enforceable security guidelines are necessary to manage the risks of international research collaborations, especially in critical technologies (2022), as noted by CISA. Shih backs this approach by indicating that flexible, context-specific security policies allow institutions to navigate geopolitical friction without compromising research and security (2024).

Institutions should be aware of sanctions by performing open-source research to comply with regulations by entities such as the US Office of Foreign Assets Control (OFAC), the US Department of Commerce's Bureau of Industry and Security (BIS), and the United Nations, or governments with robust academic research security regulations such as the European Union, United Kingdom, and Japan (C4ADS 2024).

Due Diligence in International Collaborations

The UK Research and Innovation (UKRI) recommends using a risk-based approach, tailoring the due diligence process to the level of risk involved in each collaboration. This includes reviewing financial stability and ethical standards through various due diligence questionnaires (UK Research and Innovation 2023).

Due diligence must be conducted thoroughly before entering research partnerships. This includes reviewing financial stability and ethical standards through various due diligence questionnaires (UKRI 2023). Another British institute ensures ongoing monitoring throughout the project to mitigate security threats (Lancaster University 2023). Investigative service tools are available to assist with due diligence, such as the CSL Search Engine, which filters a consolidated screening list to search for data on entities and comply with regulations (ITA 2024), or Finch Analyst by FinchAI, which filters based on activity, region, and relationships (2025).

Mandatory Disclosures and Reporting

Mandatory disclosures offer transparency and are considered an essential best practice. The OECD encourages clear policies for disclosing conflicts of interest and commitment, with checklists to aid compliance (2020). Cornell University requires that all foreign activities and partnerships be disclosed and preapproved, particularly those involving countries of concern, such as China and Iran (Cornell University 2024). Research security protocols can be organized through effective cross-coordination and centralized reporting, which allows protocols to be consistently applied. The Association of Public and Land-Grant Universities (APLU) highlights the need for working groups that integrate research, cyber security, and legal teams to manage security risks effectively (2020). Establishing a centralized reporting system ensures that security threats are identified and addressed promptly across different departments (APLU 2020). Cornell

University also implements a centralized reporting process, requiring all international collaborations and travel to be preapproved and subject to disclosure (2024). The National Science and Technology Council (NSTC) and NIST provide forms so organizations can regularly monitor conflicts of interest to make sure potential risks are identified early (NSTC 2021, Strouse *et al.* 2023). In addition, training modules for disclosures are available to assist with safeguarding from exploitation (NSF Research Security Training 2024).

Risk Assessments

Continuous and comprehensive risk assessments must be made throughout the life cycle of any research project. UKRI advises that risk assessments should not be a one-time activity. They should be done regularly to identify and respond to dynamic risks, especially during major international research collaborations. Canada's research security guidelines include risk assessments as a core component of research security, offering scenario-based assessments to help researchers better understand and respond to security threats (Canada 2024e). Lancaster University similarly stresses the importance of ongoing risk monitoring to ensure that any vulnerabilities are promptly identified and mitigated (2023). Canada's research security guidelines also include risk assessments as a core component of research security, offering scenario-based assessments to help researchers better understand and respond to security threats (Canada 2024b).

Security Audits and Reviews

UKRI recommends frequent audits of security practices, particularly data-handling partnerships, to ensure institutions comply with national and international regulations (2023). Regular security audits will improve the effectiveness of security protocols and identify potential weaknesses. UKRI recommends frequent audits of security practices, particularly data-handling

partnerships, to ensure institutions comply with national and international regulations (2023). Lancaster University also conducts regular audits as part of its due diligence process to help mitigate the risks associated with ongoing international collaborations (2024).

Export Control and Compliance

Preapproving foreign contacts or interactions is a crucial step for technologies or intellectual property that are sensitive or controlled (Cornell University 2024). Institutions must comply with national export control regulations to prevent the unauthorized transfer of sensitive technologies or information. Cornell University provides comprehensive guidance on export controls, particularly in collaborating with countries of concern, such as China and Iran (2024). The primary steps are to preapprove international contacts or interactions related to technologies or IP that are sensitive or controlled (Cornell 2024), as well as to maintain and observe export controls and procedures for adhering to these (Imperial College London 2023). The National Academies of Sciences, Engineering, and Medicine's National Science, Technology, and Security Roundtable recommends working with HEIs that establish research security and research integrity programs, rather than focusing on a specific country or group of countries. What becomes a country of concern in the future may not be on the list today (Hagan 2025).

Anonymous Reporting Tools and Whistleblower Protections

Institutions should establish anonymous reporting tools that allow staff to report potential security threats without fear of retaliation and with transparency. Hardwick and Strickland argue that anonymous reporting systems and whistleblower protections are essential for fostering an open and secure research environment (2022). Providing research with anonymous reporting channels allows employees to report incidents, breaches, or security concerns safely. Canada's

research guidelines support anonymous reporting systems to help identify potential threats while protecting those who report issues (Canada 2024).

Scenario-Based Training

Case study scenarios can include cyber risks, talent and recruitment program risks, insider threats, failure to follow procedures, and travel risks (Canada 2021). These research security guidelines emphasize using case studies and scenario-based training as best practices for improving the researcher's ability to identify vulnerabilities, particularly in cyber security and international collaborations (Canada 2024b). Clark's article on research security suggests that scenario-based training can also help shift the academic community's mindset from reactive to proactive about the risks they face and how to mitigate them (2024). Scenario-based training will give researchers the best tools to recognize and respond to security threats.

Cyber Security Process

A robust cyber security process is essential for protecting sensitive research data. The National Knowledge Security Guidelines released by the Netherlands provide a comprehensive framework for safeguarding against cyber threats, including regular assessments of cyber security measures (Netherlands 2023). Canadian guidelines highlight the need to protect "IP from foreign interference and espionage" and advise organizations to maintain control over their IP, particularly when it is vulnerable and could compromise Canada's national security interests (Canada 2024).

Pillar III - Policy

Developing and implementing policies at the organizational level is a central pillar of the research security best practices. This creates standardization, defines expectations, ensures consistency, and manages risk through accountability, insulating an organization from malign foreign influence. Designed to assist organizations across various economic landscapes, implementing the following policy recommendations has been sufficient to protect sensitive research areas without imposing hardship on researchers or research security officers.

Implementing an effective security program for research begins with developing an institution-specific security framework regarding individualized vulnerabilities and needs. First, key research areas must be prioritized for heightened protection, including national security-related fields, such as AI, quantum computing, and biotechnology, and sensitive-data-related research, such as patient information and proprietary technology. By prioritizing and deploying security controls based on the level of vulnerability and sensitivity, an institution can effectively safeguard sensitive research without compromising collaboration in less sensitive areas (Mai, Bui, and Thai Pham 2024). Once critical areas for investigation have been identified, institutions must have definite processes and policies for safeguarding information. Policies must specify the roles of administration, staff, and researchers in protecting sensitive information and have protocols for the secure handling of information. Policies can have requirements for safeguarding information through encryption, secure communication channels, disclosure of potential conflicts of interest, and regular security audits. Definite reporting and response processes for security incidents must be established to mitigate loss and prevent future events. By developing a strong security infrastructure, institutions can build a comprehensive model for research security that addresses vulnerabilities and complies with relevant laws and regulations.

Building a Tiered Research Security Capability

Establishing a dedicated research security policy at national and institutional levels offers a tiered approach for research security programs and allows the research ecosystem to maintain open data exchange. Survey results from 2017 indicate that 58 countries have "dedicated national strategies" (OECD 2021, p. 4), which should be considered a beneficial layer to reinforce research security at the academic level. Support from the government will help researchers navigate the paradigm shift from transparency, openness, and the international data exchange to the increasingly political nature of international academic cooperation. Adding research security offices at the institutional level to those at the governmental level will provide an additional layer of security and encourage adherence to research security protocols.

