Research Paper

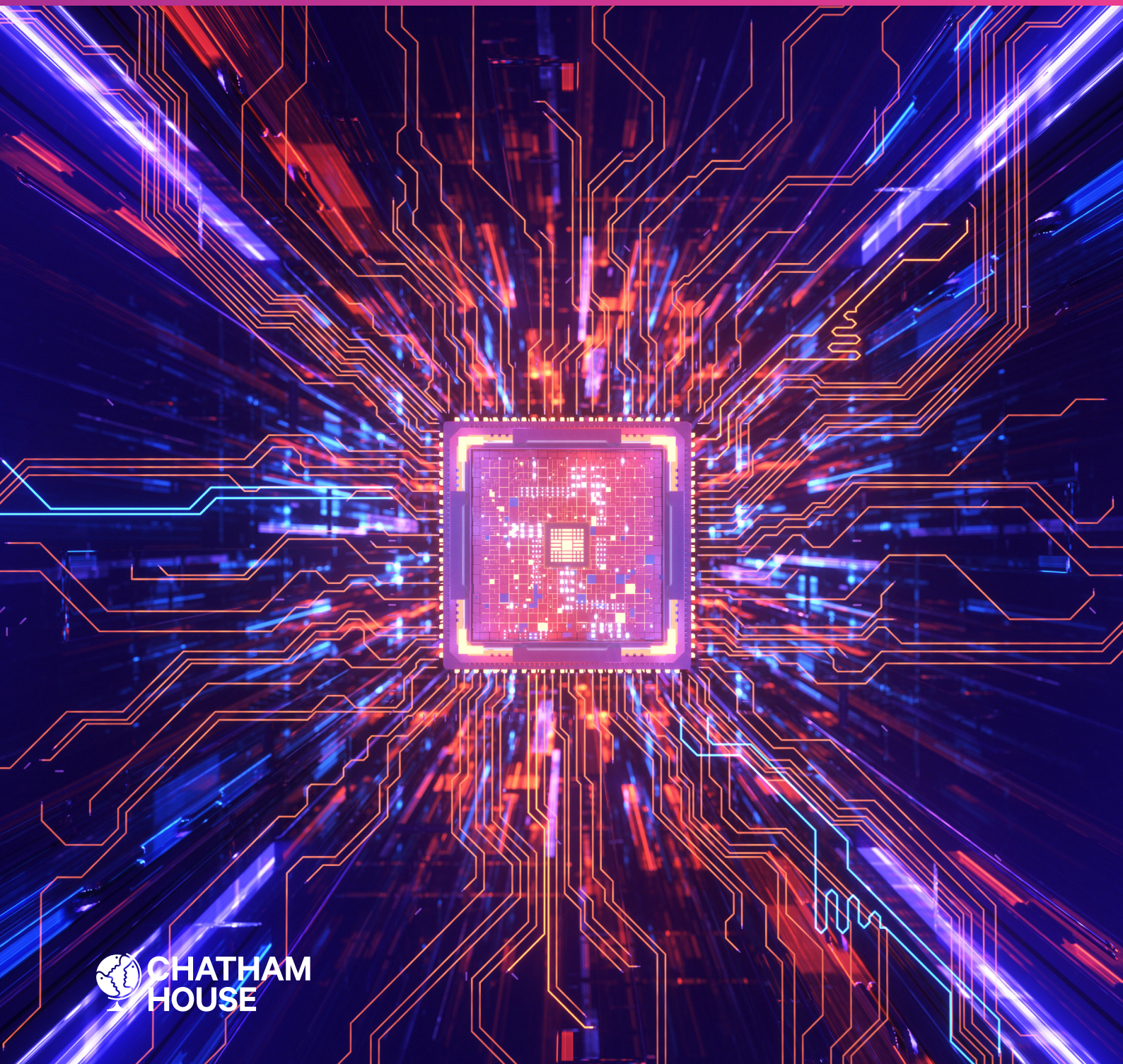
UK in the World Programme

September 2026

How the UK should protect its science and tech research from foreign state threats

A case for a more systemic approach to research security

Tahlia Peterson



CHATHAM HOUSE

Chatham House is a world-leading policy institute with a mission to address geopolitical challenges and international problems. Through this, we aim to help governments and societies to build a secure, sustainable, prosperous and just world.

Contents

Summary

The UK's world-class research in science and technology relies on openness and international collaboration, but these characteristics create vulnerabilities that foreign states – particularly China – can exploit. How can the UK strengthen its 'research security' without undermining innovation?

- As states increasingly view technological leadership as a source of economic power, military capability and national resilience, the cutting-edge research, expertise and knowledge held within the UK's university system have become targets for foreign state actors seeking strategic advantage. This paper sets out how the UK can better protect its university-derived science and technology (S&T) research assets from theft and malign transfer to foreign state actors.
- Improving 'research security' – as it is commonly termed – has emerged as an increasingly significant issue in UK national security and S&T policy. Research security can be understood as the suite of policies, institutional practices and legal mechanisms intended to protect sensitive intellectual property (IP), knowledge and expertise from espionage, theft and unauthorized transfer by foreign state actors or their proxies.
- China represents the UK's most significant and systemic research security challenge. While collaboration with China continues to generate important academic and economic benefits for the UK, the scale, nature and sophistication of Beijing's approach to gaining technological advantage create risks that distinguish China from other international research partners.
- In recent years, the UK has strengthened its research security architecture. However, because the framework has evolved reactively and in piecemeal fashion, protections remain inadequate in the face of emerging risks. Mechanisms and responsibility for addressing threats are dispersed across multiple institutions. As geopolitical competition intensifies and threat actors become more sophisticated, this paper argues, research security must move beyond a largely self-assessed, compliance-based model towards a more strategic, proactive and adaptable system. This system must be capable of anticipating and responding to complex threats.

- A number of structural characteristics of the higher education sector, combined with the inherent policy challenges of research security, hamper effective implementation of the UK's current research security policies. These obstacles include fragmented governance, uneven institutional capability, universities' financial dependence on international student fee income, and incentive structures that often prioritize research growth and international engagement over security considerations.
- The long-term challenge is to develop a coherent research security strategy that enables universities to remain globally connected and open, while safeguarding the knowledge, talent, data and technologies that underpin the UK's enduring S&T advantages from undue foreign exploitation.
- Recognizing the need for integrated responses, this paper recommends policy change across three interrelated domains:
  - **Strategic:** The government should embed research security in the UK's S&T, industrial and national security strategies. This means strengthening cross-government coordination, bolstering capacity to develop and retain technologies that confer strategic advantage, deepening collaboration with trusted international partners, and integrating universities more closely into the UK's defence-industrial base.
  - **Regulatory and governance:** Research security threats must be addressed systematically within the UK academic sector's research funding, governance and incentive structures. This will require the government – supported by universities and public and sectoral bodies – to take the following steps: (1) integrate research security into the higher education sector's existing Research Excellence Framework (REF); (2) put into operation a dedicated research security fund to support institutional capability; (3) strengthen the role of UK Research and Innovation (UKRI) – a non-departmental public body responsible for funding investment in research – in research security assurance as a supplement to internal university due diligence and wider government regulation; and (4) improve transparency around foreign affiliations, funding and research partnerships through proportionate regulatory reform.
  - **Operational:** Universities, with the support of government, need to increase their institutional capability by professionalizing the research security workforce, strengthening processes for information-sharing, and enhancing risk management across the lifecycle of S&T research. The government will also need to expand the capacity and authority of its Research Collaboration Advice Team (RCAT).

01 Introduction

Research in science and technology is key to the UK's long-term economic prospects, military strength, national resilience and geopolitical influence. As an open research ecosystem, the UK must balance the benefits of international collaboration with the need to protect strategically important intellectual assets from exploitation.

'Science has no borders, but scientists have motherlands.'
Xi Jinping, September 2020[1]

Advances in emerging science and technology (S&T) fields such as artificial intelligence (AI), quantum technologies and engineering biology hold profound transformative potential. These and other disruptive technologies are expected to revolutionize scientific discovery, medicine and a wide range of sectors in the modern economy, from manufacturing and energy to public service delivery. However, today, innovations developed for benign civilian purposes are often inherently dual-use, meaning that they can also be deployed for military and intelligence ends.[2] When exploited by malign actors, such capabilities can pose significant threats to national security and erode the foundations of peace and prosperity.

States that lead in frontier technologies are better positioned to establish technical standards, shape global norms and project influence through the capabilities on which others depend. As a result, a nation's capacity to secure technological

1 Creemers, R., Kania, E., Zhong, R. and Webster, G. (2020), 'Translation: Xi Jinping's Sept. 2020 Speech on Science and Technology Development', DigiChina, Stanford University, 22 September, 2020, https://digichina.stanford.edu/work/xi-jinpings-sept-2020-speech-on-science-and-technology-development-translation.
2 Schmidt, E. (2023), 'Innovation Power: Why Technology Will Define the Future of Geopolitics', *Foreign Affairs*, 28 February 2023, https://www.foreignaffairs.com/united-states/eric-schmidt-innovation-power-technology-geopolitics; Horowitz, M. C. (2018), 'Artificial Intelligence, International Competition, and the Balance of Power', *Texas National Security Review*, 1(3), pp. 36–57, https://doi.org/10.15781/T2639KP49.

advantage has become a foundational determinant of military capability, national resilience and geopolitical influence.[3]

As technological leadership increasingly determines each nation's position within the international order, S&T has become a predominant arena of global competition, most notably between the US and China.[4] For so-called 'middle powers' such as the UK,[5] this environment presents both opportunities and challenges. While the UK lacks the industrial scale and fiscal capacity of the US or China, it retains significant strengths, including world-class universities, a productive research base and established eminence across several technology sectors. Recognizing the growing importance of S&T to national power, successive UK governments have identified the pursuit of 'strategic advantage through science and technology' as a priority,[6] emphasizing the need to develop sovereign capabilities and reduce dependencies in frontier technologies.[7]

However, the UK's strengths are embedded in an open research ecosystem centred on universities. International collaboration, researcher mobility and global knowledge exchange are essential to scientific excellence, but also create exploitable opportunities for foreign state actors to acquire knowledge, intellectual property (IP) and expertise in S&T fields through unauthorized means.

Concerns regarding national security risks affecting the UK research sector have intensified. In April 2024, MI5 director general Ken McCallum briefed the vice-chancellors of 24 leading UK universities on the security service's concerns about unprecedented foreign state threats to the sector.[8] This followed a rare joint warning by the Five Eyes intelligence chiefs regarding what was described as China's 'sustained, scaled, and sophisticated' efforts to acquire sensitive research, expertise and IP through malign means.[9]

---

3 Parton, C. (2025), *China, science and technology: Advancing geopolitical aims*, Report, China Observatory, Council on Geostrategy, https://www.geostrategy.org.uk/all-research/china-science-and-technology-advancing-geopolitical-aims; Searle, N., Ganglmair, B. and Borghi, M. (2025), *Trusted Research and Innovation: How Knowledge Leakage Affects the Research & Innovation Ecosystem*, Innovation & Research Caucus, IRC Report No. 24, 19 June 2025, https://ircaucus.ac.uk/publications/trusted-research-and-innovation-how-knowledge-leakage-affects-the-research-innovation-ecosystem.

4 Zhang, J. (2024), *Artificial Intelligence with Chinese Characteristics: National Strategy, Security and Authoritarian Governance*, Oxford: Oxford University Press; Suleyman, M. and Bhaskar, M. (2023), *The Coming Wave: Technology, Power, and the Twenty-First Century's Greatest Dilemma*, London: Bodley Head.

5 Although the meaning of the term is open to interpretation and often imprecise, for the purpose of this paper 'middle powers' can be understood as countries that occupy an intermediate position in the international spectrum of power. They possess neither the overwhelming capabilities of 'great powers', which can exert global influence through economic, military and technological dominance, nor the limited capacity of 'small powers', but retain sufficient resources and influence to shape international outcomes and advance their sovereign interests.

6 UK Cabinet Office (2021), *Global Britain in a Competitive Age: The Integrated Review of Security, Defence, Development and Foreign Policy*, London: HM Government, https://www.gov.uk/government/publications/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy; UK Cabinet Office (2023), *Integrated Review Refresh 2023: Responding to a more contested and volatile world*, London: HM Government, p. 31, https://www.gov.uk/government/publications/integrated-review-refresh-2023-responding-to-a-more-contested-and-volatile-world.

7 UK Cabinet Office (2025), *National Security Strategy 2025: Security for the British people in a dangerous world*, London: HM Government, p. 44, https://www.gov.uk/government/publications/national-security-strategy-2025-security-for-the-british-people-in-a-dangerous-world.

8 Williams, N. (2024), 'Foreign States targeting UK universities, MI5 warns', BBC News, 26 April 2024, https://www.bbc.co.uk/news/uk-68902636.

9 Hoover Institution (2023), 'FBI Director Christopher Wray and Heads of Foreign Security Agencies Convene at Stanford to Address Threat to Innovation Posed by China', news release, 18 October 2023, https://www.hoover.org/fbi-director-christopher-wray-and-heads-foreign-security-agencies-convene-stanford-address-threat.

It is within this context that 'research security' has emerged as a central policy concern. Broadly defined in this paper, research security refers to the suite of policies, institutional practices and legal mechanisms intended to protect sensitive IP, knowledge and expertise in the research sector from espionage, theft and unauthorized transfer by foreign state actors or their proxies.[10] (In the UK policy context, the term 'trusted research' is also used in official documents and guidance to refer to the framework of principles, practices and safeguards intended to support the integrity and security of international research collaboration.)[11]

Research security presents policymakers with a fundamental dilemma: how to strike the appropriate balance between preserving the openness essential to a thriving research ecosystem and imposing the controls necessary to protect national security.

Research security presents policymakers with a fundamental dilemma: how to strike the appropriate balance between preserving the openness essential to a thriving research ecosystem and imposing the controls necessary to protect national security. Excessively restrictive approaches risk weakening the very research ecosystem they would seek to protect, as such controls could reduce collaboration and knowledge transfer, discourage global talent mobility and stifle innovation.[12] Yet insufficient safeguards may expose strategically significant knowledge and capabilities to transfer, exploitation or misuse, ultimately to the detriment of UK and allied interests.

