

Chapter 2

Academic Espionage: Finding a Better Balance between Open Science and Security Imperatives

ARTUR GRUSZCZAK

Jagiellonian University

ORCID: 0000-0002-3450-8377

Abstract: Academia has increasingly become a battleground where high-value knowledge and intellectual property are contested by public and private actors employing diverse strategies to secure or appropriate these assets for their own benefit. Universities, as centers of knowledge production, are natural targets for surveillance, recruitment, and collaboration by intelligence services. Security institutions, particularly intelligence and counterintelligence agencies, play a pivotal role in protecting the sources, repositories, and integrity of critical information and data. This chapter offers a set of recommendations addressing the challenge of safeguarding academia's principles of open research and scientific freedom against malicious activities, particularly those conducted by intelligence services.

Keywords: academia; security; espionage; intelligence; counterintelligence

Research and education have long been vulnerable to malicious and disruptive activities perpetrated by various entities, ranging from populist politicians to cybercriminals. As hubs for knowledge production, professional development, and critical inquiry, these sectors face distinct vulnerabilities that can be mitigated through awareness-raising initiatives and robust risk management strategies. Among these challenges is the issue of academic espionage, which exploits the principles of open science while leveraging actionable intelligence and conventional spying techniques employed by state and non-state actors. This short analysis examines academia as a contested space

where espionage and intelligence gathering undermine academic freedom and contribute to the securitization of academia.

The ideal university has traditionally been envisioned as an open, safe, and intellectually vibrant environment where students and faculty pursue a shared passion for investigating and understanding the complexities of the world. Students invest their time and energy in acquiring knowledge and skills for their future careers, while professors contribute specialized expertise and knowledge developed through rigorous research, often leading to groundbreaking discoveries, innovative technologies, and novel theoretical frameworks.

The principles and practices of open science, endorsed by UNESCO and implemented by organizations such as the European Union, reflect the interconnected nature of the contemporary world. Global cooperation and knowledge sharing are deemed essential for addressing complex social, environmental, and economic challenges. While scientific progress remains concentrated in the Global North, emerging powers such as China and India are increasingly participating in collaborative scientific endeavors. These efforts underscore the importance of initiatives promoting open science and FAIR (Findable, Accessible, Interoperable, and Reusable) data.¹

However, science is not only a civilizational asset but also a high-value commodity with significant economic and strategic implications. Governments and private enterprises, which finance research directly or through granting agencies and foundations, have a vested interest in securing priority access to original research findings—especially those with disruptive potential for the economy, security, and society. Governments aim to ensure sustainable development, safeguard public infrastructure, and mitigate emerging risks, while businesses seek competitive advantages and market innovation. Consequently, academia has increasingly become a battleground where high-value knowledge and intellectual property are contested by public and private actors employing diverse strategies to secure or appropriate these assets

¹ UNESCO, “An introduction to the UNESCO Recommendation on Open Science,” Canadian Commission for UNESCO, (2022), <https://doi.org/10.54677/XOIR1696>; European Commission, “Open Science,” European Commission, 2024, https://research-and-innovation.ec.europa.eu/strategy/strategy-2020-2024/our-digital-future/open-science_en.

for their own benefit. This dynamic is particularly pronounced when such knowledge is safeguarded by patents, copyrights, or trademarks, or when it holds ethical, political, or ideological sensitivities. When the vital interests of a state—its society, economy, or national security—are at stake, security institutions, particularly intelligence and counterintelligence agencies, play a pivotal role in protecting the sources, repositories, and integrity of critical information and data. Universities, as centers of knowledge production, are natural targets for surveillance, recruitment, and collaboration by intelligence services. These institutions increasingly navigate a complex relationship with intelligence agencies, framed by shared interests in research, professionalization, and national security.