Frameworks for International Travel and Collaboration

Although international collaborations are fundamental for research, security guidelines are necessary to mitigate risks. The OECD advises that clear, enforceable security guidelines are essential to manage the risks of international research collaborations, especially in critical technologies (2022). International sanctions should be continually monitored as a consequence of malign foreign influence. Open-source research can develop an awareness of past and current sanctions imposed by global governing entities. Additionally, proximity to foreign individuals providing research assistance on any academic level of effort should be considered.

Mandated Faculty Disclosures

The OECD encourages clear policies for disclosing conflicts of interest and commitment, with checklists to aid compliance (2020). Training modules should be developed to assist researchers in identifying circumstances that require disclosure and safeguard them from exploitation.

Pillar IV – Awareness and Training

Building a strong research security program begins with ensuring that everyone involved understands the importance of safeguarding IP and maintaining research integrity. Developing effective awareness and training programs is essential to promote a security-conscious culture within academic and research institutions. When researchers, staff, and students are adequately trained, they are better equipped to identify potential threats, comply with security standards, and protect sensitive data while encouraging valuable international collaborations. Well-structured training, offered regularly, will help institutions stay ahead of evolving threats and make research environments more resilient (UT Health 2024).

The US has mandated a more formal approach to research security to protect the country's intellectual property. National Security Presidential Memorandum 33 has directed that all institutions with research security programs that meet specific criteria must provide training to personnel on threat awareness and identification (Maryland 2025). Creating awareness and training programs is key to ensuring that researchers adhere to the policies and procedures outlined by research security programs. These programs are basic approaches to educating researchers and can be executed using flyers, PowerPoint briefings, or online training. They should cover all of the best practices discussed previously. This training should be provided to researchers, staff, and students, as it can help shift the culture and mindset of the institution (UT Health Houston 2024).

Coordination across various departments is required for an institution to have an effective research security program (APLU 2020). Collaboration between legal teams, IT departments, and research security offices creates a unified risk management approach. Regular inter-departmental training sessions will help everyone stay aligned while executing biannual sessions,

sharing reports, and maintaining institutional databases, which helps provide consistency and an improved framework.

Training Materials

Training materials should be provided in a diverse array to engage the researchers. Optional formats include hard-copy flyers, PowerPoint presentations, interactive online training modules, practical scenario exercises, and in-person classes and briefings.

Training Completion Tracking

Utilizing reliable tracking systems that incorporate detailed logs, centralized databases, and automated reminders will help institutions maintain compliance with research security policies. This type of setup will make it easier to identify areas that need improvement and ensure that training efforts remain effective and current.

Tailored Security Training Programs

For research security to function properly within an institution, training programs that fit the institution's needs must be created. Customized programs focusing on compliance requirements, unique vulnerabilities, and sponsor-specific guidelines tend to be more effective. Scenario-based training is beneficial because it helps researchers prepare for real-world threats (OECD 2022). Research Security Offices may develop these programs with input from department heads and external experts. Training sessions should be held at least biannually, with extra sessions scheduled as new risks or guidelines arise. Staff, faculty, and student progress and participation can be tracked using sign-in sheets, online systems, or certification processes.

Consistency Provided by the Research Security Office

Setting up dedicated research security offices at national and institutional levels will make training efforts more consistent and streamlined. These offices coordinate training

modules, create guidelines, and monitor compliance (UT Health 2024). Central coordination will also help keep protocols clear and effectively applied across the institution. Security administrators, IT departments, and compliance officers often lead these efforts, and training should be part of the onboarding process for new researchers. Research security personnel should document the completion of all training and compliance with policy.

Awareness of International Collaboration Standards

Training for international collaborations should emphasize staying cautious when working with global partners and protecting sensitive information. Research Security Offices, compliance units, or collaboration managers will be responsible for handling this training. Reviewing and updating training materials annually will help institutions adapt to changing geopolitical situations. Collecting feedback and documenting sessions will make refining and improving the training process easier.

Export Control Compliance Training

Ensuring researchers understand export control regulations helps prevent the unauthorized sharing of sensitive technologies and information. This training may involve compliance, department heads, or research security officers. Holding annual sessions with follow-up refreshers after policy updates will keep everyone informed. Using online certifications and acknowledgment forms offers a straightforward way to track participation.

Scenario-Based Training

Real-life scenario training gives researchers practical experience in spotting and responding to security threats (Canada 2024). These sessions encourage a proactive rather than reactive mindset by simulating breaches. Research security officers and cyber security experts can lead these trainings. Holding sessions twice a year and updating them as threats evolve helps

keep the material relevant and practical. Feedback from participants will help continuously improve the program.

Cyber security Training

Cyber security training is the final training process recommended by this Best Practice Guide. This paper acknowledges that cyber security and technology infrastructure require significant financial investment. Therefore, this training has been included, contingent on the fifth and final pillar of academic research security.

Strong cyber security practices protect research data from digital threats. However, they benefit most from hands-on training, workshops, and informational flyers that cover key protocols and policy directives within their institution. Keeping up with the latest cyber security developments is essential, as this helps institutions prevent breaches and improve resilience (Canada 2024). IT departments, research security offices, and cyber security experts can lead training efforts. Updating training as needed, quarterly or annually, helps keep all personnel current. IT and research security personnel should track progress through logs, quizzes, and scenario-based assessments to ensure everyone has a common understanding of cyber security. As the research security program progresses to the fifth pillar, specific guidance on implementing cyber security and technology standards follows.

Pillar V – Cyber Security and Technology

Cyber Security

Cyber security protects organizations' networks and sensitive data. Best practices include installing system updates as issued by software developers, using complex passwords and multi-factor authentication, fostering a culture of vigilance through awareness and training, implementing effective cyber security frameworks, using real-time threat detection, and having a plan for containing and responding to cyber threats.

Strong cyber security protocols are essential to protect sensitive research data. The national knowledge security guidelines in the Netherlands provide a comprehensive framework for safeguarding against cyber threats, including regular assessments of cyber security measures (Netherlands 2023). Canadian guidelines stress the need to protect IP from external interference and advise organizations on how to maintain control over their IP, particularly when it is vulnerable and could compromise Canada's national security interests (Canada 2024).

It is important to understand cyber threats clearly. Cybercriminals use more advanced tactics to access organizations' systems. There has been an increase in social engineering and phishing scams using AI. Adversaries have discovered that generative AI offers a simple way to access valuable data (Crowdstrike 2025). These threats often appear as an email with a link to something that attracts the user's attention. Unfortunately, a malicious link opens the door for adversaries to gain access to the network. These attacks are on the rise, with activity connected to China surging 150% and some industries experiencing up to 300% more attacks (Crowdstrike). This trend is expected to continue rising, and organizations must adapt and respond to this growing threat. Additional threats include individuals posing as friends or peers to gain access through unauthorized sharing, which is particularly impactful and relevant to the academic

research community. The following six procedures help institutions maintain cyber security and technology standards (Ali *et al.* 2021; Chirra 2021; Farid, Warraich, and Iftikhar 2023).

- Ensure all users install system updates as soon as developers release them.
- Ensure all users create complex passwords and enable multi-factor authentication.
- Provide vigilance through awareness and technology. Establish an organizational culture that prioritizes academic research security by understanding the risks and benefits, and invest in the technology needed to protect computer networks.
- Build a cyber security framework with secure computer networks, which include physical and cyber protections, and offer regular training to all users to ensure compliance with cyber security protocols.
- Initiate a real-time threat detection program. Utilize tools that continuously view system traffic and user behavior to flag unusual patterns to indicate a threat or malicious activity.
- Have a containment and response plan to respond immediately when the threat detection system, software developers, or governmental authorities report a threat. The plan should provide a methodical approach to isolate the threat, stop further damage, and rebuild the computer system.