These challenges are compounded in the UK by the structural misalignment between the financial incentives of universities and the national security concerns of government. The higher education sector, facing fiscal constraints, increasingly relies on foreign student fee income, international talent and international collaboration to sustain research activity; at the same time, policymakers are ever more focused on *preventing* the transfer of sensitive S&T capabilities to foreign state actors.[13]

Effective governance is further complicated by the imperative of keeping pace with rapidly evolving technological change, and by the increasing difficulty

---

10 Adapted from Walker-Munro, B. (2025), *Shifting the needle: Making Australia's research security ecosystem work smarter*, Policy Brief, Canberra: Australian Strategic Policy Institute, p. 5, https://aspi.s3.ap-southeast-2.amazonaws.com/wp-content/uploads/2025/06/25132557/Shifting-the-needle.pdf.
11 The term 'trusted research' is often used interchangeably with 'research security', the former having emerged from the 'Trusted Research' guidance initiative developed jointly by the National Protective Security Authority (NPSA) and National Cyber Security Centre (NCSC).
12 Shih, T. and Wagner, C. S. (2024), 'The Trap of Securitizing Science', *Issues in Science and Technology*, 41(1), pp. 100–03, https://doi.org/10.58875/ZSDO9141.
13 Coombs, H., Otway, A. and Iosad, A. (2025), 'Data Decoded: UK Higher Education, Immigration and Financial Sustainability', Commentary, Tony Blair Institute for Global Change, 20 June 2025, https://institute.global/insights/public-services/data-decoded-uk-higher-education-immigration-and-financial-sustainability; Zhang, C. (2025), 'Market–security tensions in UK–China academic engagement: perspectives from UK higher education', *Asian Review of Political Economy*, 4(14), https://doi.org/10.1007/s44216-025-00057-5.

of distinguishing between civilian and military applications of research.[14] Reconciling these competing objectives cannot be achieved through technical regulation alone; it requires sustained political leadership, a willingness to make strategic trade-offs in an environment of fiscal constraint, and the capacity to maintain a consistent policy direction over many years.

This paper examines how the UK can meet these challenges. Specifically, it explores how policymakers might strike an appropriate balance between scientific openness and security while ensuring that policy remains effective and adaptable to a future likely to be characterized by greater uncertainty, geopolitical friction and technological rivalry. The author argues that safeguarding the UK's long-term S&T advantages will require successive governments to treat research security as an enduring priority, and to avoid the reactive approaches seen to date. This will demand sustained political commitment from one administration to the next. It will also require a clear-eyed assessment of the national security risks posed by S&T collaboration with states – notably China – whose strategic objectives are likely to continue to conflict with those of the UK. Without such resolve, the UK's ambition to foster and sustain strategic advantage through S&T will become increasingly difficult to realize.

Methodology and scope

The paper draws on evidence gathered through four complementary research activities:

- **Desk research and literature review.** The author reviewed academic and grey literature on research security, the geopolitics of S&T competition, and UK government policy and legislation. The author also reviewed English translations of Chinese official documents.
- **Semi-structured interviews.** The author conducted 35 research interviews. The interviewees consisted of a range of academics, business development personnel and professional research security staff – including personnel in due diligence, regulatory compliance, research governance and policy roles – across the UK university sector, as well as government representatives and experts from industry bodies. The interviews explored perceptions of the current threat environment, the effectiveness of existing research security mechanisms, implementation challenges, and areas for policy and operational improvement.
- **Futures forecasting workshop.** The UK in the World Programme at Chatham House brought together subject matter experts on UK S&T policy to conduct a futures forecasting workshop, using structured analytical techniques to assess the UK's potential position within the global S&T landscape over the next five

14 Genus, A. and Stirling, A. (2018), 'Collingridge and the dilemma of control: Towards responsible and accountable innovation', *Research Policy*, 47(1), pp. 61–69, https://doi.org/10.1016/j.respol.2017.09.012; Marwaha, S., Timlin, J., Dickson, L. and Johnson, J. (2025), *Stronger cooperation, safer collaboration: Driving research security cooperation across Europe*, London: Association of Research Managers and Administrators, https://arma.ac.uk/wp-content/uploads/2025/06/Stronger-cooperation-safer-collaborations-report.pdf.

years. The exercise examined the implications of different future trajectories of the global S&T environment for the UK's national security, economic competitiveness and geostrategic influence, and for S&T policy settings.

— **Comparative policy analysis.** The author undertook comparative analysis of research security approaches in other relevant jurisdictions. This work involved desk-based research and interviews with subject matter experts on the policy experiences of Australia, Japan and Canada, including asking interviewees about their country's responses to state-based threats targeting national research ecosystems.

The scope of this paper is limited to the following themes:

— Research security is defined in this paper as the protection of sensitive IP, knowledge and expertise in emerging S&T fields from espionage, theft and unauthorized transfer by foreign state actors or their proxies. While foreign interference and transnational repression in the higher education sector – including efforts to monitor or suppress criticism of foreign states within UK universities, or to influence research agendas in line with foreign state objectives – are recognized as related security issues, they fall outside the scope of this study.

— The paper focuses on the university sector. Although research security risks and mitigation measures also apply to university spin-outs and the wider S&T commercial ecosystem, universities are the primary subject of this study due to the distinctive and acute challenges they face.

— The study examines state threats to research in fields identified as critical technologies within the UK government's Science and Technology Framework.[15] These fields include AI, engineering biology, quantum technologies, advanced connectivity technologies (previously referred to in government policy documents as 'future telecommunications') and semiconductors.

— This research primarily focuses on non-cyber threat vectors that rely on what can be termed 'non-traditional collection': that is, the acquisition of sensitive S&T knowledge and IP through human actors and mechanisms that often operate within the bounds of legitimate academic or commercial activity. Such activities can involve individuals who are not formal intelligence operatives, but who may nonetheless be directed, incentivized or leveraged – wittingly or unwittingly – by foreign states or their proxies to obtain strategically significant knowledge and expertise. The theft and transfer of research through *cyber* means by malign actors is relevant and briefly explored, but that threat is outside the detailed scope of this paper.

15 Department for Science, Innovation and Technology (2023), 'Science and Technology Framework', Policy Paper, 28 April 2025, https://www.gov.uk/government/publications/science-and-technology-framework/science-and-technology-framework.

02
The global science and technology environment

Intensifying US–China tech competition and the securitization of S&T are narrowing the strategic space for middle powers to pursue autonomous policy choices. For the UK, maintaining influence will depend on developing comparative advantage in critical niches while safeguarding the research ecosystem that enables innovation.

Technological capability has long been a driver of geopolitical competition, from the Industrial Revolution through to the nuclear age and the space race of the mid-twentieth century. However, in recent years science and technology (S&T) has arguably taken on unprecedented strategic significance. What distinguishes the contemporary period is not simply the pace of technological change, but the emergence of multiple transformative and general-purpose frontier technologies simultaneously.[16]

Today's S&T environment is more internationally interconnected than ever before. Technological leadership in frontier fields relies upon global talent networks, international research collaboration, and integrated supply chains spanning multiple jurisdictions.[17] This globalized innovation ecosystem creates opportunities for accelerated scientific discovery and diffusion of knowledge. Yet it also introduces new vulnerabilities, including exposure to external dependencies that may be leveraged by more powerful states for strategic advantage or coercion.

16 Suleyman and Bhaskar (2023), *The Coming Wave.*
17 Krelina, M. (2025), *Military and Security Dimensions of Quantum Technology: A Primer*, Stockholm: Stockholm International Peace Research Institute, https://doi.org/10.55163/ZVTL1529.

These dynamics have contributed to the rise of what can be termed 'techno-nationalism' or 'techno-economic statecraft': the tendency for states to view technological capability, supply chains and innovation ecosystems as instruments of statecraft, rather than simply as domains of scientific collaboration and commercial activity.[18] Across advanced economies, governments are adopting more interventionist approaches to S&T policy; many are deploying industrial strategy, investment screening, regulation and national security measures to strengthen their sovereign capabilities, protect critical technologies and reduce strategic vulnerabilities.[19]

Great power competition

A defining feature of this environment is intensifying strategic competition between the US and China. Both powers increasingly regard technological leadership as central to their long-term prosperity, military power and geopolitical influence, and have adopted policies intended to strengthen domestic innovation while restricting rivals' access to strategic technologies. The result is a self-reinforcing dynamic whereby efforts by one side to reduce vulnerabilities, secure supply chains or restrict technology transfers are interpreted by the other as strategic challenges requiring countermeasures.

This geopolitically linked competition intensified during the late 2010s as US concerns over China's rapid technological rise and acquisition of foreign IP and expertise, and the strategic implications of growing technological interdependence, prompted a reorientation of S&T policy in the US. Assumptions that technological progress was best served by open, market-led innovation gave way to tighter US controls on the transfer of technology and knowledge. Successive US administrations strengthened foreign investment screening and export controls, particularly targeting advanced semiconductors and semiconductor manufacturing equipment destined for China; this was in an effort to limit China's ability to leverage Western technological strengths and degrade US advantage, and involved controlling the transfer of critical technological inputs and capabilities underpinning advanced computing and AI to China.[20] Enactment in the US of the 2022 CHIPS and Science Act and the 2022 Inflation Reduction Act reflected a parallel shift towards prioritizing domestic industrial strategy, supported

18 Capri, A. (2025), *Techno-nationalism: How It's Reshaping Trade, Geopolitics and Society*, Hoboken, NJ: John Wiley & Sons; Lee, S. (2024), 'U.S.-China Technology Competition and the Emergence of Techno-Economic Statecraft in East Asia: High Technology and Economic-Security Nexus', *Journal of Chinese Political Science*, 29, pp. 397–416, https://doi.org/10.1007/s11366-023-09878-8.
19 Kara, O., O'Loughlin, R. F., Griffin, F. and Janjeva, A. (2025), *Seeking Deeper: Assessing China's AI Security Ecosystem*, Report, London: Centre for Emerging Technology and Security (CETaS), Alan Turing Institute, https://cetas.turing.ac.uk/sites/default/files/2025-07/cetas_research_report_-_seeking_deeper_-_assessing_chinas_ai_security_ecosystem.pdf; Aggarwal, V. K. and Reddie, A. W. (2020), 'New Economic Statecraft: Industrial Policy in an Era of Strategic Competition', *Issues & Studies*, 56(2), https://doi.org/10.1142/S1013251120400068.
20 Pernin, C. G. et al. (2026), *Research Security in Science and Technology*, Santa Monica, CA: RAND Corporation, https://www.rand.org/pubs/perspectives/PEA4104-1.html; Sutter, K. M. (2025), *U.S. Export Controls and China: Advanced Semiconductors*, Washington, DC: Congressional Research Service, https://www.congress.gov/crs_external_products/R/PDF/R48642/R48642.5.pdf.

by increased federal research and development (R&D) investment aimed at rebuilding the US's technological capacity and industrial base.[21]

Concurrently, the US government intensified its scrutiny of the US research sector. The Department of Justice's 'China Initiative', which ran from 2018 to 2022, targeted economic espionage, IP theft and undisclosed ties to Chinese entities that the US government deemed high-risk. The initiative focused on federally funded research in STEM fields[22] and on activities assessed as being linked to the Chinese state. Although discontinued following criticism over racial profiling and the programme's dampening effect on international S&T collaboration, the initiative contributed to a durable shift towards tighter federal oversight of the research sector.[23] Research security was further institutionalized by measures such as the National Security Presidential Memorandum-33 (NSPM-33),[24] issued in 2021, which established a government-wide baseline for research security and made compliance with standardized disclosure, research security and research integrity requirements a condition of eligibility for receipt of US federal research funding.

Central to China's approach is the concept of 'military–civil fusion', which aims to eliminate barriers between civilian and defence innovation, allowing scientific and technological advances developed in universities and industry to support military capability.

Meanwhile, China under President Xi Jinping has elevated S&T to the centre of national strategy, with technological primacy framed as essential not only for economic growth but also for national security, military modernization and what the political leadership calls the 'great rejuvenation of the Chinese nation'.[25] Policies such as 'Made in China 2025', the political leadership's Innovation-Driven Development Strategy and successive five-year plans have channelled state subsidies and incentives into strategic sectors with the aim of reducing dependence on foreign technologies and positioning China as a leading technological power.[26] Central to China's approach is the concept of 'military–civil fusion', which aims to eliminate barriers between civilian and defence innovation, allowing scientific

---

21 Calidas, D. and Li, C. (2025), *Beyond Rhetoric: The Enduring Political Appeal of U.S. Industrial Policy for Critical and Strategic Technologies*, Cambridge, MA: Belfer Center for Science and International Affairs, Harvard Kennedy School, https://www.belfercenter.org/research-analysis/beyond-rhetoric-us-industrial-policy.
22 STEM = science, technology, engineering and mathematics.
23 U.S. Department of Justice, Office of Public Affairs (undated), 'Department of Justice China Initiative Fact Sheet', https://www.justice.gov/opa/page/file/1122686/dl; German, M. (2024) 'The 'China Initiative' failed US research and national security. Don't bring it back.', Opinion, *The Hill*, 19 September 2024, https://thehill.com/opinion/national-security/4886821-china-initiative-restart-harmful; Shih and Wagner (2024), 'The Trap of Securitizing Science'; Vogel, K. M. and Ben Ouagrham-Gormley, S. (2023), '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(1), pp. 32–64, https://doi.org/10.1017/pls.2022.13.
24 The White House (2021), 'Presidential Memorandum on United States Government-Supported Research and Development National Security Policy', 14 January 2021, https://trumpwhitehouse.archives.gov/presidential-actions/presidential-memorandum-united-states-government-supported-research-development-national-security-policy.
25 Zhang (2024), *Artificial Intelligence with Chinese Characteristics*, p. 26.
26 Mei, S. and Huismans, J. (2026), *China's Science and Technology Strategy in Perspective: Historical Evolution, Political Drivers and Global Implications*, Santa Monica, CA: RAND, https://www.rand.org/pubs/research_reports/RRA4104-3.html; Parton (2025), *China, science and technology*.

and technological advances developed in universities and industry to support military capability. Complementing this is the drive, led by the Communist Party of China (CPC), to achieve technological self-reliance; this is intended to reduce dependence on foreign technologies while building indigenous strength across strategic sectors.[27]

The scale and speed of China's technological development have reshaped global perceptions of the innovation landscape. Research by the Australian Strategic Policy Institute (ASPI) suggests that China now leads globally across a majority of assessed frontier S&T domains, including AI, quantum sensing, advanced materials and biotechnology; ASPI's analysis puts China ahead in 66 of 74 technologies tracked.[28] Developments such as the rise of Chinese firm DeepSeek's AI models have challenged assumptions that China's state-led research system constrains innovation. By reportedly achieving near-frontier performance using less advanced chips but computationally efficient architecture and AI training techniques, DeepSeek has renewed debate over the effectiveness of US restrictions on advanced semiconductor exports as a means of maintaining US leadership in AI.[29]

These developments have generated cascading international effects, prompting other states to reassess dependencies, strengthen domestic capabilities, and introduce enhanced economic and research security measures. The EU's pursuit of technological sovereignty and strategic autonomy exemplifies this trend, and is driven by concerns over geopolitical overexposure, critical dependencies and threats to supply-chain resilience. This agenda has become increasingly urgent following Russia's full-scale invasion of Ukraine and amid growing uncertainty surrounding the long-term reliability of the US as a security partner under the second Donald Trump administration.