Intelligence institutions have actively sought to establish and deepen collaboration with academia for purposes such as recruitment, professionalization, and networking. Academia, in turn, has recognized several benefits of such cooperation, including professional development (e.g., incorporating former intelligence practitioners into faculty roles), enhanced research quality (through contributions by active and former intelligence professionals), and enriched scholarly output (such as intelligence-focused studies, publications, and research projects). This pragmatic engagement is conceptualized by Liam Francis Gearon through his model of the “university-security-intelligence nexus,” which operates across four intersecting domains: operational, epistemological, ethical, and existential.² In the operational domain, Gearon highlights the practical rules governing collaboration between intelligence agencies and academia, including cases of covert partnerships and mutual support. The epistemological domain frames this nexus as an epistemic community uniting scholars and intelligence practitioners to generate knowledge and expertise aimed at countering security threats. The ethical domain addresses questions of moral responsibility and the ethical implications of intelligence and security influence within academic institutions. Lastly, the existential domain situates this nexus within the broader context

² Liam Francis Gearon, “The University-Security-Intelligence Nexus: Four Domains,” in *The Routledge International Handbook of Universities, Security and Intelligence Studies*, ed. Liam Francis Gearon (London: Routledge, 2020), 15.

of pressing national security threats, societal risks, and individual vulnerabilities, emphasizing its role in mitigating complex contemporary challenges. Gearon argues that this model signifies a shift in intelligence and security paradigms, from traditional, narrowly focused frameworks to more expansive, integrated approaches that harness academic insights and intelligence expertise to mitigate evolving threats.³

Similarly, Vogel et al.⁴ examine Academic–Industry–Intelligence Collaboration through the lens of initiatives like the US National Security Agency’s (NSA) establishment of the Laboratory for Analytic Sciences (LAS). They contend that institutions such as the NSA can drive organizational innovation and adaptation by fostering inter-institutional and interdisciplinary collaboration between academics and intelligence professionals, yielding mutually beneficial outcomes for both domains.

Despite potential synergies, the entanglement between academia and intelligence often results in blurred boundaries and hidden agendas, which can undermine the core academic values of openness, freedom, and objectivity. These dynamics manifest in three key areas:

1. Exploitation of Research Outputs

Advanced research, particularly in critical fields such as defense and technology, is a prime target for espionage. For example, concerns over Chinese espionage in US universities have highlighted vulnerabilities, such as unauthorized knowledge transfer and cyber intrusions.⁵ Initiatives such as China’s Thousand Talents Program (TTP) have fueled geopolitical tensions, prompting countermeasures like the US Department of Justice’s “China

³ Ibid, 14–15. See also: Stéphane Lefebvre, “Academic-Intelligence Relationships: Opportunities, Strengths, Weaknesses and Threats,” *Journal of Policing, Intelligence and Counter Terrorism* 16, no. 2 (2021), <https://doi.org/10.1080/18335330.2021.1880020>.

⁴ Kathleen M. Vogel et al., “The Importance of Organizational Innovation and Adaptation in Building Academic-Industry-Intelligence Collaboration: Observations from the Laboratory for Analytic Sciences,” *The International Journal of Intelligence, Security, and Public Affairs* 19, no. 3 (2017), <https://doi.org/10.1080/23800992.2017.1384676>.

⁵ Larry Diamond and Orville Schell, eds. *China’s Influence & American Interests: Promoting Constructive Vigilance*. Report of the Working Group on Chinese Influence Activities in the United States, rev. ed. (Stanford, CA: Hoover Institution Press, 2019).

Initiative.”⁶ While the scale of Chinese espionage may be overstated, similar concerns have been raised by the governments of the UK, Germany, and Australia, emphasizing the risks posed by adversarial actors.