Technology

Technology plays a prominent role in research security through various tools. The ability to manage research and innovation security is facilitated by technology options from governmental and commercial entities to manage security frameworks. NIST includes a Technology Control Plan template in the US Research Security Framework, which can reduce the risk of "improper transfer of export-controlled information" (Strouse et al., p. 53) and detail

limits on the transfer of physical equipment. The sample form guides users to consider physical security, such as locking doors and limiting access with security badges. The form also plans the path to secure computer networks and databases (Strouse *et al.*). This US example demonstrates that the government assists institutions with the technology needed for academic research security.

Likewise, governments provide solutions that apply the latest technological innovations to amplify research security efforts. SECURE Analytics, the NSF-funded collaboration with Texas A&M University, will provide a platform for conducting due diligence (NSF 2025). Another innovation to perform due diligence is the application of artificial intelligence (AI) and machine learning (ML), which is being described as a "force multiplier" (Spencer 2022). The amount of data institutions must investigate while working to protect their research from malicious actors is immense, and answers must be delivered quickly. Hence, AI and ML are practical solutions for exploring potential research partners. As detailed by one research security data analytics provider, these technology solutions can "find connections, observe trends, and uncover insights faster than ever and on massive, constantly evolving data sets" (FinchAI 2024).

By executing these procedures, HEIs and RPOs can fulfill their due diligence in maintaining the modern-day technology available to advance scientific innovation while ensuring that those innovations remain controlled and reduce the risk of IP theft.

Conclusion

This study highlights the importance of research security programs regarding IP protection, cyber security, and compliance. It outlines the need to secure a competitive advantage, protect data from external threats, and secure partnerships and funding. On the other hand, the lack of a research security program puts a facility and its researchers at high risk of data loss and reputational harm. In addition, there can be legal issues and national security concerns. These repercussions present the dire need to protect academic research in an ever-growing, interconnected, and competitive environment. Academics must work with policymakers, administrators, and researchers to address these challenges, starting with implementing these best practices while supporting academic freedom policies. Industry partners can contribute to research security, most prominently in cases where educational and commercial use overlap. Industry collaboration can provide institutions access to state-of-the-art security technology and intelligence about emerging threats and best practices (Thakur 2024). Institutions should participate in national and international security programs. These programs enable best practice exchange, learning through experiences, and contributing to creating international security standards for research security. Subsequent research should aim to find standard best practices for implementing research security that may be generalized across sectors, such as academia, corporate research, and government laboratories.

Not only does research security drive advancement, but it also ensures continued innovation that will benefit society. Robust academic research security allows HEIs and RPOs to preserve ethics, protect integrity, and solve humanity's most significant challenges. Policies must specify the role of administration, staff, and researchers in protecting sensitive information and have protocols for secure information handling. By developing a strong security

infrastructure, institutions can build a systemic model for research security that addresses vulnerabilities and complies with laws and regulations. Furthermore, partner collaboration is key to a successful security research program, allowing an institution to access external expertise and assets. Government agencies should provide guidance and tools to enable institutions to secure research.

When adapted to developing country contexts, these practices provide a foundation for implementing effective research security programs that protect IP while fostering innovation and international collaboration. Developing countries can learn from the successes and failures of these case studies to create tailored approaches that address their research security challenges while maintaining beneficial international partnerships. Implementing these best practices should be approached with sensitivity to local contexts, resource constraints, and existing institutional structures. Rather than attempting to implement all measures simultaneously, developing countries might benefit from a phased approach that prioritizes fundamental security measures while building capacity for more sophisticated protocols over time. By drawing on the lessons from established research security programs while adapting them to local needs and resources, developing countries can build research security frameworks that protect intellectual assets while enabling participation in the global research community.

Bibliography

Ali, Rao Faizan, Dhanapal Durai Dominic, Syed Emad Azhar Ali, Mobashar Rehman, and Abid Sohail. 2021. "Information Security Behavior and Information Security Policy Compliance: A Systematic Literature Review for Identifying the Transformation Process from Noncompliance to Compliance." April 9. *Applied Sciences*. 11(8): 3383. https://doi.org/10.3390/app11083383 (accessed 1/17/2025)

Antoni, Ntorina. 2020. "Definition and Status of Space Security." June 27. *Handbook of Space Security,* pp. 1-25. https://doi.org/10.1007/978-3-030-22786-9_126-2 (accessed 3/28/2025)

Armond, Anna Catharina Vieira, and Peter Kakuk. 2021. "Research Integrity Guidelines and Safeguards in Brazil." September 16. *Accountability in Research, Ethics, Integrity, and Policy*, vol. 30, 2023 – Issue 3, pp. 133-149. Taylor and Francis Online. https://www.tandfonline.com/doi/full/10.1080/08989621.2021.1979969#abstract (accessed 1/17/2025)

Association of Public and Land-Grant Universities (APLU). 2020. "University Actions to Address Concerns about Security Threats and Undue Foreign Government Influence on Campus." November 1. https://www.aplu.org/wp-content/uploads/effective-science-and-security-practices-what-campuses-are-doing.pdf (accessed 11/1/2024).

Aston University. 2022. Outside Party Due Diligence Procedures. Birmingham, U.K. June. https://www.aston.ac.uk/sites/default/files/Outside%20Party%20Due%20Diligence%20Procedures.pdf (accessed 9/28/2024).

Atlamazoglou, Stavros. 2024. "The US Economy Is Losing as Much as $600 Billion a Year in Intellectual Property from Chinese Espionage." The National Interest. https://nationalinterest.org/blog/buzz/us-economy-losing-much-600-billion-year-intellectual-property-chinese-espionage-210956 (accessed 11/14/2024).

Australian Government, National Health and Medical Research Council (NHMRC). 2018. *Australian Code for the Responsible Conduct of Research.* Universities Australia. https://www.nhmrc.gov.au/about-us/publications/australian-code-responsible-conduct-research-2018#block-views-block-file-attachments-content-block-1 (accessed 4/12/2025)

Australian National University (ANU). 2019. "Incident Report on the Breach of the Australian National University's Administrative Systems." Department of Strategic Communications and Public Affairs. https://imagedepot.anu.edu.au/scapa/Website/SCAPA190209_Public_report_web_2.pdf (accessed 4/12/2025)

Baylis, John, Steve Smith, and Patricia Owens. 2022. "The Globalization of World Politics: An Introduction to International Relations." December 15. Oxford University Press, USA. https://www.oxfordpoliticstrove.com/display/10.1093/hepl/9780192898142.001.0001/hepl-9780192898142 (accessed 3/19/2025)

Berg, Ryan C., and Carlos Baena. 2023. "The Great Balancing Act: Lula in China and the Future of US-Brazil Relations." April 19. Center for Strategic Studies (CSIS). https://www.csis.org/analysis/great-balancing-act-lula-china-and-future-us-brazil-relations (accessed 1/24/2025)

Bochorodycz, Beata. 2023. "The Security Policy Community and the Consensus on the US–Japan Alliance: The Role of Think Tanks, Experts, and the Alliance Managers." September 11. *The Pacific Review, vol.* 37, 2024, Issue 5, pp. 853–883. https://www.tandfonline.com/doi/full/10.1080/09512748.2023.2246664 (accessed 2/2/2025)

Briffa, Hillary. 2023. "Small States and COVID-19: Challenges and Opportunities for Multilateralism." January 20. *Global Perspectives.* 4(1): 57708. https://doi.org/10.1525/gp.2023.57708 (accessed 3/19/2025)

Brown, Michael, and Pavneet Singh. 2018. "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. https://nationalsecurity.gmu.edu/wp-content/uploads/2020/02/DIUX-China-Tech-Transfer-Study-Selected-Readings.pdf (accessed 4/22/2025)

Bui, Hoai Thi, Tung Bui, and Binh Thai Pham. 2024. "The Role of Higher Education in Achieving Sustainable Development Goals: An Evaluation of Motivation and Capacity of Vietnamese Institutions." The International Journal of Management Education, 22(3): 101088. https://www.sciencedirect.com/science/article/pii/S1472811724001599 (accessed 12/29/2024)