In parallel, US S&T policy under President Trump has become more volatile. While the administration has advanced select minilateral initiatives aimed at 'friendshoring' critical mineral[30] and semiconductor supply chains,[31] it has rolled back elements of previous policy architecture. Most notably, the rescinding of the Biden-era AI Diffusion Rule in May 2025 and the subsequent relaxation of restrictions on exports of NVIDIA's H200 advanced chips to China signalled a shift away from a rules-based export control framework towards a more flexible and transactional approach.[32] Although later measures have sought to tighten enforcement and close regulatory loopholes – including through strengthened restrictions on Department of War-funded research involving institutions deemed 'Foreign Institutions Engaging

---

27 Ibid.; Krelina (2025), *Military and Security Dimensions of Quantum Technology*; Kara, O'Loughlin, Griffin and Janjeva (2025), *Seeking Deeper*.
28 Leung, W. J., Robin, S. and Cohen, L. (2025), 'ASPI's Critical Technology Tracker: 2025 updates and 10 new technologies', The Strategist, Australian Strategic Policy Institute,1 December 2025, https://www.aspi.org.au/strategist-posts/aspis-critical-technology-tracker-2025-updates-and-10-new-technologies.
29 Kara, O'Loughlin, Griffin and Janjeva (2025), *Seeking Deeper*.
30 Blakemore, R. and Harmon, A. (2026), 'US critical minerals policy goes collaborative with FORGE', Atlantic Council, Dispatches, 12 February 2026, https://www.atlanticcouncil.org/dispatches/us-critical-minerals-policy-goes-collaborative-with-forge.
31 U.S. Department of State (2025), 'PAX Silica', https://www.state.gov/pax-silica.
32 Kozlowskyj, C. (2026), 'Trump Reverses US AI Chip Export Policy to China', Bloomsbury Intelligence & Security Institute, 9 February 2026, https://bisi.org.uk/reports/trump-reverses-us-ai-chip-export-policy-to-china.

in Problematic Activities', alongside Department of War-ordered research security audits of 30 US academic institutions[33] – the overall direction of policy raises questions about the consistency and durability of US strategy.

Stuck in the middle

For middle powers, including the UK, the growing securitization of S&T creates a more constrained strategic environment in which economic, technological and security choices are increasingly shaped by decisions in Washington and Beijing.[34] In contrast to the US and China, middle powers lack the market size, capital resources and technological breadth necessary to achieve self-sufficiency across as many aspects of critical technology. Moreover, such countries remain deeply dependent on global research networks, international talent flows, foreign investment, and supply chains increasingly affected by great power competition.

Within this international environment, middle powers find themselves caught between competing imperatives. Economic prosperity in the modern age depends on continued engagement with China through trade, research collaboration, investment and manufacturing networks. At the same time, for historically US-aligned liberal democratic states, security partnerships, intelligence cooperation and access to advanced military technology remain anchored to the US. Growing uncertainty surrounding Trump's transactional, 'America First' approach to foreign policy and alliances, alongside intensifying US–China rivalry, has complicated this balancing act. Decoupling from either power is neither feasible nor desirable, yet excessive dependence on either carries growing risks.[35]

The central challenge for middle powers is to preserve a degree of strategic autonomy. As the international economic and security order becomes more fragmented and less predictable, resilience and strategic leverage become increasingly important. For most middle powers, this does not mean pursuing technological self-sufficiency. Rather, it means identifying areas where they can develop sovereign capability, reduce critical dependencies, and retain influence despite lacking superpower scale.[36]

---

33 In July 2026, the US Department of War published an updated list of foreign institutions deemed to have engaged in problematic activities under section 1286 of the FY19 National Defence Authorization Act. Under the Act, the department is prohibited from using funds to conduct research involving collaboration with any listed entity, including 130 academic institutions located in China, Russia and Iran. U.S. Department of War (2026), 'The Department of War Releases Updated List of Foreign Institutions Engaging in Problematic Activities to Counter Unauthorised Technology Transfer', 23 July 2026, https://www.war.gov/News/Releases/Release/Article/4553101/the-department-of-war-releases-updated-list-of-foreign-institutions-engaging-in; U.S Department of War (2026), 'Department of War Orders Research Security Audits at 30 Academic Institutions', 17 August 2026, https://www.war.gov/News/Releases/Release/Article/4575019/department-of-war-orders-research-security-audits-at-30-academic-institutions.

34 Job, B. (2020), 'Between a Rock and a Hard Place: The Dilemmas of Middle Powers', *Issues & Studies*, 56(2), pp. 1–24, https://www.researchgate.net/publication/342725892_Between_a_Rock_and_a_Hard_Place_The_Dilemmas_of_Middle_Powers.

35 House of Lords International Relations and Defence Committee (2026), *Adjusting to new realities: rebalancing the UK-US partnership*, https://publications.parliament.uk/pa/ld5901/ldselect/ldintrel/290/290.pdf; Job (2020), 'Between a Rock and a Hard Place'; Matthews, W. (2025), *What the UK must get right in its China strategy: Resilience, flexibility and autonomy as core principles for engagement*, Research Paper, London: Royal Institute of International Affairs (Chatham House), https://www.chathamhouse.org/2025/07/what-uk-must-get-right-its-china-strategy; Wye, R. F. (2023), 'The UK's Response to the Challenge of Managing Its Relationships with China and the US', in Grano, S. A. and Huang, D. W. F. (eds), *China-US Competition: Impact on Small and Middle Powers' Strategic Choices*, Switzerland: Palgrave Macmillan, https://doi.org/10.1007/978-3-031-15389-1_8.

36 Matthews (2025), *What the UK must get right in its China strategy.*

For the UK, S&T represents one of the most important foundations of such leverage. Despite a relatively limited domestic market, the UK remains one of the world's leading S&T powers: it has the third-largest technology ecosystem by aggregate enterprise value – estimated at approximately US$1.2 trillion, behind only the US and China[37] – with strengths across a range of fields that include AI, quantum technologies, advanced materials, synthetic biology and advanced sensing.[38] These advantages are rooted less in industrial scale than in the strength of the UK's research and innovation ecosystem, particularly its universities. In an increasingly competitive global S&T landscape, the UK's ability to maintain strategic autonomy and national advantage will depend heavily on its capacity to protect and sustain these assets.

37 UK Government (2025), *The UK's Modern Industrial Strategy: Digital and Technologies Sector Plan*, https://assets.publishing.service.gov.uk/media/685862e5b328f1ba50f3cea4/industrial_strategy_digital_and_technologies_sector_plan.pdf.
38 Leung, J. W., Robin, S. and Cave, D. (2024), *ASPI's two-decade Critical Technology Tracker: The rewards of long-term research investment*, Report, Canberra: Australian Strategic Policy Institute, 28 August 2024, https://ad-aspi.s3.ap-southeast-2.amazonaws.com/2024-08/ASPIs%20two-decade%20Critical%20Technology%20Tracker_1.pdf.

03
State threats to UK universities

The culture of openness that makes UK universities world-leading also exposes them to exploitation by foreign states seeking technological advantage. China represents the most significant systemic challenge, leveraging a whole-of-state approach to technology acquisition that blurs civilian and military boundaries.

Universities occupy a critical position in the UK's S&T ecosystem. They are primary sites of scientific discovery, foundational research and early-stage technological innovation, while serving as central hubs of highly skilled STEM talent.[39] UK universities produce around 6 per cent of the world's research publications, despite the fact that the UK's population of 69 million accounts for less than 1 per cent of the global total; UK universities also rank first among countries assessed on field-weighted citation impact in research.[40] British universities function as key nodes within global research networks, facilitating the international exchange of knowledge and expertise. In doing so, they contribute not only to innovation and economic growth but also to the UK's international influence and soft power.[41]

The UK government's National Protective Security Authority (NPSA), an arm of MI5, has repeatedly warned that some states seek to exploit the openness of British universities and international research collaboration to acquire knowledge, IP, data and expertise that advance their own military, intelligence,

39 Universities UK (2023), 'How do universities lead world research?', https://www.universitiesuk.ac.uk/what-we-do/policy-and-research/publications/features/impact-universities-numbers/how-do-universities-lead-world-research.
40 UK Department for Science, Innovation and Technology (2025), 'International comparison of the UK research base, 2025', 5 June 2025, https://www.gov.uk/government/publications/international-comparison-of-the-uk-research-base-2025/international-comparison-of-the-uk-research-base-2025.
41 Hughes, M. et al. (2025), *Securing the UK's AI Research Ecosystem*, Report, Centre for Emerging Technology and Security, The Alan Turing Institute, March 2025, https://cetas.turing.ac.uk/publications/securing-uks-ai-research-ecosystem.

economic or strategic objectives.[42] The UK is particularly exposed to these threats because of the scale, calibre and international orientation of its higher education sector. While research excellence places UK universities at the forefront of global innovation, it makes them high-priority targets for foreign state actors.[43]

This exposure is amplified by the sector's deep international integration. Analysis by the Department for Science, Innovation and Technology (DSIT) in 2025 found that over 60 per cent of the UK's academic publications in 2022 were co-authored with at least one non-UK researcher, the highest share among the countries studied.[44] In the past decade, the government has encouraged UK universities to expand their 'transnational education' (TNE) offer by opening overseas campuses, joint institutes and collaborative research centres: as of the 2023/24 academic year, more than 650,000 students were pursuing UK degrees internationally. UK TNE has seen significant growth in the past decade, with the number of TNE students increasing by 70 per cent from around 380,000 in 2014/15 to roughly 645,000 in 2023/24.[45]

Analysis by the Department for Science, Innovation and Technology in 2025 found that over 60 per cent of the UK's academic publications in 2022 were co-authored with at least one non-UK researcher, the highest share among the countries studied.

Financial pressures compound these vulnerabilities. Universities have become increasingly reliant on international student fee income to support teaching and research. In 2023/24, international students accounted for approximately one-quarter of all UK higher education students, generating approximately 23 per cent of the income of UK universities.[46] Overseas students, particularly from China, are disproportionately concentrated in postgraduate STEM programmes, where they play a significant role in sustaining the UK's research capacity, particularly in engineering, computing and technology-intensive disciplines.[47]

---

42 National Protective Security Authority (2025), *Trusted Research: Guidance for Academics*, https://www.npsa.gov.uk/system/files/NPSA%20TR%20Guidance%20for%20Academics_2025.pdf.
43 Intelligence and Security Committee of Parliament (2023), *China*, https://isc.independent.gov.uk/wp-content/uploads/2023/07/ISC-China.pdf; Universities UK (2023), 'Security and risk: how universities can protect their research and people', 8 June 2023, https://www.universitiesuk.ac.uk/topics/funding-finance-and-operations/security-and-risk-how-universities-can.
44 UK Department for Science, Innovation and Technology (2025), 'International comparison of the UK research base, 2025'.
45 UK Government (2026), *The UK's International Education Strategy: Excellence in Education, Partnerships for Growth*, https://assets.publishing.service.gov.uk/media/696a6164448fedc1eb4248ef/international-education-strategy-2026.pdf; Universities UK International (2025), 'The scale of UK higher education transnational education 2023–24', 17 December 2025, https://www.universitiesuk.ac.uk/topics/international/scale-uk-higher-education-transnational-0?utm.
46 Bolton, P., Lewis, J. and Gower, M. (2026), *International students in UK higher education,* House of Commons Library, Research Briefing, https://commonslibrary.parliament.uk/research-briefings/cbp-7976.
47 Coe, J., Brodie, K. and Lister, J. (2025), *Powering the engine: The non-financial contribution of international postgraduate students to the UK*, Universities UK International, https://www.universitiesuk.ac.uk/universities-uk-international/insights-and-publications/uuki-publications/powering-engine-non-financial; Quimbre, F., Carlyon, P., Dewaele, L. and Drew, A. (2022), *Exploring Research Engagement with China: Opportunities and Challenges*, Santa Monica, CA: RAND Corporation, p. 1, https://www.rand.org/pubs/research_reports/RRA1839-1.html.

While the international and open character of UK higher education is a major source of scientific strength, it provides a broad attack-surface for foreign intelligence services and state-linked actors to exploit.

Why does this matter?

Research security is ultimately about protecting the UK's prosperity, national security and strategic advantages in an increasingly competitive technological environment. At the economic level, loss or leakage of sensitive IP, knowledge and expertise can erode competitive advantage and reduce financial returns on public and private research investment. As emerging technologies become increasingly concentrated around intangible assets and specialized know-how, the transfer of cutting-edge research and knowledge can enable foreign competitors to replicate UK capabilities without incurring the costs and risks associated with their development.[48]

In regard to national security, meanwhile, adversarial exploitation of UK research – even research conducted purely for civilian applications – may contribute directly or indirectly to the development of foreign state military or intelligence capabilities contrary to the UK's interests, due to the dual-use nature of the research in question[49] (see Table 1). Authoritarian countries, unconstrained by the rule of law and democratic principles, may use S&T knowledge and expertise they acquire to create and deploy technologies to strengthen surveillance, political repression and social control.[50] Strategically, any loss of critical S&T knowledge would risk undermining the UK's ability to shape global technology standards, governance frameworks, supply chains and innovation trajectories – this ability is central to maintaining long-term national competitiveness and strategic autonomy.[51]

Institutionally, universities potentially face reputational and operational risks should collaborations with international partners result in the misuse or theft of technology or IP or be perceived as having been subject to inadequate risk management. Such outcomes can affect public trust, international collaboration opportunities, and access to future funding streams across both government and industry.[52] As S&T innovation becomes more embedded in the UK's defence industrial strategy, high research security standards in the university sector are increasingly likely to feature as express criteria for the receipt of defence-related public funding. Perceptions of poor security practices will have an increasingly deleterious impact on an institution's ability to qualify for government grants.

---

48 Searle, Ganglmair and Borghi, M. (2025), *Trusted Research and Innovation*.
49 Intelligence and Security Committee of Parliament (2023), *China*.
50 Hoover Institution (2023), 'FBI Director Christopher Wray and Heads of Foreign Security Agencies Convene at Stanford to Address Threat to Innovation Posed by China'; National Protective Security Authority (2025), *Trusted Research: Guidance for Academics*.
51 Intelligence and Security Committee of Parliament (2023), *China*.
52 Universities UK (2020), *Managing Risks in Internationalisation: Security Related Issues*, https://www.universitiesuk.ac.uk/sites/default/files/uploads/Reports/managing-risks-in-internationalisation.pdf.

Table 1. Examples of 'dual-use' emerging technologies

	Civilian applications	Military or intelligence applications
AI	Processing, analysing and extrapolating insights from large data sets to support public service and financial management functions; natural language processing and translation tools; autonomous vehicles and devices.	Autonomous weapons systems; cognitive warfare, including AI-enabled information campaigns and social media manipulation; identification and exploitation of cyber vulnerabilities; optimized intelligence-targeting and analysis.
Quantum computing	Molecular modelling for medical and pharmaceutical research; financial, climate and materials modelling and optimization.	Breaking existing cryptographic systems and decrypting sensitive communications.
Quantum sensing	Geological mapping; environmental monitoring; advanced medical imaging and diagnostics.	GPS-independent military positioning, navigation and targeting systems.
Engineering biology	Vaccine development; drug discovery; genomic treatments for diseases; development of new agricultural food sources and biofuels.	Development of targeted biological agents (biological weapons); enhancement of human performance for military personnel.
Advanced connectivity technologies	5G/6G telecommunications; 'Internet of Things' (IoT) devices; smart city infrastructure; connected critical national infrastructure including healthcare and energy.	Intelligence interception and surveillance; coordination of autonomous military systems; military command-and-control networks.