Elizabeth A. Rowe, a Professor of Law at the University of Virginia School of Law, investigated cases of academic espionage and compiled a list of eleven Chinese “professors in handcuffs.” She interpreted these cases as evidence of a disconnect between the individual criminal liability of academic staff and the distributed accountability of universities as legal entities.⁷ Despite controversies surrounding the measures adopted by the US authorities, reports detailing extensive espionage efforts to circumvent research security protocols and exploit the principles of open science for adversarial purposes have also been released by the governments of the UK, Germany, and Australia. While these reports primarily focus on China’s operations, they also underscore escalating espionage activities by Russia, particularly after 2022.⁸

2. Personal Ties Between Academia and Intelligence

Scholars can become associated with intelligence institutions in various ways. From the perspective of national intelligence services in a scholar’s country of residence, their knowledge, expertise, experience, and exceptional intellectual capabilities are regarded as particularly valuable resources. Scholars are often approached for cooperation, typically in an advisory capacity, to help intelligence services refine their intelligence cycle and enhance analytical capabilities. For example, media reports have highlighted that distinguished American academics such as Robert Jervis, Joseph S. Nye, and H. Bradford Westerfield served as advisors to the CIA.⁹ A specific

⁶ Kathleen M. Vogel and Sonia Ben Ouagrham-Gormley, “Scientists as Spies? Assessing U.S. Claims about the Security Threat Posed by China’s Thousand Talents Program for the U.S. Life Sciences,” *Politics and the Life Sciences* 42, no. 1 (2023), <https://doi.org/10.1017/pls.2022.13>.

⁷ Eileen Guo, Jess Aloe, and Karen Hao, “The US Crackdown on Chinese Economic Espionage Is a Mess. We Have the Data to Show It,” *MIT Technology Review*, December 2, 2021, <https://www.technologyreview.com/2021/12/02/1040656/china-initiative-us-justice-department/>.

⁸ Alexander Martin, “British Intelligence Moves to Protect Research Universities from Espionage,” *The Record*, April 26, 2024, <https://therecord.media/MI5-protect-british-universities-from-espionage>.

⁹ David N. Gibbs, “Academics and Spies: The Silence That Roars,” *Los Angeles Times*, January 28, 2001, <https://irp.fas.org/news/2001/01/lat012801.html>.

pattern has emerged in the field of intelligence studies, where former intelligence officials are hired as faculty members. They bring practical knowledge and firsthand experience, enriching academic discourse and contributing to the professional education of future intelligence personnel. From a counterintelligence perspective, academia is a significant target for espionage and adversarial intelligence activities by foreign services. These entities aim to identify and recruit informants among students and professors. If successful, they can gain access to restricted or sensitive research data or collect large volumes of data generated in critical fields of science and technology.

3. Future Careers

Outstanding students, top graduates, and prominent activists within student circles are often targeted as valuable assets for long-term collaboration with intelligence institutions. Domestic intelligence services employ headhunting strategies to recruit individuals with high potential as effective personnel. Conversely, adversary services deploy tactics to identify and groom potential agents of influence by offering discreet assistance—whether material or financial—facilitating career advancements or integrating them into strategically designed networks of influence. The case of Ana Montes serves as a compelling example of how academia can function as a fertile environment for recruitment.¹⁰

It is overly optimistic to regard academia as a “neutral ground” where the noble pursuit of science is achieved through the objective search for truth. The collegial academic environment, characterized by a spirit of freedom, openness, and the unrestricted exchange of ideas, has long been a hallmark of academia’s role in a complex and interconnected world. Features such as unrestricted access to university facilities, open admissions to conferences, seminars, and public lectures, minimal security screening of students enrol-

¹⁰ Ana Belen Montes was a graduate student at the Johns Hopkins University where she was recruited in 1984 by a fellow student to collaborate with the Cuban Intelligence Directorate (G2). Under guidance from G2 officers, she was employed as an intelligence analyst at the Defense Intelligence Agency (DIA) and later became its most senior Cuban analyst.

ling in programs, and tolerance for unconventional or unorthodox behaviors displayed by students or faculty have traditionally been seen as valuable and integral to academic culture.