Bureau of Industry and Security (BIS). 2025. "Chapter VII §730.3 "Dual Use" and Other Types of Items Subject to the EAR." US Department of Commerce. February 25. https://www.bis.gov/ear/title-15/subtitle-b/chapter-vii/subchapter-c/part-730/ss-7303-dual-use-and-other-types-items (accessed 3/5/2025)

Bureau of Industry and Security (BIS). n.d. "About Export Administration Regulations (EAR)". US Department of Commerce. https://www.bis.gov/regulations (accessed 3/5/2025)

Bureau of Industry and Security (BIS). 2024. "Commerce Control List (CCL)". US Department of Commerce. https://www.bis.doc.gov/index.php/regulations/commerce-control-list-ccl (accessed 3/5/2025)

Bureau of Industry and Security (BIS). 2024b. "Export Control Classification Number (ECCN)". US Department of Commerce. https://www.bis.doc.gov/index.php/licensing/commerce-control-list-classification/export-control-classification-number-eccn (accessed 3/5/2025)

Bureau of Industry and Security (BIS). 2024c. "Mission Statement". US Department of Commerce. https://www.bis.doc.gov/index.php/about-bis/mission-statement (accessed 3/5/2025)

C4ADS. 2024. *Sanctions Explorer.* https://sanctionsexplorer.org/analytics (accessed 11/21/2024)

Campoli, Jessica Suárez, Tatiana Kimura Kodama, Marcelo Seido Nagano, and Heloisa Lee Burnquist. 2025. "Progress of G20 Nations on the 6th Sustainable Development Goal Under the Circular Economy Perspective." Journal of the Knowledge Economy. January 15. https://doi.org/10.1007/s13132-024-02475-x (accessed 3/19/2025)

CAPES. 2023. "History and Goals." September 12. Government of Brazil. https://www.gov.br/capes/en/access-to-information/institutional/history-and-goals (accessed 2/3/2025)

"CCP on the Quad: How American Taxpayers and Universities Fund the CCP's Advanced Military and Technological Research." 2024. Select Committee on the CCP. https://selectcommitteeontheccp.house.gov/media/reports/ccp-quad-how-american-taxpayers-and-universities-fund-ccps-advanced-military-and (accessed 11/23/2024).

Cerdà-Navarro, Antoni, Carmen Touza, Mercè Morey-López, and Elvira Curiel. 2022. "Academic Integrity Policies against Assessment Fraud in Postgraduate Studies: An Analysis of the Situation in Spanish Universities." Heliyon 8(3). https://www.sciencedirect.com/science/article/pii/S2405844022004583 (accessed 10/28/2024)

Chirra, Dinesh Reddy. 2021. "AI-Enabled Cyber security Solutions for Protecting Smart Cities Against Emerging Threats." International Journal of Advanced Engineering Technologies and Innovations 1, no. 2: 237-254. https://www.academia.edu/125039298/AI_Enabled_Cyber security_Solutions_for_Protecting_Smart_Cities_Against_Emerging_Threats?auto=download&auto_download_source=social-news (accessed 10/15/2024).

Christiansen, Younna. 2021. *Pragmatic, Not Liberal Peace? Examining the State of Research on Brazil's Engagement in International Peace Operations.* Frankfurt am Main: Hessische Stiftung Friedens-und Konfliktforschung. https://nbn-resolving.org/urn:nbn:de:0168-ssoar-75573-6 (accessed 3/20/2025)

Claeys-Kulik, Anna-Lena, Thomas E. Jorgensen, Henriette Stober *et al*. 2020. "International Strategic Institutional Partnerships and the European Universities Initiative: Results of the EUA Survey." European University Association (EUA). April 27. https://www.eua.eu/publications/reports/international-strategic-institutional-partnerships-and-the-european-universities-initiative.html (accessed 10/30/2024).

Clark, David. 2024. "How Higher Education Leaders Can Protect Research Security and Enforce a Data Governance Program." November 25. https://www.bdo.com/insights/blogs/nonprofit-standard/how-higher-education-leaders-can-protect-research-security-and-enforce-a-data-governance-program (11/25/2024).

Cornell University. 2024. “Export Controls: Iran Sanctions Guidance Document.” https://researchservices.cornell.edu/policies/export-controls-iran-sanctions-guidance-document (accessed 9/30/2024).

Cornell University. 2021. “Responsible Conduct of Research (RCR) Symposium: Conflict of Interest.” https://researchservices.cornell.edu/sites/default/files/2022-07/2021%20RCR%20Symposium%20Case%20Studies%20%5Bfinal%5D.pdf (accessed 10/15/2024)

Crandall, Carla. 2023. “Protecting Federally-Funded Research and Development: A Primer on National Security Decision Directive 189 for Legal Practitioners.” Summer. https://www.americanbar.org/content/dam/aba/publications/Jurimetrics/summer-2023/protecting-federally-funded-research-and-development-a-primer-on-national-security-decision-directive-189-for-legal-practitioners.pdf (accessed 10/17/2024).

Cross, Di, Simon Thomson, and Alexandra Sinclair. 2017. “Research in Brazil – A Report for CAPES by Clarivate Analytics.” https://www.gov.br/capes/pt-br/centrais-de-conteudo/17012018-capes-incitesreport-final-pdf (accessed 2/27/2025)

d’Hooghe, Ingrid. Jonas Lammertink. 2023. *How National Governments and Research Institutions Safeguard Knowledge Development in Science and Technology*. Leiden Asia Centre. https://leidenasiacentre.nl/wp-content/uploads/2022/11/How-National-Governments-and-Research-Institutions-Safequard-Knowledge-Development-in-Science-and-Technology.pdf (accessed 10/19/2024).

d'Hooghe, Ingrid, and Brigitte Decker. 2020. Clingendael Report. Clingendael: Netherlands Institute of International Relations. https://www.clingendael.org/sites/default/files/2020-07/Rapport_politieke_beinvloeding_in_het_onderwijs_juni_2020.pdf (accessed 1/19/2025)

Dodge, Samuel. 2024. “Chinese University Poses Security Risk to University of Michigan, House GOP Committee Says.” https://www.mlive.com/news/ann-arbor/2024/11/chinese-university-poses-security-risk-to-university-of-michigan-house-gop-committee-says.html (accessed 11/8/2024).

Efstathopoulos, Charalampos. 2021. "Southern Middle Powers and the Liberal International Order: The Options for Brazil and South Africa." International Journal 76(3): 384-403. https://journals.sagepub.com/doi/10.1177/00207020211042915 (accessed 3/21/2025).

El-Bawab, Nadine. 2023. “Former Harvard Professor Charles Lieber Sentenced to Time Served, Fine for Lying About China Ties.” ABC News. https://abcnews.go.com/US/former-harvard-professor-charles-lieber-sentenced-time-served/story?id=98871088 (accessed 1/26/2025)

Enkhtur, Ariunaa, Ming Li, and Xixi Zhang. 2021. “Case Studies of Japanese Universities’ Collaborations with ASEAN, China, and Mongolia.” December 6. *Journal of Comparative and International Higher Education,* vol. 13, issue 5, pp. 145-163. https://files.eric.ed.gov/fulltext/EJ1326671.pdf (accessed 1/24/2025)

European Commission. 2023. “Commission Recommendation of 3.10.2023 on Critical Technology Areas for the EU’s Economic Security for Further Risk Assessment with Member States.” Strasbourg, France. March 10. https://defence-industry-space.ec.europa.eu/commission-recommendation-03-october-2023-critical-technology-areas-eus-economic-security-further_en (accessed 08/28/2024).

Farid, Ghulam, Nosheen Fatima Warraich, and Sadaf Iftikhar. 2023. “Digital information security management policy in academic libraries: A systematic review (2010–2022).” *Journal of Information Science.* April 5. https://journals.sagepub.com/doi/abs/10.1177/01655515231160026 (accessed 10/18/2024).