Source: Krelina (2025), *Military and Security Dimensions of Quantum Technology*; OECD (2026), *Building capacity in technology horizon scanning: A guide for policymakers*, Science, Technology and Industry Working Papers 2026/06, https://www.oecd.org/content/dam/oecd/en/publications/reports/2026/04/building-capacity-in-technology-horizon-scanning_7a0a98c6/b4f0d383-en.pdf.

The convergence of emerging technologies is likely to create dual-use capabilities far more transformative than any one technology alone. For example, the convergence of AI, quantum computing and engineering biology could accelerate scientific discovery by enabling researchers to model complex biological systems, optimize genetic designs and rapidly identify new materials, therapeutics and manufacturing processes. At the same time, these technologies may accelerate the development of chemical and biological threats and enable the design of bioengineered weapons.[53]

How are these threats realized in practice?

Foreign state activity targeting the UK research sector is not limited to any single country and spans a spectrum of methods, both licit and illicit, to access and acquire sensitive knowledge and expertise from UK universities. At the most serious end of the threat spectrum, individuals acting on behalf of foreign states may engage in illegal economic espionage, cyber intrusion and IP theft, including the targeted extraction of proprietary research data, unpublished findings and commercially sensitive technological information.[54]

53 Krelina (2025), *Military and Security Dimensions of Quantum Technology;* Hynek, N. (2026), 'Synthetic biology/AI convergence (SynBioAI): security threats in frontier science and regulatory challenges', *AI & Society*, 41, pp. 951–68, p. 952, https://doi.org/10.1007/s00146-025-02576-4.
54 Intelligence and Security Committee of Parliament (2023), *China*, p. 31.

However, intelligence and security agencies consistently assess that the malign transfer of sensitive S&T knowledge predominantly occurs through the use of 'non-traditional collectors': that is, individuals who are not formal intelligence agents, but who are nonetheless directed or (wittingly or unwittingly) incentivized or leveraged by foreign states to acquire sensitive S&T information on their behalf. These actors largely operate within the bounds of legitimate academic, commercial or research activities.[55] By using legitimate vectors, adversarial foreign state actors remove the need to mount sophisticated covert espionage or cyber operations to acquire sensitive S&T knowledge and expertise.

The scale of this activity is inherently difficult to quantify. The theft or malign transfer of dual-use S&T knowledge, expertise and IP is difficult to identify and rarely disclosed publicly, while universities may have strong reputational and commercial incentives to manage potential security concerns internally. Consequently, publicly known cases are likely to represent only a small proportion of the overall research security challenge.[56] This limited visibility further complicates efforts to assess the prevalence and scale of non-traditional collection across the UK research sector.

In practice, non-traditional collection is enabled through a wide range of legitimate academic and professional vectors. These include formal collaboration mechanisms such as joint research programmes, international consortiums, visiting-scholar arrangements, talent recruitment schemes, industrial partnerships and overseas research institutes. Such vectors also extend to less formal but highly consequential channels of knowledge exchange, including conference participation, peer-to-peer collaboration, co-authorship networks, and the circulation of pre-publication or early-stage research findings.[57]

China as the primary threat actor

Within the broader landscape of state threats to UK universities, China presents the most significant and systemic research security challenge. On the one hand, it is one of the UK's most significant partners in scientific collaboration.[58] On the other, the UK Parliament's Intelligence and Security Committee has characterized China as a 'strategic threat', warning that UK universities provide a 'rich feeding ground' for China to acquire IP and accelerate its technological development through unauthorized means.[59]

While China is not unique in seeking access to foreign S&T ecosystems, it is distinguished by the scale of its ambitions, the resources it can mobilize, and the centrality of S&T to both its economic model and military modernization agenda.[60]

---

55 Ibid., p. 31.
56 Walker-Munro, B. and Young, A. (2025), '"How is Research Dangerous?": A Study of Australian Universities and Research Security Incidents', *University of Queensland Law Journal*, 44(3), p. 40, https://doi.org/10.38127/uqlj.v44i3.16015.
57 Coventry University, Protective Security Lab (2025), *State Threats and Universities: Case Studies from the United Kingdom*, https://www.coventry.ac.uk/globalassets/media/global/08-new-research-section/ctpsr/pdfs/state_threat_uni_7-1.pdf; National Protective Security Authority (2025), *Trusted Research: Guidance for Academics*.
58 Center for Security and Emerging Technology, Georgetown University (2025), 'Emerging Technology Observatory', https://cat.eto.tech.
59 Intelligence and Security Committee of Parliament (2023), *China*.
60 Quimbre, Carlyon, Dewaele and Drew (2022), *Exploring Research Engagement with China.*

Key to the security challenge is not simply that China poses an unprecedented espionage risk to UK S&T, but that it operates a 'whole-of-state' approach to S&T development. Civilian researchers, universities and firms are increasingly mobilized alongside defence and security actors to transfer knowledge and expertise gained abroad back to China in support of CPC objectives.[61] The UK intelligence community assesses that China is 'agnostic about the means employed to achieve its objectives',[62] willing to use a combination of lawful, grey-zone and illicit methods simultaneously to acquire strategic advantage, and able to adapt its methods to avoid detection. During Xi Jinping's presidency, S&T policy has become increasingly centralized under party-state control,[63] and explicitly framed as a core instrument for achieving the CPC's strategic objectives, including military capability development and the achievement of national security outcomes. This agenda has been operationalized through China's military–civil fusion strategy, ensuring that civilian S&T developments can be rapidly adapted or mobilized for military use.[64]

Alongside dedicated People's Liberation Army (PLA) research institutes and defence laboratories, a wider network of state-linked research organizations such as the Chinese Academy of Science and defence-linked universities – including the so-called 'Seven Sons of National Defence'[65] – maintain extensive links to China's defence-industrial base through military laboratories, defence research programmes and talent pipelines.[66] Despite the apparent risks China's system and agenda present, a 2026 report by UK-China Transparency found that the UK maintains the largest number of collaborations globally with Seven Sons of National Defence entities. Based on data reported by China's Ministry of Education in June 2026, the UK accounted for 19 such partnerships, followed by Russia with 10 and France with eight.[67]

---

61 Mei and Huismans (2026), *China's Science and Technology Strategy in Perspective.*
62 Intelligence and Security Committee of Parliament (2023), *China*, p. 30.
63 In March 2023, the CPC established the Central Science and Technology Commission (CSTC), placing responsibility for national S&T policy across government ministries, research institutions and industry under the direct supervision of centralized CPC control and of President Xi Jinping himself. By superseding the Ministry of Science and Technology, the CSTC continues the trend under Xi's leadership of prioritizing party control over governmental ministers' power. Mok, C. (2023), 'The Party Rules: China's New Central Science and Technology Commission', *The Diplomat*, 23 August 2023, https://thediplomat.com/2023/08/the-party-rules-chinas-new-central-science-and-technology-commission.
64 Mei and Huismans (2026), *China's Science and Technology Strategy in Perspective*; Groenewegen-Lau, J. and Laha, M. (2023), *Controlling the Innovation Chain: China's strategy to become a science & technology superpower*, MERICS Report, Berlin: Mercator Institute for China Studies (MERICS), https://merics.org/sites/default/files/2023-11/merics-report-controlling-the-innovation-chain.pdf; Kara, O'Loughlin, Griffin and Janjeva (2025), *Seeking Deeper*; McFaul, C., Bresnick, S. and Chou, D. (2025), *Pulling Back the Curtain on China's Military-Civil Fusion: How the PLA Mobilizes Civilian AI for Strategic Advantage*, Report, Center for Security and Emerging Technology (CSET), Georgetown University, https://cset.georgetown.edu/publication/pulling-back-the-curtain-on-chinas-military-civil-fusion.
65 The 'Seven Sons of National Defence' network consists of seven Chinese universities administered by the Ministry of Industry and Information Technology (MIIT) and closely integrated with China's defence-industrial base through the State Administration for Science, Technology and Industry for National Defence (SASTIND). These universities have a long-standing role in conducting defence-related research and training personnel for China's military-industrial sector. Murphy, D. (2024), *The Seven Sons of National Defence*, Cambridge: Harvard Kennedy School, Ash Center for Democratic Governance and Innovation, Occasional Paper, https://rajawali.hks.harvard.edu/wp-content/uploads/sites/2/2024/11/240948-HKS-Occasional-Seven-Sons-FINAL-11-19.pdf.
66 Joske, A. (2019), *The China Defence Universities Tracker: Exploring the military and security links of China's universities*, Australian Strategic Policy Institute, Policy brief, Report No. 23/2019, https://www.aspi.org.au/report/china-defence-universities-tracker.
67 Benincasa, E. (2026), *One Network, Two Systems: The Research Security Risks of UK/China University Cyber Partnerships*, Report, UK-China Transparency, https://drive.google.com/drive/folders/1llinG6fpj1NNYiN4zwh45vdDEWTqTw0O.

Beyond identifiable PLA-linked entities, the distinction between civilian and military institutions has become increasingly blurred as dual-use research programmes expand and as the work of civilian universities and companies is integrated into national strategic priorities. This creates risks for UK universities engaged in research collaboration with Chinese entities, as due diligence assessments will become more difficult over time, and the security risks posed by Chinese universities and companies harder to mitigate.[68]

Box 1. Case study: Government blocking of proposed dual-use tech IP licence agreement with China

In 2022, the UK government blocked a proposed licence agreement between the University of Manchester and a Chinese company, Beijing Infinite Vision Technology (BIVT), under the National Security and Investment Act – this was the first prohibition of an IP transaction under the 2021 legislation.[69] The University of Manchester had voluntarily notified the government of the transaction. The agreement would have transferred rights for the university's SCAMP-5 and SCAMP-7 vision-sensing technology, enabling BIVT to develop, manufacture and commercialize products based on advanced neuromorphic vision sensors.

Such technology has a range of dual-use applications, including in autonomous vehicles, drones, missile guidance, surveillance systems and advanced military robotics. The UK government concluded that the transfer could contribute to capabilities contrary to the UK's national security.[70]

This structural integration of civilian and military elements is reinforced by China's legal and regulatory frameworks. China's national security laws place broad obligations on Chinese citizens, companies and institutions to support intelligence services when requested, including outside China.[71] In parallel, China's cybersecurity and data governance legislation provides the state with extensive powers to access data held by, or transiting through, Chinese networks and digital infrastructure, including in Hong Kong. While this does not automatically mean that all Chinese researchers or students working and studying in the UK, or Chinese universities and companies collaborating with UK institutes, are engaged in malign technology transfer on behalf of the Chinese state, it creates a legal and political environment in which ostensibly benign actors may be subject to direction

68 McFaul, Bresnick and Chou (2025), *Pulling Back the Curtain on China's Military-Civil Fusion*.
69 Cabinet Office and Department for Business, Energy and Industrial Strategy (2022), 'Acquisition of know-how related to SCAMP-5 and SCAMP-7 vision sensing technology: notices of final order and variation of final order', 20 July 2022, https://www.gov.uk/government/publications/acquisition-of-know-how-related-to-scamp-5-and-scamp-7-vision-sensing-technology-notice-of-final-order.
70 BBC News (2022), 'UK blocks University of Manchester sensor deal with Chinese company', 23 July 2022, https://www.bbc.co.uk/news/technology-62243424.
71 Creemers, R. (2015), 'National Security Law of the People's Republic of China', 1 July 2015, DigiChina, Stanford University, https://digichina.stanford.edu/work/national-security-law-of-the-peoples-republic-of-china; U.S. National Counterintelligence and Security Center (2023), *Safeguarding Our Future: U.S. Business Risk: People's Republic of China (PRC) Laws Expand Beijing's Oversight of Foreign and Domestic Companies*, https://www.odni.gov/files/NCSC/documents/SafeguardingOurFuture/NCSC_SOF_2023-06-30_China-Laws.pdf; Mei and Huismans (2026), *China's Science and Technology Strategy in Perspective*.

or pressure by the CPC.[72] Furthermore, the capacity of the state to access data within Chinese cyberspace raises broader concerns around the security of research data and the sharing of digital infrastructure, particularly through joint ventures within mainland China or Hong Kong. Considering that the UK maintains more structured university partnerships with China than any other European country does (ranking behind only the US and Russia in terms of newly established partnerships with China in 2025), UK research is particularly vulnerable to exploitation under these legal structures.[73]

China's talent recruitment programmes further illustrate how civilian academic engagement can facilitate technology transfer. The most prominent of these, the now-defunct 'Thousand Talents Programme', was a Chinese state-based initiative which expressly aimed 'to attract more high-level foreign experts to participate in China's modernization and to promote a deeper implementation of the "talent superpower" strategy'.[74] While participation in the programme did not inherently translate into illicit activity, concerns sometimes arose that the programme created pathways for the transfer of IP, know-how and sensitive research to China.[75] Although the programme has since been restructured, analysts assess that similar talent recruitment mechanisms continue to operate under successor schemes.[76]

Similar concerns have been raised regarding state-sponsored scholarship schemes, particularly the China Scholarship Council (CSC), which funds thousands of Chinese students and researchers overseas, including a substantial number of STEM PhD candidates in UK universities. Analysis by Georgetown University's Center for Security and Emerging Technology of CSC funding agreements indicates the presence of contractual obligations for scholars to uphold the interests and laws of the Chinese state and report to Chinese diplomatic missions while abroad. This has raised concerns among some commentators about potential channels for knowledge transfer and state influence.[77]

---

72 Intelligence and Security Committee of Parliament (2023), *China*.
73 Benincasa (2026), *One Network, Two Systems*.
74 The 'talent superpower' strategy is a long-term national strategy to make China a global leader in science, technology and innovation by attracting, cultivating, retaining and strategically deploying high-level talent, particularly foreign talent in strategically significant emerging fields. Center for Security and Emerging Technology, Georgetown University (2020), 'Detailed Rules for the "Thousand Talents Program" High-Level Foreign Expert Project', translation, 8 July 2020, https://cset.georgetown.edu/publication/detailed-rules-for-the-thousand-talents-program-high-level-foreign-expert-project.
75 United States Senate Permanent Subcommittee on Investigations (2019), *Threats to the U.S. Research Enterprise: China's Talent Recruitment Plans,* Staff Report, *https://www.govinfo.gov/content/pkg/GOVPUB-Y4_G74_9-PURL-gpo128826/pdf/GOVPUB-Y4_G74_9-PURL-gpo128826.pdf;* Vogel and Ben Ouagrham-Gormley, S. (2023), 'Scientists as spies?'.
76 Lee, Y. and Baptista, E. (2023), 'China quietly recruits overseas chip talent as U.S. tightens curbs', Reuters, 24 August 2023, https://www.reuters.com/technology/china-quietly-recruits-overseas-chip-talent-us-tightens-curbs-2023-08-24.
77 Fedasiuk, R. (2020), *The China Scholarship Council: An Overview*, Report, Center for Security and Emerging Technology, Georgetown University, https://cset.georgetown.edu/publication/the-china-scholarship-council-an-overview.