However, as Anthony Bishop—an academic and former CIA officer—notes, these very attributes create “the perfect opportunity for undercover foreign intelligence officers or their human sources to slip onto campus and search for students who have potential for entering sensitive positions in the US. government or landing jobs with American companies engaged in the development and production of emerging and advanced technologies.”¹¹ Elisabeth A. Rowe underscores that “academia is grounded not in a culture of ownership and secrecy, but of openness and sharing.”¹² Yet, this culture—geared towards disseminating research outcomes through papers, articles, books, speeches, seminars, and conferences—renders academia “a valuable, vulnerable, and low-risk target for foreign espionage.”¹³ While open science promotes greater accessibility, inclusivity, and transparency, advancing the right of all individuals to share in scientific progress and its benefits, it does not adequately address the challenges of safeguarding scientific achievements against unlawful or malicious exploitation by academic and non-academic actors alike.

Recommendations

The challenge of safeguarding academia’s principles of open research and scientific freedom against malicious activities, particularly those conducted by intelligence services, can be addressed through the following recommendations:

Awareness raising through training courses for faculty and administrative staff

Both basic and advanced training courses should be implemented to heighten awareness of the risks and vulnerabilities that make academia a target

¹¹ Anthony Bishop, “International Espionage on Campus,” *The World Deciphered*, November 6, 2016, https://www.thecipherbrief.com/column_article/international-espionage-on-campus.

¹² Elisabeth A. Rowe, “Academic Economic Espionage?” *William & Mary Law Review* 65, no. 1 (2023), 7, <https://scholarship.law.wm.edu/wmlr/vol65/iss1/2>.

¹³ Daniel Golden, *Spy Schools: How the CIA, FBI, and Foreign Intelligence Secretly Exploit America’s Universities* (New York: Henry Holt & Co., 2017), 23.

for espionage. Such courses can be designed and delivered systematically by intelligence professionals in collaboration with university authorities.

Resilience building through security preparedness for sensitive research and educational programs

Scholars engaged in sensitive and high-stakes research should receive proper guidance on the risks posed by foreign intelligence services. They must also be held accountable for ensuring that the outcomes of their research are handled responsibly and securely.

Ethics and diligence in open science (addressing the AI dilemma)

The growing reliance on AI-driven research necessitates the establishment of robust regulations and standards to ensure full adherence to ethical principles and due diligence. These measures will mitigate risks without stifling innovation.

Stricter knowledge management and intellectual property protection

Security vetting of key research projects should become standard practice to prevent unauthorized or illicit access to sensitive findings. Universities must cultivate a culture of proprietary awareness and establish systematic infrastructures for safeguarding intellectual property. While these measures do not undermine the principle of open science, they promote a more prudent approach to managing research outcomes and translating them into practical applications.

A more targeted visa policy

Universities, in coordination with relevant authorities, should implement a more nuanced approach to long-term visa issuance. While protecting individuals' rights to study and reside (including students and faculty), visa processes can serve as an initial screening mechanism to reduce the risk of infiltration by individuals potentially involved in espionage.

Effective and balanced cooperation with state security and counterintelligence agencies

Elizabeth A. Rowe described the academic sphere as a site of “collision between espionage, secrecy, national security, criminal law, and the academic environment.”¹⁴ This contrasts with Liam Francis Gearon’s symbiotic perspective, highlighting divergent views on academia’s role within the interplay of government, security services, the judiciary, private enterprise, and civil society. Despite academia’s discomfort with such entanglements, the growing scale and diversity of espionage activities targeting universities require decisive, precautionary measures. These actions should involve close collaboration between university authorities and state security agencies.

A Necessary Disclaimer

The above recommendations apply to academic environments where the principles of open science serve as the foundation for education and research. They are not intended for authoritarian systems, where ideological agendas and political objectives often suppress academic freedom. In such regimes, partnerships between academia and intelligence services are typically government-mandated, aiming to place universities and research institutions under strict control and surveillance. Under these conditions, academia often becomes a tool of the state, unable to fulfill its mission of advancing truly open science.