Fedele, Alessandro, and Cristian Roner. 2022. “Dangerous games: A literature review on cyber security investments.” Journal of Economic Surveys 36, no. 1: 157-187. https://onlinelibrary.wiley.com/doi/full/10.1111/joes.12456 (accessed 10/18/2024).

Federal Ministry of Education and Research (German: Bundesministerium für Bildung und Forschung - BMBF). 2024. “Position paper of the German Federal Ministry of Education and Research on research security in light of the Zeitenwende.” Bonn, Germany. March. https://www.bmbf.de/SharedDocs/Downloads/DE/2024/position-paper-research-security.pdf?__blob=publicationFile&v=4 (accessed 10/15/2024).

Fife, Robert, and S. Chase. 2022. "Canadian academics involved in joint research with Iranian institutions on drone technology." The Globe and Mail, February 11. https://www.theglobeandmail.com/politics/article-canadian-academics-involved-in-joint-research-with-iranian/ (accessed 10/14/2024)

FinchAI. 2025. “Uncover the Unknown.” Finch Analyst. https://finchai.com/analyst/ (accessed 4/13/2025)

Flagg, Melissa, Autumn Toney, and Paul Harris. 2021. “Research Security, Collaboration, and the Changing Map of Global R&D”. Center for Security and Emerging Technology. June. https://cset.georgetown.edu/wp-content/uploads/CSET-Research-Security-Collaboration-and-the-Changing-Map-of-Global-RD.pdf (accessed 3/5/2025)

French Presidency of the Council of the European Union. 2022. *Marseille Declaration on International Cooperation in Research and Innovation (R&I)*. March 8. https://www.cesaer.org/content/10-library/2022/en-marseille-declaration-17075.pdf (accessed 3/19/2025).

Gabriel, G. 2020. "A Review of China's and Japan's International Engagement in South America: The Cases of Brazil, Chile, and Venezuela." May. Institute of Developing Economies, Discussion Paper 785. https://www.ide.go.jp/English/Publish/Reports/Dp/785.html (accessed 3/16/2025)

Gamache, Kevin R. 2024. *Residency Week Lecture*. Executive Master of Public Service and Administration Capstone Course at the Bush School of Government and Public Service (PSAA 675-700). Washington, D.C. 9/10/2024.

Gardner, Allison, Adam Leon Smith, Adam Steventon, Ellen Coughlan, Marie Oldfield. 2022. "Ethical Funding for Trustworthy AI: Proposals to Address the Responsibilities of Funders to Ensure That Projects Adhere to Trustworthy AI Practice." AI and Ethics. June 13. doi: https://doi.org/10.1007/s43681-021-00069-w (accessed 1/7/2025)

Gaviao, L. O., Dutra, L. D., and Kostin, S. 2021. "Prioritization of Multilateral Agreements on Export Control of Defense Products and Sensitive by Hierarchical Technologies Analysis Process." *AUSTRAL: Brazilian Journal of Strategy & International Relations, Vol. 10, No. 20.* December. https://seer.ufrgs.br/austral/article/view/119666 (accessed 2/24/2025)

Geer, Dan, Eric Jardine, and Eireann Leverett. 2020. "On market concentration and cyber security risk." Journal of Cyber Policy 5, no. 1: 9-29. February 24. https://www.tandfonline.com/doi/full/10.1080/23738871.2020.1728355 (accessed 10/18/2024).

German National Academy of Sciences Leopoldina (German: Deutsche Akademie der Naturforscher Leopoldina – Nationale Akademie der Wissenschaften). 2022. *The Handling of Security-Relevant Research in Germany: An Overview*. Halle, Germany. https://www.sicherheitsrelevante-forschung.org/wpcontent/uploads/2022/10/The-Handling-of-Security-Relevant-Research-inGermany-An-Overview.pdf (accessed 10/26/2024).

German Rectors' Conference (German: Hochschulrektorenkonferenz – HRK). 2020. "Guiding Questions on University Cooperation with the People's Republic of China." September 9. https://www.hrk.de/resolutions-publications/resolutions/beschluss/detail/guiding-questions-on-university-cooperation-with-the-peoples-republic-of-china/ (accessed 9/28/2024).

German Research Foundation (German: Deutsche Forschungsgemeinschaft (DFG)). 2022. *Scientific Freedom and Scientific Responsibility, Recommendations for Handling of Security-Relevant Research*. (German: Empfehlungen zur Sicherstellung der Integrität in der Forschung.) Berlin, Germany. January 1. https://www.leopoldina.org/uploads/tx_leopublication/2014_06_DFG-Leopoldina_Scientific_Freedom_Responsibility_EN.pdf (accessed 10/30/2024)

Giumelli, Francesco, and Michal Onderco. 2021. "States, Firms, and Security: How Private Actors Implement Sanctions, Lessons Learned from the Netherlands." *European Journal of International Security*, vol. 6, issue 2, pp. 190–209. https://www.cambridge.org/core/journals/european-journal-of-international-security/article/states-firms-and-security-how-private-actors-implement-sanctions-lessons-learned-from-the-netherlands/2D74ECCB8252B534F2B36C2375BA88F1 (accessed 11/14/2024)

Government of Canada. 2024. *Safeguarding Your Research.* Science.gc.ca. https://science.gc.ca/site/science/en/safeguarding-your-research (accessed 11/1/2024).

Government of Canada. 2024b. *Case Studies: How a security breach can impact your research.* https://science.gc.ca/site/science/en/safeguarding-your-research/guidelines-and-tools-

implement-research-security/case-studies-how-security-breach-can-impact-your-research/scenario-2-participation-foreign-talent-and-recruitment-programs (accessed 11/1/2024).

Government of Canada. 2024c. *Safeguarding Your Research, Guidelines and Tools to Implement Research Security, Case Studies-Scenarios*. Science.gc.ca. https://science.gc.ca/site/science/en/safeguarding-your-research/guidelines-and-tools-implement-research-security/case-studies-how-security-breach-can-impact-your-research (accessed 11/21/2024)

Government of Canada. 2024d. *Sensitive Technology Research and Affiliations of Concern.* Science.gc.ca. https://science.gc.ca/site/science/en/safeguarding-your-research/guidelines-and-tools-implement-research-security/sensitive-technology-research-and-affiliations-concern (accessed 11/21/2024)

Government of Canada. 2024e. *Safeguarding Your Research, Guidelines and Tools to Implement Research Security, Named Research Organizations*. Science.gc.ca. https://science.gc.ca/site/science/en/safeguarding-your-research/guidelines-and-tools-implement-research-security/sensitive-technology-research-and-affiliations-concern/named-research-organizations (accessed 11/21/2024)

Government of Canada. 2024f. *Notice to Exporters No. 1129 – Amendment to the Export Control List: Quantum Computing and Advanced Semiconductors.* International.gc.ca. https://www.international.gc.ca/trade-commerce/controls-controles/notices-avis/1129.aspx?lang=eng (accessed 3/2/2025)

Government of Japan. 2023. "Checklist for New Risks Associated with Increasing Internationalization and Openness of Research (Universities and Research Institutions Template)." https://www8.cao.go.jp/cstp/english/doc/checklist_for_univ_en.pdf (accessed 1/9/2025)

Government of Japan. 2021. "Guidelines for Appropriate Execution of Competitive Research Funds." https://www8.cao.go.jp/cstp/english/doc/guidelines_en.pdf (accessed 1/9/2025)

Government of Japan. 2021b. "Policy Directions for Ensuring Research Integrity in Response to New Risks Associated with Increasing Internationalization and Openness of Research Activities." https://www8.cao.go.jp/cstp/english/doc/policy_directions_en.pdf (accessed 1/9/2025)

Grimaldi, Michele, Marco Greco, and Livio Cricelli. "A framework of intellectual property protection strategies and open innovation." Journal of Business Research 123 (2021): 156-164. https://www.sciencedirect.com/science/article/abs/pii/S0148296320306263 (accessed 10/27/2024).