04 International comparisons and lessons for the UK

Comparative experience suggests there is no single optimal model for research security governance. However, Australia, Japan and Canada demonstrate the value of stronger cross-government coordination, government support for universities, and clearer risk frameworks.

International experience demonstrates that there is no single ideal model for research security governance. However, several comparable countries have developed approaches that offer useful lessons for the UK as it seeks to strengthen and modernize its own framework. While each country in the examples below operates within its own legal, political and higher education context, Australia, Japan and Canada illustrate different approaches to balancing research openness, national security and economic competitiveness.

Australia

Australia is frequently characterized as a 'first mover' in research security due to its early adoption of counter-foreign interference and espionage reforms in 2018 as a result of heightened concerns over Chinese political interference and espionage. A defining feature of the Australian response was the establishment of the University Foreign Interference Taskforce (UFIT), which brought together government and universities to co-design the 'Guidelines to Counter Foreign

Interference in the Australian University Sector'.[78] This collaborative model was complemented by an Australian Security Intelligence Organisation (ASIO) campaign, 'collaborate with care', which sought to raise awareness of national security risks in international research collaboration across academia.[79]

Australia's experience highlights both the strengths and limitations of a voluntary, guidance-based approach. While UFIT improved awareness and built trust between government and universities, policy development has 'languished' after early progress and implementation has remained uneven.[80] The guidelines have not been substantially updated since 2021, and universities have continued to call for more detailed operational guidance to support decision-making.[81] Critically, Australia's approach has until recently remained largely voluntary and guidance-driven, with no uniform national baseline for compliance.[82]

Australia is frequently characterized as a 'first mover' in research security due to its early adoption of counter-foreign interference and espionage reforms in 2018.

Australia has sought to address these shortcomings by embedding research security more directly into the public funding system.[83] The Australian Research Council (ARC), Australia's primary public funding body for research, now plays a more active role in assessing foreign interference, defence and national security risks associated with grant applications, explicitly recognizing that publicly funded research, and the protection thereof, should advance Australia's national interest.[84] ARC grant applicants are subject to extensive disclosure requirements relating to foreign affiliations, appointments, associations and sources of funding, and are required to cooperate with additional information requests where national security concerns arise. In May 2026, Australia's minister for education refused 13 ARC grant applications on grounds relating to security, defence or international relations.[85] A further significant development has been proposed through reforms to Australia's Foreign Arrangements Scheme, which grants the minister for foreign affairs powers to cancel, vary or impose conditions on foreign arrangements (including university partnerships) deemed to undermine Australia's foreign policy. The Foreign Relations (State and Territory Arrangements) Amendment Bill 2026, introduced in July 2026

---

78 Australian Government, Department of Education (2021), *Guidelines to Counter Foreign Interference in the Australian University Sector*, last modified 17 November 2021, https://www.education.gov.au/countering-foreign-interference-australian-university-sector/guidelines-counter-foreign-interference-australian-university-sector.
79 Walker-Munro (2025), *Shifting the needle*.
80 Walker-Munro and Young (2025),'"How is Research Dangerous?"'.
81 Ibid.
82 Ibid.; Walker-Munro (2025), *Shifting the needle*.
83 Australian Research Council (2026), *ARC Research Security Framework*, https://www.arc.gov.au/system/files/2026-05/arc-research-security-framework.pdf.
84 Walker-Munro, B. (2025), '(Professor) Hadrian's Wall: The Role of the Australian Research Council in Research Security', *UNSW Law Journal*, 48(1), pp. 348–74, https://www.austlii.edu.au/au/journals/UNSWLawJl/2025/10.pdf?__cf_chl_f_tk=OwcqGLCefi.4HVVCxVrkPvMalAP_ugeV4XUzJNEBtCc-1783187237-1.0.1.1-uPvBfregBcRUTwHjKQcCyf9ybeFdGBDN9fuvP6AGLBg.
85 Australian Research Council (2026), *Update on Research Security*, 14 May 2026, https://www.arc.gov.au/news-and-publications/media/update-research-security.

and currently before parliament, would strengthen oversight of foreign arrangements involving public universities by broadening the scope of legislation to capture foreign arrangements that adversely affect the 'national interest', expanding information disclosure requirements and enabling ASIO security advice to inform the foreign minister's decisions.[86]

Lessons for the UK

- The UK's collaborative approach to advising universities on research security risks, including on a case-by-case basis through RCAT, remains a strength and should continue to be prioritized.
- Research security guidance should be regularly reviewed and updated so that it remains relevant to emerging risks. To be useful for universities, advice needs to be as specific and actionable as possible.
- Consideration should be given to whether UKRI and other public funders should play a more active role in research security assurance, rather than relying primarily on institutional self-assessment and risk management.
- Voluntary guidance alone is unlikely to deliver consistent implementation across the sector without clearer baseline expectations and appropriate enforcement capacity. Where approaches characterized by voluntary guidance and institutional self-assessment become ill suited to an evolving threat landscape and national security objectives, the government should consider enabling targeted intervention in cases of concern, informed by security advice.

Japan

Japan's approach to research security is best understood as part of its prioritization of economic security as a strategic imperative. The Economic Security Promotion Act (2022) links the protection of critical technologies, supply chains and research capability directly to national resilience and competitiveness. Coordination is overseen centrally through the Cabinet Office's Economic Security Secretariat, which helps align policy across economic, science and technology, and national security portfolios.[87]

A defining feature of Japan's approach is the emphasis on 'strategic indispensability' – the pursuit of a national innovation base that is so embedded in global technology networks that it becomes irreplaceable to key partners, and

86 Parliament of Australia (2026), *Australian Foreign Relations (State and Territory Arrangements) Amendment Bill 2026*, Bills Digest No. 7, 2026-27, 6 August 2026, https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/bd/bd2627/27bd007.
87 Government of Japan (2022), *Outline of the Economic Security Promotion Act*, https://www.japaneselawtranslation.go.jp/outline/75/905R403.pdf; Suzuki, K. (2023), 'How Will the Economic Security Law Change Japan's Sci-Tech Policy?', Tokyo Foundation, 9 May 2023, https://www.tokyofoundation.org/research/detail.php?id=943; Lee (2024), 'U.S.-China Technology Competition and the Emergence of Techno-Economic Statecraft in East Asia'.

therefore a bulwark against economic coercion and overdependence. This has been accompanied by significant investment in technology partnerships with allies, particularly in semiconductors, advanced computing and AI.[88]

Japan's model is notable for its coherence, integrating research security into thinking on industrial policy, supply-chain resilience and geo-economic planning.[89] While implementation at the university sector level remains uneven due to reliance on self-assessment and limited compliance infrastructure, Japan's centrally coordinated model has in effect embedded research security within broader strategic goals.

Lessons for the UK

- Research security should be integrated within wider economic security, industrial strategy and S&T policy objectives.
- Stronger central coordination across government, including at the ministerial and cabinet level, could improve coherence between S&T, trade, industrial and national security policy domains.
- Research security should be viewed not only as a defensive activity but also as a means of strengthening strategic advantage and technological competitiveness.
- Trusted international partnerships can reduce strategic dependencies and bolster sovereign autonomy and the national innovation ecosystem.

Canada

Canada has adopted one of the most structured research security frameworks among peer countries. Its Sensitive Technology Research and Affiliations of Concern (STRAC) policy prohibits federal funding of research projects that involve designated foreign entities or rely on affiliations of national security concern. To support implementation of the STRAC policy, the Canadian government maintains publicly available lists of sensitive technology areas and foreign institutions assessed as presenting elevated risk due to state or military linkages; this provides researchers and institutions with clear criteria for what constitutes an intolerable security risk in the eyes of the government and warrants enhanced scrutiny.[90]

---

88 Sasae, K. (2026), 'Introduction: A Strategic Perspective for 2026: Japan's Strategic Autonomy and Indispensability in an Era of Uncertainty', *Strategic Outlook 2026*, Tokyo: The Japan Institute of International Affairs, 31 March 2026, https://www.jiia.or.jp/eng/report/2026/03/Outlook2026jp00.html; Kawai, D. (2025), 'Reinventing Japan's Economic Security: Balancing Interdependence with Strategic Technology', The National Bureau of Asian Research, 27 January 2025, https://nbr.org/publication/reinventing-japans-economic-security-balancing-interdependence-with-strategic-technology; Osaki, M. (2025), 'NVIDIA to Help Elevate Japan's Sovereign AI Efforts Through Generative AI Infrastructure Build-Out', blog post, NVIDIA, 14 May 2024, https://blogs.nvidia.com/blog/japan-sovereign-ai.
89 Aggarwal and Reddie (2020), 'New Economic Statecraft'.
90 Government of Canada (2024), *Policy on Sensitive Technology Research and Affiliations of Concern*, https://science.gc.ca/site/science/en/safeguarding-your-research/guidelines-and-tools-implement-research-security/sensitive-technology-research-and-affiliations-concern/policy-sensitive-technology-research-and-affiliations-concern; Walker-Munro, B. (2025), 'National security, foreign investment & research security: the current state of art', *Griffith Law Review*, 33(2), pp. 167–88, https://doi.org/10.1080/10383441.2025.2459007; Marwaha, Timlin, Dickson and Johnson (2025), *Stronger cooperation, safer collaboration*.

Alongside regulatory tools, Canada has established the Research Support Fund to meet the institutional costs of implementing this increasingly detailed framework.[91] The fund provides financial support to universities and research organizations for developing internal research security systems, including enhanced due diligence, risk assessment tools, governance structures and staff training.

Canada's approach offers greater clarity and consistency than many peer systems; however, concerns have been raised that static lists may struggle to keep pace with evolving threats and could encourage a complacent security culture within universities, should they remain overly reliant on prescriptive government guidance.[92]

Lessons for the UK

- Clearer guidance on high-risk technology and foreign entities of concern can improve the consistency of decision-making across institutions. Furthermore, more transparent risk assessment criteria can improve institutional confidence. However, static list-based approaches have limitations, and may not be appropriate in all contexts.
- The UK government should allocate dedicated funding to support research security capability within universities.

91 Government of Canada (undated), 'Research security', Research Support Fund, https://www.rsf-fsr.gc.ca/apply-demande/research_security-securite-recherche-eng.aspx.
92 Kharon (2025), 'The University Research Security Challenge: Balancing Collaboration and Compliance', 27 June 2025, https://www.kharon.com/resources/use-cases/research-security/the-university-research-security-challenge-balancing-collaboration-and-compliance.

05
The current UK policy landscape

The UK's approach to research security has improved in recent years, but it still relies on a patchwork of regulations, guidance and institutional practices.

The UK occupies a position of considerable strength within the global S&T landscape. Successive governments, recognizing the importance of S&T, have increasingly framed S&T as a central pillar of national security, military capability, economic resilience and geopolitical influence. This recognition has been reflected in public investment commitments, including an £86 billion S&T funding package for research and innovation in emerging fields, plans to increase annual public R&D expenditure to £22.5 billion by 2029, and targeted support for priority S&T areas, underpinned by dedicated government strategies for these fields.[93]

Simultaneously, the government has sought to bolster protections for the UK's S&T sector against growing geopolitical and security risks. In recent years, the UK has made significant progress in strengthening its research security policies. While these efforts have enhanced awareness and risk management, the policy landscape has developed reactively and incrementally; responsibilities and capabilities remain dispersed across multiple entities. The government's forthcoming research security strategy will represent an important next step in consolidating this approach.

93 Department for Science, Innovation and Technology, HM Treasury, The Rt Hon Rachel Reeves MP and The Rt Hon Peter Kyle MP (2025), 'Transformative £86 billion boost to science and tech to turbocharge economy', press release, 8 June 2025, https://www.gov.uk/government/news/transformative-86-billion-boost-to-science-and-tech-to-turbocharge-economy-with-regions-backed-to-take-cutting-edge-research-into-own-hands; Department for Science, Innovation and Technology and The Rt Hon Peter Kyle MP (2025), 'Tech innovators backed to set up and scale up in Britain through Industrial Strategy', press release, 23 June 2025, https://www.gov.uk/government/news/tech-innovators-backed-to-set-up-and-scale-up-in-britain-through-industrial-strategy; Department for Science, Innovation and Technology (2025), 'AI Opportunities Action Plan', independent report, 13 January 2025, https://www.gov.uk/government/publications/ai-opportunities-action-plan/ai-opportunities-action-plan; Department for Science, Innovation and Technology (2023), *National Quantum Strategy,* https://www.gov.uk/government/publications/national-quantum-strategy; Department for Science, Innovation and Technology (2023), *National Semiconductor Strategy,* https://www.gov.uk/government/publications/national-semiconductor-strategy; Department for Science, Innovation and Technology (2023), *National Vision for Engineering Biology,* https://www.gov.uk/government/publications/national-vision-for-engineering-biology.

Publication of the strategy will provide an opportunity to establish a more coherent national framework that aligns research excellence, international collaboration and national security objectives.[94]

The UK's research security landscape comprises a layered and increasingly interconnected and fast-evolving system of government policy, regulatory controls, funding conditionality and institutional governance. Overall policy responsibility now sits within the newly created Department for Business, Innovation, Science and Trade (DBIST). Following the July 2026 'machinery of government' reforms introduced by the new prime minister, Andy Burnham, DBIST inherited the science, research and innovation functions previously exercised by DSIT. Research security nevertheless remains a cross-government responsibility, with important roles continuing to be played by the Foreign, Commonwealth and Development Office (FCDO), the Home Office, the Cabinet Office and the Department for Education.

The UK's research security landscape comprises a layered and increasingly interconnected and fast-evolving system of government policy, regulatory controls, funding conditionality and institutional governance.