The challenge of safeguarding academia’s principles of open research and scientific freedom against malicious activities, particularly those conducted by intelligence services, can be addressed through the following recommendations:

- Awareness raising through training courses for faculty and administrative staff.
- Resilience building through security preparedness for sensitive research and educational programs.
- Ethics and diligence in open science (addressing the AI dilemma).
- Stricter knowledge management and intellectual property protection.

¹⁴ Elizabeth A. Rowe, “Academic Economic Espionage?” *William & Mary Law Review* 65, no. 1 (2023), 76, <https://scholarship.law.wm.edu/wmlr/vol65/iss1/2>.

- A more targeted visa policy.
- Effective and balanced cooperation with state security and counterintelligence agencies.

Bibliography

- UNESCO. "An introduction to the UNESCO Recommendation on Open Science." *Canadian Commission for UNESCO*, 2022. <https://doi.org/10.54677/XOIR1696>.
- Bishop, Anthony. "International Espionage on Campus." *The World Deciphered*, November 6, 2016. https://www.thecipherbrief.com/column_article/international-espionage-on-campus.
- Diamond, Larry and Orville Schell, eds. *China's Influence & American Interests: Promoting Constructive Vigilance. Report of the Working Group on Chinese Influence Activities in the United States*, rev. ed. Stanford: Hoover Institution Press, 2019.
- Gearon, Liam Francis. "The University-Security-Intelligence Nexus: Four Domains." In *The Routledge International Handbook of Universities, Security and Intelligence Studies*, edited by Liam Francis Gearon. Routledge, 2020, 15.
- Gibbs, David N. "Academics and Spies: The Silence That Roars." *Los Angeles Times*, January 28, 2001. <https://irp.fas.org/news/2001/01/lat012801.html>.
- Golden, Daniel. *Spy Schools: How the CIA, FBI, and Foreign Intelligence Secretly Exploit America's Universities*. New York: Henry Holt & Co., 2017.
- Guo, Eileen, Jess Aloe and Karen Hao. "The US Crackdown on Chinese Economic Espionage Is a Mess. We Have the Data to Show It." *MIT Technology Review*, December 2, 2021. <https://www.technologyreview.com/2021/12/02/1040656/china-initiative-us-justice-department/>.
- Lefebvre, Stéphane. "Academic-Intelligence Relationships: Opportunities, Strengths, Weaknesses and Threats." *Journal of Policing, Intelligence and Counter Terrorism* 16, no. 2 (2021). <https://doi.org/10.1080/18335330.2021.1880020>.
- Martin, Alexander. "British Intelligence Moves to Protect Research Universities from Espionage." *The Record*, April 26, 2024. <https://therecord.media/MI-5-protect-british-universities-from-espionage>.
- European Commission. "Open Science." *European Commission*, 2024. https://research-and-innovation.ec.europa.eu/strategy/strategy-2020-2024/our-digital-future/open-science_en.

ACADEMIC ESPIONAGE: FINDING A BETTER BALANCE BETWEEN OPEN SCIENCE...

- Rowe, Elizabeth A. "Academic Economic Espionage?" *William & Mary Law Review* 65, no. 1 (2023). <https://scholarship.law.wm.edu/wmlr/vol65/iss1/2>.
- Vogel, Kathleen M., and Sonia Ben Ouagrham-Gormley. "Scientists as Spies? Assessing U.S. Claims about the Security Threat Posed by China's Thousand Talents Program for the U.S. Life Sciences." *Politics and the Life Sciences* 42, no. 1 (2023): 32–64. <https://doi.org/10.1017/pls.2022.13>.
- Vogel, Kathleen M., et al. "The Importance of Organizational Innovation and Adaptation in Building Academic-Industry-Intelligence Collaboration: Observations from the Laboratory for Analytic Sciences." *The International Journal of Intelligence, Security, and Public Affairs* 19, no. 3 (2017). <https://doi.org/10.1080/23800992.2017.1384676>.