Hagan, Karla. 2025. *National Science, Technology, and Security Roundtable Capstone: Proceedings of a Workshop*. Washington, DC: The National Academies Press. https://nap.nationalacademies.org/catalog/27976/national-science-technology-and-security-roundtable-capstone-proceedings-of-a (accessed 1/28/2025).

Hardwick, Clay, and Kacey Strickland. 2022. "Developing a Proactive Research Security Program in an Era of Heightened Foreign Influence". SRAI News. July 13. https://www.srainternational.org/blogs/srai-news/2022/07/13/developing-a-proactive-research-security-program-i (accessed 10/4/2024)

Hayward, Freddie. 2021. "How the Chinese Government is Buying its Way into UK Universities." *The New Statesman*. July 13. https://www.newstatesman.com/politics/2021/07/how-chinese-government-buying-its-way-uk-universities (accessed 1/28/2025)

He, Chris Zhijian, Tracie Frost, and Robert E. Pinsker. 2020. "The impact of reported cyber security breaches on firm innovation." Journal of Information Systems 34, no. 2: 187-209. June 1. https://www.researchgate.net/publication/336947778_The_Impact_of_Reported_Cybersecurity_Breaches_on_Firm_Innovation (accessed 10/21/2024).

Heathershaw, John. 2019. "Evidence on Autocracies and UK Foreign Policy." UK Parliament Foreign Affairs Committee. https://committees.parliament.uk/writtenevidence/104927/html/ (accessed 1/17/2025)

Hossain, Zakir, Özgür Çelik, and Corinne Hertel. 2024. "Academic Integrity and Copyright Literacy Policy and Instruction in K-12 Schools: A Global Study from the Perspective of School Library Professionals." International Journal for Educational Integrity 20(1). https://edintegrity.biomedcentral.com/articles/10.1007/s40979-024-00150-x (accessed 10/9/2024)

Ige, Adebimpe Bolatito, Eseoghene Kupa, and Oluwatosin Ilori. 2024. "Developing comprehensive cyber security frameworks for protecting green infrastructure: Conceptual models and practical applications." GSC Advanced Research and Reviews 20, no. 1: 025-041. https://gsconlinepress.com/journals/gscarr/content/developing-comprehensive-cybersecurity-frameworks-protecting-green-infrastructure-conceptual (accessed 10/30/2024).

Imperial College London. 2023. *Export Controls and the Impact on Teaching.* London, U.K. https://www.imperial.ac.uk/research-and-innovation/research-office/research-security/research-security-legislation/export-controls/impact-on-teaching/ (accessed 10/14/2024).

International Center for Academic Integrity (ICAI). n.d. "Fundamental Values of Academic Integrity." https://academicintegrity.org/aws/ICAI/pt/sp/values (accessed 4/5/2025)

International Science Council (ISC). 2024. "Statutes and Rules of Procedure." March 8. https://council.science/wp-content/uploads/2024/03/ISC_Statutes_RulesProcedure_8march2024.pdf (accessed 3/19/2025).

International Trade Administration (ITA). 2024. "Data Visualization." Department of Commerce. https://www.trade.gov/data-visualization/csl-search (accessed 11/20/2024)

International Trade Administration. 2025. “US Export Controls.” Department of Commerce. https://www.trade.gov/us-export-controls (accessed 3/5/2025)

Job, Brian L. 2022. "Between a Rock and a Hard Place: The Dilemmas of Middle Powers." June 22. *The Strategic Options of Middle Powers in the Asia-Pacific*, 1st ed: pp. 34-56. London: Routledge. https://doi.org/10.1142/S1013251120400081 (accessed 3/18/2025)

Jordan, Javier. 202. "International Competition Below the Threshold of War: Toward a Theory of Gray Zone Conflict." Journal of Strategic Security 14 (1):1–24. https://www.jstor.org/stable/26999974?seq=1 (accessed 3/5/2025).

Komljenovic, Janja, and Ben Williamson. 2024. Behind the Platforms: Safeguarding Intellectual Property Rights and Academic Freedom in Higher Education. Brussels, Belgium: Education International. https://www.ei-ie.org/en/item/28484:behind-the-platforms-safeguarding-intellectual-property-rights-and-academic-freedom-in-higher-education (accessed 10/3/2024)

Kundu, Debolina, and Devarupa Gupta. 2024. "Building a Fairer Future: Joint Actions for Poverty, Hunger and Inequality Reduction by G20 Nations." November. Brasilia: *Revista Tempo do Mundo.* https://doi.org/10.38116/rtm34art3 (accessed 3/20/2025)

Kianpour, Mazaher, Stewart J. Kowalski, and Harald Øverby. 2021. “Systematically understanding cyber security economics: A survey.” Sustainability 13, no. 24: 13677. https://www.mdpi.com/2071-1050/13/24/13677 (accessed 11/1/2024).

Kimball, Daryl. 2022. “The Wassenaar Agreement at a Glance.” Arms Control Association. February. https://www.armscontrol.org/factsheets/wassenaar (accessed 2/3/2025)

Lancaster University. 2024. “Due Diligence.” https://www.lancaster.ac.uk/research/research-services/trusted-researchand-innovation/due-diligence/ (accessed 11/5/2024).

Larionova, M., and Shelepov, A. 2021. "Emerging Regulation for the Digital Economy: Challenges and Opportunities for Multilateral Global Governance." *International Organisations Research Journal*, vol. 16, no 1, pp. 29-63. https://iorj.hse.ru/data/2021/09/09/1388491189/Larionova_iorj_2021_01_05_07_21__f-20-44.pdf (accessed 3/20/2025)

Mazarr, Michael J. 2015. “Mastering the Gray Zone: Understanding a Changing Era of Conflict.” Strategic Studies Institute, The United States Army War College Press. https://archive.org/details/DTIC_AD1000186/mode/2up (accessed 3/1/2025)

Mervis, Jeffery. 2024. “US Invests $67 Million in National Research Security Centers”. Science Insider. July 26. https://www.science.org/content/article/u-s-invests-67-million-national-research-security-centers (accessed 3/5/2025)

Milevski, Lukas. 2024. "When Does Gray Zone Confrontation End? A Conceptual Analysis." National Defense University Press. February 15. https://ndupress.ndu.edu/Media/News/News-Article-View/Article/3678004/when-does-

gray-zone-confrontation-end-a-conceptual-analysis/#:~:text=To%20demonstrate%2C%20this%20article%20first%20discusses%20conceptual%20analysis%2C,of%20generating%20a%20gray%20zone%20theory%20of%20suc (accessed 3/1/2025)

Mullins, Sam. 2024. "The Role of Non-State Actors as Proxies in Irregular Warfare and Malign State Influence." Arlington, Virginia: Irregular Warfare Center. March. https://irregularwarfarecenter.org/wp-content/uploads/The-Role-of-Non-State-Actors-as-Proxies-in-Irregular-Warfare-and-Malign-State-Influence.pdf (accessed 3/1/2025)

National Institute of Standards and Technology (NIST). n.d. "Research Security Office." https://www.nist.gov/adlp/research-security-office (accessed 9/7/2025)

National Intelligence Council (NIC). 2007. "Nonstate actors: Impact on International Relations and Implications for the United States". August 23. https://irp.fas.org/nic/nonstate_actors_2007.pdf (accessed 2/23/2025)

National Protective Security Authority (NPSA). 2024. *Trusted Research for Academia*. U.K. July 2. https://www.npsa.gov.uk/trusted-research-academia (accessed 10/16/2024).