The UK has linked S&T capability directly to defence and national security policy, positioning early-stage research and innovation as central to delivering long-term strategic advantage – this imperative is made all the more urgent by Russia's ongoing war on Ukraine and by the deteriorating global security environment.[95] Within the evolving policy landscape, universities are increasingly viewed as forming part of a whole-of-society approach to defence. For instance, a key objective of the 2025 Strategic Defence Review was the development of closer relationships between defence and the S&T ecosystem, especially in academia. This agenda progressed further through initiatives such as the Defence Universities Alliance (DUA), announced in the 2025 Defence Industrial Strategy, which sought to formalize collaboration between universities, the Ministry of Defence and industry through a structured network for fostering sovereign research, skills and innovation in defence-relevant areas. Together with the recently published Defence Investment Plan – which advocates defence investment in dual-use technology, and emphasizes closer relationships between the defence sector and start-ups, scale-ups and academia – these reforms are likely to reshape research funding, collaboration

94 Ashdown, N. (2025), 'The Government Needs to Send a Wake-Up Call on Research Security', RUSI Commentary, 3 December 2025, https://www.rusi.org/explore-our-research/publications/commentary/government-needs-send-wake-call-research-security.
95 Ministry of Defence (2025), 'The Strategic Defence Review 2025 – Making Britain Safer: secure at home, strong abroad', policy paper, published 2 June 2025, updated 8 July 2025, https://www.gov.uk/government/publications/the-strategic-defence-review-2025-making-britain-safer-secure-at-home-strong-abroad/the-strategic-defence-review-2025-making-britain-safer-secure-at-home-strong-abroad; Ministry of Defence (2025), *Defence Industrial Strategy 2025: Making Defence an Engine for Growth*, https://assets.publishing.service.gov.uk/media/68bea3fc223d92d088f01d69/Defence_Industrial_Strategy_2025_-_Making_Defence_an_Engine_for_Growth.pdf.

and technology priorities across the UK R&D ecosystem.[96] As universities become more deeply embedded in the government's efforts to deliver national capability, they will face growing expectations to demonstrate robust research security practices as a prerequisite for participating in defence-linked partnerships and programmes.[97]

Alongside the government departments mentioned above, the UK's technical security authorities play a central operational role. Through the Trusted Research initiative, the National Protective Security Authority (NPSA) and the National Cyber Security Centre (NCSC) provide specialist guidance informed by intelligence inputs on physical, personnel, cyber and information security risks affecting universities and research-intensive organizations.[98]

A significant development in the UK framework was the establishment of the Research Collaboration Advice Team (RCAT). Created by the UK government, and launched in 2022, as a dedicated advisory service for the research sector, RCAT was intended to provide universities and research organizations with a clear first point of contact for advice on national security risks associated with international research collaboration.[99] Since its creation, RCAT has become an important intermediary within the UK research security architecture, helping to bridge the gap between government security concerns and the operational realities of academic research. Its role is significant because RCAT offers institutions access to government-backed advice without relying on dispersed formal regulatory enforcement mechanisms.[100] Following the July 2026 'machinery of government' changes, RCAT will continue to play an important role under the direction of the newly formed DBIST.

Beneath the strategic and advisory layer sits a more fragmented set of legislative and regulatory controls (see Annex 1). Research security obligations in the UK are governed through multiple mechanisms, including export controls, investment screening, immigration and visa processes, and IP law – however, the majority of these mechanisms were not originally designed with research security in mind. Research security functions are spread across different departments and agencies, which often have overlapping requirements.[101] As a result, universities frequently describe the UK system as a regulatory 'patchwork', in which compliance responsibilities are dispersed rather than consolidated within a single framework.[102] Public funders of research have become increasingly influential in shaping research security behaviour. In recent years UK Research and Innovation (UKRI), the UK's largest such funder, has strengthened its 'trusted research and innovation' guidance and has introduced more stringent compliance requirements.[103]

---

96 Ministry of Defence (2026), *The Defence Investment Plan: Equipping our forces, defending our future*, p. 66, https://assets.publishing.service.gov.uk/media/6a44e989167a99cf0018da38/The_Defence_Investment_Plan.pdf.
97 Ministry of Defence (2026), 'Guidance: Apply to become a founding member of the Defence Universities Alliance', published 20 April 2026, updated 15 May 2026, https://www.gov.uk/guidance/apply-to-become-a-founding-member-of-the-defence-universities-alliance.
98 National Protective Security Authority (2025), *Trusted Research: Guidance for Academics*.
99 Research Collaboration Advice Team (2026), 'Research Collaboration Advice Team: 2026 update', corporate report, 20 March 2026, https://www.gov.uk/government/publications/research-collaboration-advice-team-2026-update/research-collaboration-advice-team-2026-update.
100 Walker-Munro (2025), 'National security, foreign investment & research security'.
101 Hughes et al. (2025), *Securing the UK's AI Research Ecosystem*.
102 Author's interviews with research security professionals.
103 UK Research and Innovation (2025), 'UKRI trusted research and innovation principles', published 22 August 2021, last updated 13 June 2025, https://www.ukri.org/publications/ukri-trusted-research-and-innovation-guidance.

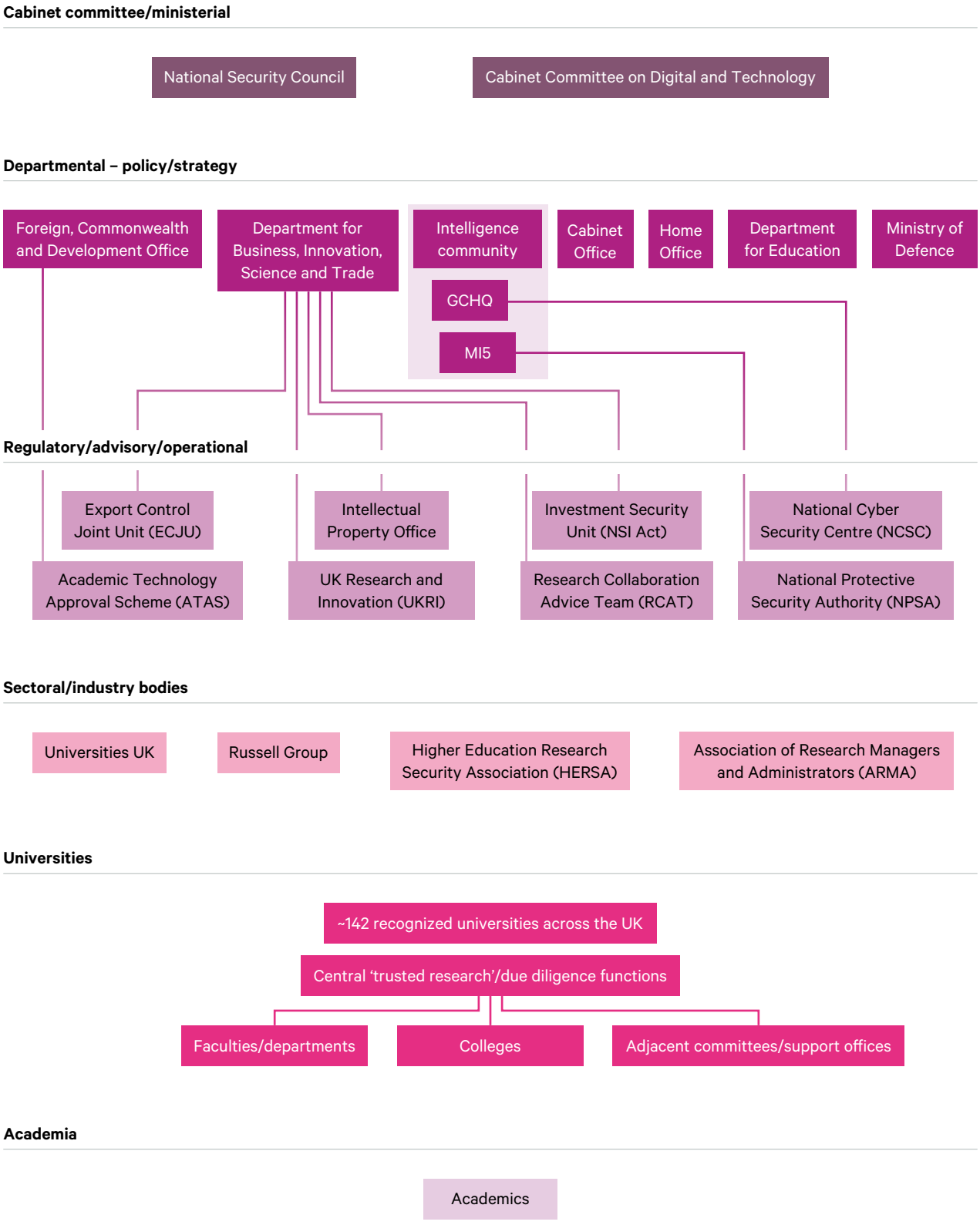
Sectoral bodies and professional networks play supporting roles in translating national policy into operational practice. Organizations such as Universities UK (UUK), the Russell Group, the Higher Education Research Security Association (HERSA) and the Association of Research Managers and Administrators (ARMA) increasingly provide guidance, training and forums for knowledge exchange. These organizations have an intermediary role in interpreting government expectations, sharing emerging practice, and helping institutions implement research security requirements in ways that are workable within academic environments.[104] Their involvement in co-designing and disseminating practical approaches has helped build trust and legitimacy around the research security agenda, contributing to greater awareness, institutional buy-in and more consistent implementation. Bodies such as HERSA have also become important for building bilateral and multilateral engagement with like-minded international partners at the sectoral level.

At the institutional level, most UK universities now maintain dedicated research security teams. These teams are generally responsible for coordinating compliance with legal, regulatory and funder requirements, conducting due diligence on international partnerships, delivering staff training and overseeing internal risk management. In larger and more decentralized institutions, responsibility for research security may also be distributed across faculties, departments, colleges, ethics committees, export control offices, and legal or compliance teams.[105]

Ultimately, however, responsibility also rests with researchers. Academics are expected to comply with institutional policies and relevant legal obligations. Failure to comply may have consequences ranging from loss of funding and reputational damage to disciplinary action and, in certain circumstances, civil or criminal liability.

104 Searle, Ganglmair and Borghi (2025), *Trusted Research and Innovation*; Hughes et al. (2025), *Securing the UK's AI Research Ecosystem*.
105 Universities UK (2020), *Managing Risks in Internationalisation.*

Figure 1. The UK's research security landscape



Sources: Author's compilation.

06 Structural challenges and policy recommendations

The effectiveness of the UK's research security framework depends not only on formal controls but on the environment in which they are applied. With structural challenges constraining implementation, the UK needs a more coordinated and adaptive approach.

While the UK has strengthened its research security legal and policy architecture, ultimately the effectiveness of a research security framework depends not only on the robustness of formal controls but on the institutional, financial and operational realities in which those controls are implemented. These constraints determine which reforms are feasible and where policy, resources and regulatory attention need to be targeted.[106] This chapter sets out the principal challenges and gaps in the UK's research security regime, and proposes how policy could be improved.

106 Searle, Ganglmair and Borghi (2025), *Trusted Research and Innovation*.

Lack of coherent strategy

Commentators have increasingly argued that UK research security has been reactive rather than strategic, and that policy often responds to specific incidents only after they have emerged in public or political discourse. This has largely been driven by the absence of a consistently articulated and public whole-of-government strategy on China and, more broadly, by the lack of a long-term vision for the UK's position within an increasingly competitive global S&T environment.[107] In its 2023 China report, the Intelligence and Security Committee of Parliament noted that overall, the UK government lacked understanding and was slow to identify and protect strategic assets such as emerging technology from exploitation by China.[108]

Strategic coherence has been limited by a lack of policy continuity. Successive UK governments have introduced new strategic frameworks, funding priorities and institutional mechanisms for science and innovation, often without fully embedding or sustaining previous approaches. While periodic policy refreshes are necessary in a rapidly changing technological landscape, excessively frequent shifts can undermine long-term capability-building and reduce clarity for universities and industry partners operating in strategically sensitive areas. This lack of coherence limits the government's ability to define which areas of research constitute 'critical' or 'sensitive' technologies, why they matter, and how risk tolerance and protections should vary across different domains.[109]

A more coherent approach would involve systematically identifying where the UK holds, or could realistically develop, a comparative advantage in emerging technology niches, and aligning innovation policy, public funding and research security efforts accordingly. Steps have already been taken in this direction. They include UKRI's investments in strategic technology, and the programme-based efforts of the Advanced Research and Invention Agency (ARIA) to identify high-impact opportunities.[110] However, these initiatives have generally lacked specificity and have not yet produced a comprehensive, cross-government assessment of the UK's relative strengths, dependencies and vulnerabilities across the full spectrum of emerging technologies.

Nor have priorities always been clearly communicated across government and to academia, industry and investors in a manner that provides consistent long-term direction.[111] While the recent merging of S&T policy and business and trade functions into a single department – DBIST – may bring greater alignment between industrial and innovation strategy, there is a risk that Prime Minister Burnham's 'machinery of government' reforms further impede momentum in building

---

107 Matthews (2025), *What the UK must get right in its China strategy*; Quimbre, Carlyon, Dewaele and Drew (2022), *Exploring Research Engagement with China*; Wye (2023), 'The UK's Response to the Challenge of Managing Its Relationships with China and the US'.
108 Intelligence and Security Committee of Parliament (2023), *China*, p. 4.
109 Hüsch, P. and Buckley, N. (2025), *UK National Security Advantage from Disruptive Technologies: Understanding UK Assets, Needs and Dependencies*, Royal United Services Institute (RUSI), p. 1, https://www.rusi.org/explore-our-research/publications/research-papers/uk-national-security-advantage-disruptive-technologies; Wye (2023), 'The UK's Response to the Challenge of Managing Its Relationships with China and the US'.
110 UK Research and Innovation (2026), 'UKRI Technology Missions Fund', last updated 13 July 2026, https://www.ukri.org/what-we-do/browse-our-areas-of-investment-and-support/ukri-technology-missions-fund; Advanced Research and Invention Agency (undated), 'About ARIA', https://aria.org.uk/about-aria.
111 Hüsch and Buckley (2025), *UK National Security Advantage from Disruptive Technologies*.

UK S&T advantage as key areas of government are distracted by bureaucratic restructuring at a time when pace is essential for the UK's economic growth and geopolitical standing.

More fundamentally, research security cannot be treated as a discrete policy domain separate from broader geopolitical and industrial dynamics. It is indivisible from the global S&T system, which in turn is shaped by supply-chain dependencies, international collaboration networks and intensifying US–China technological competition.[112] Effective policy also requires an integrated understanding of the full innovation life cycle – from 'upstream' inputs such as critical minerals and talent to R&D, 'downstream' scaling of research innovations, and commercialization. The new prime minister's initial reforms to the organization of government have explicitly sought to align S&T with industrial policy and economic growth, reflecting the reality that technological advantage depends on translating research and innovation into scaled-up commercial opportunities. However, the reforms do little to resolve the long-standing challenge of integrating S&T policy with national security decision-making. Furthermore, industry leaders have argued that the abolition of DSIT risks diluting the political prominence and strategic focus previously afforded to S&T, potentially slowing decision-making.

Research security cannot be treated as a discrete policy domain separate from broader geopolitical and industrial dynamics. It is indivisible from the global S&T system, which in turn is shaped by supply-chain dependencies, international collaboration networks and intensifying US–China technological competition.

An approach that aligns the UK's security, S&T and foreign policy imperatives will also require stronger cooperation with like-minded foreign partners through the 'friendshoring' of critical technologies – that is, the UK sourcing raw materials, components and technological capabilities from countries it trusts. Given that no state can achieve full self-sufficiency in advanced S&T supply chains, collaboration with trusted partners is increasingly central to resilience and security.[113]

For the UK, this points to a clear need to prioritize deeper integration with Europe's S&T and defence-industrial base.[114] At present, this agenda remains underdeveloped, despite its potential importance for innovation capacity and national resilience, particularly in the context of the UK's wider reset with the EU. Although the UK's rejoining of Horizon Europe as an associate member

---

112 Ibid.
113 Job (2022), 'Between a Rock and a Hard Place'; Lee (2024), 'U.S.-China Technology Competition and the Emergence of Techno-Economic Statecraft in East Asia'.
114 Department for Science, Innovation and Technology (2024), *UK Position Paper on the 10th EU Research and Innovation Framework Programme*, 26 September 2024, https://www.gov.uk/government/publications/uk-position-on-eus-research-and-innovation-framework-programme.

in 2024 restored UK access to Europe's flagship research programme, the UK no longer benefits from the same degree of institutional integration with European research, regulatory and industrial ecosystems that it did pre-Brexit. Nor has the UK yet negotiated entry into Horizon Europe's successor, the 10th Research and Innovation Framework Programme (FP10). More generally, the UK's lack of sufficient progress in resetting its relationship with the EU has reduced the UK's ability to operate seamlessly as a bridge between the US and European innovation ecosystems at a time when technological governance is becoming increasingly fragmented.