National Science Foundation (NSF). 2025. "NSF SECURE Analytics Leadership Showcase Due Diligence Tool at Annual ASCE Conference." February 25. https://secure-analytics.org/asce2025/ (accessed 4/13/2025)

National Science Foundation (NSF). 2024. "Research Security Training." Office of the Chief of Research Security Strategy and Policy. https://www.nsf.gov/research-security/training (accessed 11/16/2024)

National Science and Technology Council (NSTC). 2022. "Guidance for Implementing National Security Presidential Memorandum 33 (NSPM-33) on National Security Strategy for United States Government-Supported Research and Development." January. https://bidenwhitehouse.archives.gov/wp-content/uploads/2022/01/010422-NSPM-33-Implementation-Guidance.pdf (accessed 10/21/2024)

National Science and Technology Council. 2021a. "Recommended Practices for Strengthening the Security and Integrity of America's Science and Technology Research Enterprise." January. https://trumpwhitehouse.archives.gov/wp-content/uploads/2021/01/NSTC-Research-Security-Best-Practices-Jan2021.pdf (accessed 10/18/2024).

Nuclear Suppliers Group. n.d. "About the Nuclear Suppliers Group." https://www.nuclearsuppliersgroup.org/index.php/en/ (accessed 2/28/2025)

Office of Foreign Assets Control (OFAC). n.d. "Mission Statement". US Department of the Treasury. https://ofac.treasury.gov (accessed 3/5/2025)

Office of the Director of National Intelligence (ODNI). 2021. "Protecting Critical and Emerging US Technologies From Foreign Threats." The National Counterintelligence and Security Center (NCSC).

https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/FIN (accessed 08/28/2024).

Office of the Director of National Intelligence (ODNI). 2024. “Research Security.” National Counterintelligence and Security Center (NCSC). https://www.dni.gov/index.php/safeguarding-science/research-security#Mitigation (accessed 1/17/2025)

Office of the Director of National Intelligence, Department of Education, and Federal Bureau of Investigation (ODNI *et al.*). 2024. “Foreign Malign Influence and Higher Education.” https://www.fbi.gov/file-repository/foreign-malign-influence-and-higher-education-101824.pdf/view (accessed 3/1/2025)

Ollongren, Kajsa. "Letter to Parliament: Disruption of Russian Economic Espionage Activities by AIVD." Dutch Ministry of the Interior and Kingdom Relations (BZK), 10 December 2020. https://www.aivd.nl/documenten/kamerstukken/2020/12/10/kamerbrief-verstoring-russische-economische-spionageactiviteiten-door-aivd (accessed 8/29/2024)

Olweny, Florence. 2024. “Navigating the Nexus of Security and Privacy in Modern Financial Technologies.” GSC Advanced Research and Reviews 18(2): 167–97. doi: 10.30574/gscarr.2024.18.2.0043. https://gsconlinepress.com/journals/gscarr/sites/default/files/GSCARR-2024-0043.pdf (accessed 9/27/2024)

Organization for Economic Cooperation and Development (OECD). 2022. “Integrity and security in the global research ecosystem.” OECD Science, Technology and Industry Policy Papers, No. 130. June. Paris: OECD Publishing. https://doi.org/10.1787/1c416f43-en. (accessed 3/19/2025).

Organization for Economic Cooperation and Development (OECD). 2023. “Knowledge Security Policy Initiative in the Netherlands.” Paris, France. July 11. https://stip.oecd.org/stip/interactive-dashboards/policy-initiatives/2023%2Fdata%2FpolicyInitiatives%2F99997610 (accessed 10/17/2024).

Organization for Economic Cooperation and Development (OECD). 2021. “Recommendation of the Council Concerning Access to Research Data from Public Funding.” https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0347 (accessed 3/19/2025).

Organization for Economic Cooperation and Development (OECD). 2019. “Recommendation of the Council on Artificial Intelligence.” https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449 (accessed 3/19/2025).

Ordoñez de Pablos, Patricia. 2024. "Science Diplomacy and Digital Transformation for Greener, More Inclusive and Resilient Economies and Societies." January 25. *Journal of Science and Technology Policy Management.* Vol. 15 No. 2, pp. 221-225. https://doi.org/10.1108/JSTPM-03-2024-223 (accessed 3/18/2025)

Pannier, Alice. 2023. “Balancing Security and Openness for Critical Technologies: Challenges for French and European Research.” https://www.ifri.org/sites/default/files/migrated_files/documents/atoms/files/ifri_pannier_balancing_security_openness_critical_technologies_2023.pdf (accessed 11/2/2024).

Parliament of Canada. 2024c. “The Nexus Between Science and National Security in Canada: The Case of the National Microbiology Laboratory in Winnipeg.” House of Commons, Canada. https://www.ourcommons.ca/documentviewer/en/44-1/CACN/report-8/page-30 (accessed 2/6/2025)

Paulsen, Mona. 2024. "The Past, Present, and Potential of Economic Security." May 26. London School of Economics, Law School. Forthcoming, to be published in the Yale Journal of International Law, vol. 50. http://dx.doi.org/10.2139/ssrn.4604958 (accessed 3/20/2025)

Pawlikowski, Andrzej. 2024. “Emerging and Innovative Military Technologies in the EU Member States: Background and Issues.” Studies of the Central European Professors’ Network: 109–58. doi: 10.54237/profnet.2024.zkjeszcodef_3. https://www.researchgate.net/publication/386442589_Emerging_and_Innovative_Military_Technologies_in_the_EU_Member_States_Background_and_Issues (accessed 11/2/2024)

Prabhakar, Arati. 2024. *Memorandum for the Heads of Federal Research Agencies. Executive Office of the President, Office of Science and Technology Policy*. Washington, D.C. July 9. https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/07/OSTP-RSP-Guidelines-Memo.pdf (accessed 9/30/2024).

Resnik, David B. 2020. "What Is Ethics in Research & Why Is It Important?". National Institute of Environmental Health Sciences. https://www.niehs.nih.gov/research/resources/bioethics/whatis (accessed 9/22/2024).

Ross, John. 2024. “Excessive Secrecy ‘Undermining Security’ of Australian Research.” Times Higher Education (THE). September 25. https://www.timeshighereducation.com/news/excessive-secrecy-undermining-security-australian-research#:~:text=Excessive%20secrecy%20in%20Australian%20security,risks%2C%20according%20to%20an%20expert. (accessed 10/5/2024).

Sarraf, Samira. 2019. “ANU details findings of data breach.” October 3. CSO Online. https://www.csoonline.com/article/569789/anu-details-findings-of-data-breach.html (accessed 2/8/2025)

Shih, Tommy. 2024. “We Cannot Adopt a Blanket Approach to Research Security.” https://www.universityworldnews.com/post.php?story=20241001140316637 (accessed 11/2/2024).

Smith, Marcus, and Patrick Walsh. 2023. “Security Sensitive Research: Balancing Research Integrity, Academic Freedom and National Interest.” Journal of Higher Education Policy & Management. 45(5), 495–510. April 13.

https://www.tandfonline.com/doi/abs/10.1080/1360080X.2023.2202328 (accessed 10/12/2024).

Spencer, Susie. 2022. “Artificial Intelligence as a Force Multiplier.” SailPoint. May 4. https://www.sailpoint.com/blog/artificial-intelligence-as-a-force-multiplier-2 (accessed 4/13/2025)

Stilgherrian. 2019. “ANU incident report on massive data breach: A must-read.” October 2. ZDNet. https://www.zdnet.com/article/anu-incident-report-on-massive-data-breach-a-must-read/ (accessed 1/29/2025)

Strouse, Gregory F., Claire M. Saundry, Timothy Wood, Philip Bennett, and Mary Bedner. 2023. *Safeguarding International Science : Research Security Framework.* National Institute of Standards and Technology (NIST). August 31. https://doi.org/10.6028/NIST.IR.8484 (accessed 4/13/2025)

Tapay-Cueva, Jack, and David Dong. 2023. "What Brazil’s 'Multipolar' Foreign Policy Means for the Bretton Woods Institutions." August 23. Atlantic Council. https://www.atlanticcouncil.org/blogs/econographics/what-brazils-multipolar-foreign-policy-means-for-the-bretton-woods-institutions/ (accessed 11/14/2024)

Thakur, Manikant. 2024. “Cyber Security Threats and Countermeasures in Digital Age.” Journal of Applied Science and Education (JASE) 4(1): 1–20. doi: 10.54060/a2zjournals.jase.42. https://jase.a2zjournals.com/index.php/ase/article/view/42 (accessed 1/6/2025)

Tiffert, Glenn, ed. 2020. *Global Engagement: Rethinking Risk in the Research Enterprise*. Hoover Institution Press: Stanford, California. https://www.hoover.org/global-engagement-rethinking-risk-research-enterprise (accessed 9/12/2024)

Trump, Donald J. 2021. *Presidential Memorandum on United States Government Supported Research and Development National Security Policy*. January 14. https://trumpwhitehouse.archives.gov/presidential-actions/presidential-memorandum-united-states-government-supported-research-development-national-security-policy/ (accessed 9/29/2024).

U.K. Foreign Affairs Committee (UK FAC). 2019. “A Cautious Embrace: Defending Democracy in an Age of Autocracies.” House of Commons. https://publications.parliament.uk/pa/cm201919/cmselect/cmfaff/109/10905.htm (accessed 1/13/2025)

U.K. Research and Innovation (UKRI). 2022. “Due Diligence Guidance and Supporting Documents.” October 26. https://www.ukri.org/publications/due-diligence-guidance-and-supporting-documents/ (accessed 9/30/2024).

United Nations (U.N.) Human Rights Office of the High Commissioner. 1966. “International Covenant on Economic, Social and Cultural Rights.” https://www.ohchr.org/en/professionalinterest/pages/cescr.aspx (accessed 3/19/2025).

Universities UK International (UUKI). 2024. “Case Studies: How Universities Are Managing Risk in Internationalisation.” https://www.universitiesuk.ac.uk/universities-uk-international/insights-and-publications/uuki-insights/case-studies-how-universities-are (accessed 2/2/2025)

US Department of State. 2017. "21st Century Statecraft." February 27. https://2009-2017.state.gov/statecraft/overview/index.htm (accessed 2/27/ 2025)

US Department of State. n.d.-a. “Directorate of Defense Trade Controls.” https://www.state.gov/bureaus-offices/under-secretary-for-arms-control-and-international-security-affairs/bureau-of-political-military-affairs/directorate-of-defense-trade-controls-pm-ddtc/ (accessed 3/23/2025)

US Department of State. n.d.-b. “The International Traffic in Arms Regulations (ITAR).” Directorate of Defense Trade Controls. https://www.pmddtc.state.gov/ddtc_public/ddtc_public?id=ddtc_kb_article_page&sys_id=24d528fddbfc930044f9ff621f961987 (accessed 2/12/2025)

US Department of State. n.d.-c. “Missile Technology Control Regime (MTCR) Frequently Asked Questions.” https://www.state.gov/bureau-of-international-security-and-nonproliferation/releases/2025/01/missile-technology-control-regime-mtcr-frequently-asked-questions (accessed 2/16/2025)

US Government Accountability Office (GAO). 2005. “Defense Trade: Arms Export Control Vulnerabilities and Inefficiencies in the Post-9/11 Environment.” April 7. https://www.gao.gov/products/gao-05-468r (accessed 2/28/2025)

US Government Accountability Office (GAO). 2022. “Export Controls: Enforcement Agencies Should Better Leverage Information to Target Efforts Involving US Universities: Report to Congressional Requesters.” https://www.gao.gov/assets/gao-22-105727.pdf (accessed 2/21/2025)

US Government Accountability Office (GAO). 2011. “Export Controls: Improvements Needed to Prevent Unauthorized Technology Releases to Foreign Nationals in the United States: Report to Congressional Requesters.” https://www.gao.gov/products/gao-11-354 (accessed 2/21/2025)

US Government Accountability Office (GAO). 2023. “Export Controls: State Needs to Improve Compliance Data to Enhance Oversight of Defense Services: Report to the Chairman, Committee on Foreign Relations.” https://www.gao.gov/assets/gao-23-106379.pdf (accessed 2/21/2025)

US Government Accountability Office (GAO). 2020. “Federal Research. Agencies Need to Enhance Policies to Address Foreign Influence—Committee on Finance, United States Senate. https://www.gao.gov/assets/gao-21-130.pdf

US Government Accountability Office (GAO). 2023. “Highlights of GAO-24-106074, a report to Congressional Committees: Strengthening Disclosure Requirements and Assessing

Training Could Improve Research Security." GAO Highlights. December. https://www.gao.gov/assets/d24106074.pdf (accessed 2/24/2025).

US Government Accountability Office (GAO). 2008. "Oversight of Government Management, the Federal Workforce, and the District of Columbia, Committee on Homeland Security and Government Affairs, US Senate." https://www.hsgac.senate.gov/subcommittees/archives/oversight-of-government-management/ (accessed 2/21/2025).

University of Calgary. 2025. "International Travel Loaner Device Program." https://www.ucalgary.ca/risk/risk-management-insurance/travel/international-travel-loaner-device-program (accessed 3/29/2025)

University of Maryland Baltimore. 2025. "Research and Development: Research Security Training." March 08. https://www.umaryland.edu/ord/umb-research-security-program/research-security-training/ (accessed 3/8/2025).

Universities of the Netherlands. 2023. "Capability Maturity Model for Knowledge Security." https://www.universiteitenvannederland.nl/files/publications/UNL%20Capability%20Maturity%20Model%20Knowledge%20Security%20ENG-DEF.pdf (accessed 10/24/2024).

University of Texas Health Houston. 2024. "Research Security Framework." January. https://www.uth.edu/hoop/policy.htm?id=9bf91791-7713-490d-9e58-ea5b07a7323f (accessed 3/9/2025).

Van Der Molen, Irna. 2023. "Viewpoint: We Need to Talk About Research Security on Campus". Science Business. October 19. https://sciencebusiness.net/viewpoint/universities/viewpoint-we-need-talk-about-research-security-campus (accessed 3/5/2025)

Virginia Polytechnic Institute and State University (VT). 2024. "Case Studies Regarding Foreign Influence." Virginia Tech, Research and Innovation. https://www.research.vt.edu/osp/researchers/compliance/nonfinancial-compliance/foreign-influence/case-studies.html (accessed 1/15/2025)

von Uexkull, Nina, and Halvard Buhaug. 2021. "Security Implications of Climate Change: A Decade of Scientific Progress." Journal of Peace Research 58(1): 3–17. doi:10.1177/0022343320984210. https://journals.sagepub.com/doi/10.1177/0022343320984210 (accessed 2/27/2025)

Willoughby, Scott. 2024. PowerPoint Presentation: "Foreign Compliance and Research Security." University of Adelaide, Australia. September.

World Conferences on Research Integrity/. 2010. "Singapore Statement on Research Integrity." September 22. https://www.wcrif.org/statement# (accessed 3/19/2025).

Xu, Yixiang. 2024. “A Zeitenwende for Science and Technology Research?” American-German Institute. https://americangerman.institute/2024/05/a-zeitenwende-for-science-and-technology-research/ (accessed 11/14/2024).

Zhang, D., Lawrence, C., Sellitto, M., Wald, R., Schaake, M., Ho, D. E., and Grotto, A. 2022. "Enhancing International Cooperation in AI Research: The Case for a Multilateral AI Research Institute." Stanford Institute for Human-Centered Artificial Intelligence. April 14. https://hai.stanford.edu/policy/white-paper-enhancing-international-cooperation-ai-research-case-multilateral-ai-research-institute (accessed 3/5/2025)

Additional Resources

The content in this paper is the work of the authors.

The authors used the following augmented intelligence systems and reasoning models to assist with content organization, identification and validation of resources, proper citation, grammar, clarity, statement refinement, engagement, and delivery:

ChatGPT 4.o from OpenAI
Claude 3.7 Sonnet from Anthropic
Finch Analyst from FinchAI
Grammarly Pro, Large Language Model
RefWorks from ExLibris

Copies of chats are available upon request.