Beyond Europe, the UK already participates in a range of multilateral groupings – including the G7, Pillar II of AUKUS, and the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) – that provide important foundations for strengthening research security cooperation. In particular, the G7 has made progress through initiatives such as the Common Values and Principles on Research Security and Research Integrity, and through publication of the G7 Best Practices for Secure and Open Research.[115] These initiatives provide a model for shared approaches to research security across the dispersed interests of member states. Pillar II of AUKUS, meanwhile, remains an underused opportunity. As a framework focused on coordinating development of emerging and dual-use technologies, it offers potential for deeper integration between the three partners – Australia, the UK and the US – as demonstrated by the introduction of a streamlined AUKUS export control licence framework in 2024. Yet progress under Pillar II has been slow and uneven, raising questions about whether the scheme is being sufficiently prioritized within the UK's S&T and defence strategies, given its potential to underpin deeper integration of allied defence-industrial bases.

Recommendations

- The UK government should prioritize funding and S&T policy efforts in strategic areas where the UK possesses, or could realistically develop, comparative advantage. Research security efforts should be calibrated accordingly, with protective measures prioritized towards areas of greatest strategic significance.[116] To inform these efforts, the government should:
  - Revive the defunct National Security Technology and Innovation Exchange (NSTIx), with the express mission to undertake cross-government technology forecasting and horizon-scanning. The NSTIx should work closely with the Government Office for Science, the Government Chief Scientific Adviser and the national security community to map national

115 In 2022, the G7's Security and Integrity of the Global Research Ecosystem (SIGRE) Working Group developed and adopted the Common Values and Principles on Research Security and Research Integrity, establishing shared principles for protecting the global research ecosystem while preserving openness and collaboration; in 2024, the working group published Best Practices for Secure and Open Research, translating these principles into practical guidance on risk identification, due diligence and proportionate mitigation for governments, funders, institutions and researchers. Government of Canada (2022), 'G7 Common Values and Principles on Research Security and Research Integrity', https://science.gc.ca/site/science/en/safeguarding-your-research/general-information-research-security/international-research-security-resources/g7-common-values-and-principles-research-security-and-research-integrity; Government of Canada (2024), 'G7 Best Practices for Secure and Open Research', https://science.gc.ca/site/science/en/safeguarding-your-research/general-information-research-security/international-research-security-resources/g7-best-practices-secure-and-open-research.
116 This is in line with the ambitions to 'increase sovereign and asymmetric capabilities', particularly in frontier technologies articulated in the National Security Strategy.

strengths and dependencies, identify vulnerabilities and anticipate future areas of emerging technological competition. Such a capability would provide a stronger evidence base for research security policy, industrial strategy and public investment decisions.[117]

- Develop mechanisms to channel a greater share of long-term pension capital into strategic technologies, building on the 2023 Mansion House reforms.[118] By combining pension fund investment with targeted public co-investment and partnerships with trusted allies, the UK can strengthen its ability to develop and commercialize early-stage research and innovation domestically.[119]

- The UK government should prioritize more robust 'friendshoring' of S&T capabilities and critical supply chains with trusted international partners. To these ends, the government should:
  - Strengthen UK–EU integration on S&T and industrial policy. The UK should prioritize negotiating associate membership of the EU's FP10, the successor framework to Horizon Europe. The UK should seek to shape FP10 policies so that these focus on shared strategic technology priorities (e.g. AI, quantum, advanced materials, semiconductors) while embedding common research security standards.
  - Strengthen multilateral coordination on research security and S&T collaboration between trusted partners. This should involve the following steps:
    - The UK should introduce joint approaches through existing forums such as the G7 and the CPTPP. Such efforts must move beyond shared principles towards promoting interoperability between allied countries' research and innovation systems, harmonizing export control regimes, expanding information-sharing (again, between trusted partners), horizon-scanning, and developing co-funded R&D missions in strategically important S&T fields.
    - Pillar II of AUKUS should be explicitly prioritized as a vehicle for 'friendshoring' critical scientific research and technology. Building on efforts to streamline export controls between Australia, the UK and the US, future reforms of the programme should focus on reducing remaining barriers to collaboration, including differences in IP regimes, visa systems

---

117 House of Commons Business and Trade Committee (2025), *Toward a new doctrine for economic security*, HC 835, 24 November 2025, https://committees.parliament.uk/publications/50340/documents/288805/default.
118 The Mansion House reforms are a package of UK government financial and pension reforms announced in July 2023 that sought to increase long-term investment by defined-contribution pension funds in unlisted and high-growth companies. Through the voluntary Mansion House Compact, major pension providers committed to the objective of allocating at least 5 per cent of default funds to unlisted equities by 2030. The intention is to improve access to what the financial sector often refers to as 'patient capital' – that is, long-term investment characterized by a lack of expectation for quick profits and by a high tolerance for risk for sectors including UK emerging S&T.
119 HM Treasury, Torsten Bell MP and The Rt Hon Rachel Reeves MP (2025), 'Major pension schemes back £200 million initial fund to scale UK science and tech', press release, 20 November 2025, https://www.gov.uk/government/news/major-pension-schemes-back-200-million-initial-fund-to-scale-uk-science-and-tech; Wolthuizen, A. (2025), 'How the UK can harness the power of research for its Industrial Strategy', Chatham House Expert Comment, 4 July 2025, https://www.chathamhouse.org/2025/07/how-uk-can-harness-power-research-its-industrial-strategy; HM Treasury (2023), 'Mansion House 2023', published 11 July 2023, updated 19 July 2023, https://www.gov.uk/government/collections/mansion-house-2023.

and research security frameworks. Greater emphasis should also be placed on coordinating long-term public investment and industrial policy across AUKUS members, with export finance agencies playing a more active role in de-risking joint technology development.

— Work with trusted international partners to map innovation supply chains in strategically important technologies. This will involve identifying dependencies, supply chokepoints and complementarities. It would enable allies to specialize in sectors where they hold comparative advantage, jointly mitigate shared vulnerabilities, and better direct public and private investment towards secure technology ecosystems. This could form part of broader bilateral and multilateral agreements on economic security.[120]

Misaligned incentives

Scientific progress has always depended on openness, collaboration, and the cumulative and iterative development of knowledge across institutions, disciplines and borders. Within Western research systems, this globalized model of open science is reinforced by strong institutional norms of academic freedom. This autonomy is widely regarded as a cornerstone of scientific excellence, as it enables researchers to pursue novel lines of inquiry without undue political intervention.[121]

The evolution of the financial model of higher education threatens the advantages engendered by the UK's open research model. In the UK specifically, the contemporary university system operates within a set of increasingly pronounced financial constraints that shape institutional incentives and behaviours, sometimes to the detriment of national security objectives.[122] Over recent decades, the financial model of UK higher education has become increasingly dependent on diversified revenue streams, with efforts to increase international student fee income a particular focus. Unlike domestic tuition fees, which are capped by the government, international fees are largely unregulated, enabling universities to charge significantly higher prices and use the resulting income to cross-subsidize teaching, research and the provision of degree courses to the domestic student cohort.

The UK's income from international student fees has almost trebled in real terms since the early 2000s.[123] Students from China represent one of the largest cohorts of international students in the UK,[124] and are particularly concentrated in postgraduate STEM-related programmes.[125] At the same time, domestic public funding for research has not always kept pace with the rising costs of conducting cutting-edge science. Modern S&T research frequently requires access to expensive instrumentation, advanced computational infrastructure, specialist materials and

120 Matthews (2025), *What the UK must get right in its China strategy.*
121 Shih and Wagner (2024), 'The Trap of Securitizing Science'.
122 Zhang (2025), 'Market–security tensions in UK–China academic engagement'; author's interviews with academics.
123 Bolton, Lewis and Gower (2026), *International students in UK higher education*.
124 According to analysis by the *Financial Times* based on data from the UK's Higher Education Statistics Agency, the Russell Group – a coalition of 24 research-intensive public universities in the UK – relied on tuition fees from Chinese students for approximately 10 per cent of revenue in 2023–24. Borrett, A. and Hughes, L. (2025), 'British universities' reliance on Chinese fees fuelling self-censorship, say academics', *Financial Times*, 8 December 2025, https://www.ft.com/content/a1234b4f-5096-42d4-a76b-2f2a116373fd.
125 Higher Education Statistics Agency (2026), 'Where do HE students come from?', 27 January 2026, https://www.hesa.ac.uk/data-and-analysis/students/where-from.

highly skilled technical staff. As a result, institutions often rely on a combination of public grants, industry partnerships and international funding to sustain activity at the frontier of innovation.[126]

These financial dynamics are complicated by the growing overheads associated with research security compliance. A 2023 analysis by ARMA estimated that UK universities spent between £9.5 million and £10.8 million annually on personnel and tools to meet due diligence and regulatory requirements related to research security.[127] These costs are expected to rise as regulatory frameworks expand, placing additional pressure on university budgets and diverting resources from core research activity and innovation. The government has recognized these challenges and has initiated work to establish a dedicated fund to help support the operational costs of implementing research security measures across the university sector. However, at the time of writing, the fund is not yet in operation, leaving institutions to absorb most compliance costs themselves.

Universities have limited incentives to allocate their own resources to strengthening research security, which is often viewed as an administrative overhead rather than as an activity that generates revenue or enhances competitive advantage.

Moreover, universities have limited incentives to allocate their own resources to strengthening research security, which is often viewed as an administrative overhead rather than as an activity that generates revenue or enhances competitive advantage.[128] Efforts to improve research security should also consider what happens when research is not taken forward for security reasons. Universities report that, in these cases, the underlying research or technology is often abandoned because no alternative domestic funding is available.

These pressures are arguably amplified by government-defined performance metrics. The Research Excellence Framework (REF), the UK's primary mechanism for assessing research quality and allocating public research funding, exerts a powerful influence over institutional behaviour.[129] The REF's assessment criteria strongly incentivize activities associated with global academic engagement, including producing internationally recognized research, cultivating globally connected research environments, and demonstrating wide-reaching academic and societal influence.[130] Yet existing assessment frameworks make no reference to research

---

126 Author's interviews with academics; author's interview with business development manager.
127 Marwaha, S. et al. (2023), *Complex Collaborations: Efficiency, Equity, Quality and Security in International Research*, Association of Research Managers and Administrators, March 2023, p. 25, https://arma.ac.uk/wp-content/uploads/2023/03/Trusted-Report_Booklet_v7.pdf.
128 Author's interviews with research security professionals.
129 Research Excellence Framework (REF 2029) (2025), 'Guidance', Research England, published 16 January 2025, last updated 10 December 2025, https://2029.ref.ac.uk/guidance.
130 Research Excellence Framework (REF 2029) (2025), 'Section 6 – Engagement and Impact guidance', 10 December 2025, https://2029.ref.ac.uk/guidance/section-6-engagement-and-impact-guidance; Research Excellence Framework (REF 2029), 'Section 7 – Strategy, People, and Research Environment (SPRE) guidance', 10 December 2025, https://2029.ref.ac.uk/guidance/section-7-strategy-people-and-research-environment-guidance.

security or to institutional management of the risks associated with international collaboration on sensitive research topics (for example, research with potential dual-use applications). Furthermore, while initiatives focused on higher education policy, such as the government's 2026 International Education Strategy, strongly encourage the growth of TNE, most make only cursory reference to managing the security risks inherent in operating overseas, or to the long-term financial and legal risks of winding back international partnerships due to national security concerns or geopolitical shifts.[131]

The result is a structural tension at the heart of the UK research system. The openness, international partnerships and global talent flows that underpin scientific excellence are often the same factors that create research security vulnerabilities.[132] Addressing this challenge requires greater coherence between S&T policy and the UK's wider national security, defence and industrial objectives. Research security should not be treated as a standalone compliance exercise, but as part of a broader effort to ensure that academic research supports the UK's long-term prosperity, technological advantage and national security.

While proportionate protective mechanisms remain necessary, they are unlikely to generate sustained behavioural change unless accompanied by positive incentives that make secure research practices institutionally attractive and financially viable.[133] As the UK's civilian research base becomes more integrated with defence innovation – reflecting the government's ambition for the UK to become a 'leading tech-enabled defence power'[134] – universities are likely to face growing expectations to strengthen research security capabilities in order to qualify for roles in strategic defence and dual-use programmes. A more effective model would combine targeted regulatory 'sticks' with credible 'carrots'; the latter would reward strong research security practices with enhanced access to public funding, participation in strategic research programmes, and opportunities within the UK's defence and national security innovation ecosystem. Initiatives such as the Defence Universities Alliance (DUA) represent an important step in this direction, although broader mechanisms will be required to support institutions with differing levels of research intensity and security capability.

More fundamentally, reducing systemic vulnerabilities will require addressing some of the underlying pressures that can incentivize universities to enter into higher-risk partnerships, such as with military-linked Chinese entities. Ultimately, the goal should be to embed research security into the culture of academia as an enabling factor that delivers greater collaboration opportunities for industry, government and trusted international partners.

131 UK Government (2026), *The UK's International Education Strategy*.
132 Author's interviews with academics.
133 Author's interviews with academics, research security professionals and a business development manager.
134 Ministry of Defence (2025), 'The Strategic Defence Review 2025'.

Recommendations

- The UK government should make strengthening links between academia and government a central pillar of national S&T strategy, using defence investment as a strategic mechanism to align university research and innovation with long-term national priorities and research security best practice. In particular:
  - The DUA should be expanded beyond the initial 35 founding member universities[135] to encompass a wider range of institutions across the UK. An effective long-term model could grade universities across a spectrum of capability, so that some would be identified as 'centres of excellence' capable of delivering classified sensitive research with direct defence applicability at the highest level, while less well-equipped institutions that still met baseline criteria for the sophistication and maturity of their safeguards would be allowed to deliver unclassified dual-use research.
- Research assessment frameworks should be aligned with research security objectives. The REF should explicitly recognize adherence to best-practice research security as a metric indicating a strong research environment. Assessment criteria relating to international engagement should be reviewed to ensure they are balanced with appropriate risk management considerations.
- Where a research project is judged strategically valuable enough to be blocked from involving overseas collaboration or funding, the government should facilitate access to alternative domestic funding to retain capability within the UK. This could include streamlined pathways through UKRI, ARIA and the National Security Strategic Investment Fund.
- Policymakers and universities should treat over-reliance on international student fee income as a systemic dependency risk. The government should incorporate contingency plans for income diversification, and for potential reductions in international student levels in sensitive STEM fields, into its higher education and S&T policies so that universities can adapt their funding models accordingly without increasing exposure to research security risk.
- The government should operationalize a dedicated research security fund. This fund should help universities pay for due diligence, compliance with research security obligations, and capability-building.[136]

Fragmented governance

Governance of research security in the UK is fragmented, spanning a complex network of government departments, intelligence agencies, regulators, and funding and sectoral bodies (see Figure 1). At the strategic level, responsibility is divided between cabinet committees rather than consolidated within a single forum. Technology and innovation policy is primarily considered through the

135 Ministry of Defence and Luke Pollard MP (2026), 'Boost for skills and research as 35 universities across the UK partner in new defence alliance', press release, 13 July 2026, https://www.gov.uk/government/news/boost-for-skills-and-research-as-35-universities-across-the-uk-partner-in-new-defence-alliance.
136 Cabinet Office, Department for Science, Innovation and Technology, The Rt Hon Michelle Donelan and The Rt Hon Oliver Dowden CBE MP (2024), 'Government to launch new consultation to protect UK universities from security threats', press release, 26 April 2024, https://www.gov.uk/government/news/government-to-launch-new-consultation-to-protect-uk-universities-from-security-threats.

Cabinet Committee on Digital and Technology, while responsibility for economic security is subsumed within the National Security Council (NSC). The appointment in July 2026 of a dedicated minister for AI – Kanishka Narayan – within the cabinet represents a positive step in recognizing the strategic importance of AI and strengthening political leadership in this area. However, the role is necessarily focused on AI and does not provide equivalent ministerial leadership across the wider landscape of emerging S&T, nor in the broader early-stage research and innovation ecosystem on which long-term technological capability depends.

The institutional challenge remains the absence of a governance structure that consistently integrates S&T policy, economic policy and national security considerations.

More fundamentally, the institutional challenge remains the absence of a governance structure that consistently integrates S&T policy, economic policy and national security considerations. The NSC's broad remit – encompassing foreign policy, international relations, resilience, trade, development and economic security – limits the committee's capacity for sustained focus on cross-cutting issues such as research security.[137] Coordination relies on variable departmental participation and issue-specific escalation rather than on institutionalized integration. This contributes to persistent fragmentation between nominally security- and prosperity-related policy domains. The dissolution in 2023 of the NSC's Economic Security Sub-Committee further limited the capacity for cabinet-level interaction between policymakers focused on S&T and those responsible for national security.[138]

At the departmental level, the Burnham administration's 'machinery of government' reforms, introduced in July 2026, have the potential to improve coherence across a number of research security functions. The bringing together of the functions of DSIT and the Department for Business and Trade (DBT) within the new DBIST means that more of the policy levers underpinning research security – including S&T policy, oversight of public R&D funding, export controls and RCAT – are now situated within a single department. In principle, this should facilitate closer alignment between industrial strategy, S&T policy, research funding and research security, resembling the more integrated departmental model that existed under the former Department for Business, Energy and Industrial Strategy (BEIS).

However, responsibility for a number of other key regulatory mechanisms remains distributed across different entities, creating administrative complexity.[139] Moreover, even where functions are now housed within the same department,

---

137 Cabinet Office (2026), 'List of Cabinet Committees and their membership', updated 11 May 2026, https://www.gov.uk/government/publications/list-of-cabinet-committees/list-of-cabinet-committees-and-their-membership.
138 House of Commons Business and Trade Committee (2025), *Toward a new doctrine for economic security*.
139 Marwaha et al. (2023), *Complex Collaborations*.

long-established organizational siloes and regulatory regimes are unlikely to integrate rapidly. As a result, universities and research organizations are still required to navigate a complex landscape of overlapping obligations, guidance and regulatory mechanisms. The principal governance challenge is therefore no longer simply one of negotiating departmental boundaries, but of achieving effective coordination on an inherently cross-government issue.

This fragmentation is complicated by the UK's devolved constitutional governance arrangements, whereby regional responsibility for higher education and aspects of research and innovation policy falls to the national administrations of Scotland, Wales and Northern Ireland, while responsibility for national security remains the preserve of the UK central government. The result is that coordination across multiple governments and regulatory systems is needed to deliver a coherent UK-wide approach to research security.

Within this fragmented landscape, RCAT plays an important practical convening role by providing a first point of contact for universities seeking government advice on international research collaborations. RCAT helps translate a dispersed policy and regulatory framework into a more navigable operational interface, and helps coordinate stakeholders within relevant areas of Whitehall.[140] Furthermore, sectoral organizations have increasingly emerged to fill coordination gaps. Bodies such as UUK and HERSA have developed guidance, shared resources and capacity-building initiatives to support universities in meeting research security expectations. While these developments are widely regarded as constructive and have improved practical awareness and capability across parts of the sector, universities continue to encounter overlapping requirements, differing terminologies and multiple points of engagement; this increases administrative burdens and uncertainty over accountability.[141]

Recommendations

- The government should re-establish the Economic Security Sub-Committee of the NSC, with the secretary of state for business, innovation, science and trade and the new minister for AI as permanent members. The remit of the sub-committee should explicitly include protecting critical and emerging technologies from national security risks.[142]
    - The sub-committee should be supported by a dedicated secretariat and working group, bringing together senior representatives from DBIST, RCAT, the FCDO, the Cabinet Office, UKRI, NPSA, the NCSC and the intelligence community. The secretariat and working group should coordinate cross-government policy development, oversee implementation, facilitate information-sharing and support collective ministerial decision-making.

140 Research Collaboration Advice Team (2026), 'Research Collaboration Advice Team: 2026 update'.
141 Author's interviews with research security professionals and academics.
142 These responsibilities include implementing the lessons from Japan's cross-government coordination at the ministerial level.

— The government should reactivate the NSTIx, which was dissolved in 2025. The NSTIx should provide cross-government insights on the intersection between national security and S&T, and should seek to foster collaboration and coherence across Whitehall.

Sectoral diversity

The UK's university sector is highly heterogeneous, with institutions varying significantly in size, availability of resources, research intensity, disciplinary focus, student and academic composition, and international engagement. Universities have adopted research security policies and practices at markedly different speeds, resulting in substantial variation in the sophistication and maturity of their institutional security policies and protocols.[143]

Some universities have taken a proactive approach, often developing their policies before formal government guidance is available, supported by strong senior leadership, dedicated resourcing, the development of specialist teams, and structured due diligence and risk management. Other institutions remain largely reactive in their approaches, formulating research security policies only after reputational or security-related incidents occur. In such cases, research security is often treated primarily as an administrative compliance burden and, at times, as an obstacle to funding opportunities rather than as a strategic institutional function.[144]

Variation is also evident across disciplines within universities. Researchers and managers in fields rooted in fundamental science, or reliant on highly internationalized research networks, may exhibit lower awareness of security risks than their counterparts in applied-science or defence-adjacent disciplines, where risk considerations are more embedded due to regulatory oversight and closer industry engagement.[145] The result is uneven research security both across the university sector and within institutions, reflecting differences in leadership priorities, institutional culture and resource allocation.

Given that responsibility for implementation of research security policies largely rests with universities, these disparities translate into systemic vulnerability. Research security practitioners increasingly highlight the risk of 'forum shopping', whereby external actors may seek out institutions perceived as having weaker controls when access is restricted elsewhere. Put simply, the sector is only as strong as its weakest link.[146]

A key cause of this unevenness is the absence of a sufficiently detailed and shared national baseline of standards for research security due diligence. The establishment in 2024 of NPSA's Trusted Research Evaluation Framework (TREF) has been a step forward, but the robustness and maturity of institutional security systems remain largely self-assessed against broad indicators, such as the existence of training

143 Hüsch and Buckley (2025), *UK National Security Advantage from Disruptive Technologies*; author's interviews with research security professionals and academics.
144 Marwaha et al. (2023), *Complex Collaborations*.
145 Interviewees noted that research security procedures in the life sciences, including engineering biology, were generally less mature than in fields like quantum computing; author's interviews with academics and a research security professional.
146 Author's interviews with research security professionals.

programmes or relevant internal policies.[147] Institutions are left to determine their own risk appetite and develop protocols and practice to meet their own requirements, with limited prescriptive detail from government.[148] Recent initiatives by NPSA and the NCSC, as well as collaboration checklists and UKRI and ARMA due diligence questionnaires, have improved consistency at the margins. However, these tools remain high-level and generic in nature: for example, requiring evidence that a conflict-of-interest policy exists but not details of how the policy has been applied to a specific project.[149]

There are no mandatory, UK-wide standards for minimum evidentiary requirements, verification processes or thresholds for unacceptable risk in international research collaborations.

More broadly, there are no mandatory, UK-wide standards for minimum evidentiary requirements, verification processes or thresholds for unacceptable risk in international research collaborations. The absence of common benchmarks is particularly acute in relation to strategically sensitive dual-use research and partnerships involving Chinese institutions.[150] As a result, different universities may reach materially different risk judgments for similar types of collaboration; these judgments will depend on each institution's capability, experience and risk tolerance.[151]

Such inconsistencies are compounded by unequal access to the data sources, analytical tools and expertise required for rigorous due diligence. Alongside support from government bodies such as RCAT, universities rely on a wide range of open-source intelligence (OSINT) platforms, commercial databases and proprietary research security tools to conduct due diligence, each with differing methodologies and access to information.[152] Consequently, different institutions may arrive at substantially different assessments of the same foreign research partner or potential partner.

For example, a specialist tool such as ASPI's Defence Universities Tracker – used widely across the UK university sector to map links between Chinese universities and China's defence-industrial ecosystem – may produce significantly different risk assessments from those generated from other publicly available OSINT resources. Access in the UK to due diligence capabilities is also uneven. Many advanced platforms are expensive and subscription-based, placing them beyond the reach

147 National Protective Security Authority and National Cyber Security Centre (2024), *Trusted Research Evaluation Framework*, https://www.npsa.gov.uk/system/files/6.8537_npsa_tr_evaluation-framework_v5_final_web2_0.pdf.
148 Author's interviews with research security professionals.
149 UK Research and Innovation (UKRI) (2022), 'Due diligence guidance and supporting documents', 26 October 2022, https://www.ukri.org/publications/due-diligence-guidance-and-supporting-documents; Marwaha et al. (2023), *Complex Collaborations*.
150 Author's interviews with research security professionals.
151 Quimbre, Carlyon, Dewaele and Drew (2022), *Exploring Research Engagement with China*; Marwaha et al. (2023), *Complex Collaborations*.
152 Author's interviews with research security professionals.

of smaller or less well-resourced institutions. These universities may lack the financial and analytical capacity to conduct comprehensive risk assessments of complex international partnerships.[153] Strengthening coherence, institutional capability and minimum standards across the sector is essential to improving the consistency and effectiveness of UK research security policy.

Recommendations

- The UK should operationalize a planned research security fund along the lines of Canada's Research Support Fund (see Chapter 4). The fund should be structured around two complementary pillars:[154]
  - **Sector-wide capability uplift.** The fund should pay for shared infrastructure and common services that foster standardized approaches to due diligence and risk management. The UK should consider the feasibility of setting up a sector-wide due diligence platform – where institutions can share anonymized assessments and indicators – and developing and rolling out training programmes and model governance frameworks endorsed by the government.
  - **Targeted institutional capability-building.** The fund should provide financing to enable academic institutions to (a) establish and grow research security teams with specialized expertise, (b) develop internal compliance and governance systems, (c) invest in cyber and physical security systems, and (d) procure OSINT tools to assist due diligence functions.
- Building on existing 'Trusted Research' guidance developed by NPSA and the NCSC, and drawing on established training models created by HERSA (such as its courses on navigating the export control and National Security and Investment Act regimes), the UK government and university sector should co-create a formalized professional accreditation for research security personnel.
  - A structured training programme should cover due diligence and risk assessment methodologies, investigation skills for identifying foreign affiliations, funding and influence risks, and key legislative requirements; it should also include briefings from NPSA and the NCSC on emerging research security threats.

Protecting know-how and managing people-centred risks

A persistent challenge for research security policy is that some of the most strategically valuable forms of knowledge are not easily captured through formal regulatory protections. In emerging S&T fields, critical expertise is often tacit in nature: embedded in individual researchers' skills, judgment, technical know-how and problem-solving practices rather than codified in documents or datasets. This tacit knowledge is frequently transferred through informal human interaction

153 Marwaha et al. (2023), *Complex Collaborations*.
154 This proposed approach recognizes that both pillars are critical to the embedding of research security across the university system as well as within institutions. A fund focused only on institutional programmes risks reinforcing existing inequalities and divergence across the sector. A fund focused only on sector-wide services risks creating common resources which institutions may lack the staff or governance capacity to use effectively.

such as laboratory work, mentorship, collaborative experimentation and researcher mobility, making it more difficult to monitor and regulate through conventional compliance mechanisms.[155]

Academics and experts interviewed for this paper consistently identified people-centred risks and tacit knowledge transfer as among the least understood and most difficult-to-mitigate vulnerabilities.[156] Joint PhD programmes, postdoctoral positions and other long-term collaborative arrangements such as talent programmes place researchers, many of whom are international, at the centre of cutting-edge STEM research and embed them within laboratory ecosystems. Through sustained presence in these environments, researchers may acquire technical skills, methodological know-how and exposure to emerging research that is not yet publicly documented or commercially protected. In some cases, individuals may subsequently return to their home institutions or move into industry roles carrying this expertise into different national innovation systems.[157] The risk of unauthorized or otherwise problematic knowledge transfer may be especially pronounced where PhD and postdoctoral researchers are sponsored or funded by foreign government-linked programmes such as the China Scholarship Council (CSC).[158]

From a research security perspective, visa and immigration screening mechanisms represent an important first layer of protection. The UK's Academic Technology Approval Scheme (ATAS) provides formal vetting of international students and researchers in sensitive STEM disciplines as part of the visa application process. However, coverage is not comprehensive. In particular, newer visa routes – such as the Global Talent visa pathway – do not require an ATAS certificate, creating potential gaps in pre-arrival screening for individuals entering highly sensitive research environments.[159] Anecdotal evidence suggests that international researchers are being encouraged to pursue these visa routes as they are quicker and less administratively burdensome.

In any event, visa screening alone cannot address tacit-knowledge leakage risks. Other regulatory frameworks and institutional due diligence processes in the UK overwhelmingly focus on formal arrangements – such as memorandums of understanding, grant agreements, visiting fellowships or joint ventures – at the point of initiation of a research project or collaboration. Comparatively limited attention is paid to the informal and evolving relationships that develop throughout the life cycle of research collaboration.[160]

As a result, institutions may conduct rigorous due diligence at the commencement of a project but possess limited mechanisms for continuous monitoring once a project or collaboration with foreign entities or researchers is under way. Researchers may acquire additional affiliations, participate in overseas talent or fellowship schemes,

---

155 Hughes et al. (2025), *Securing the UK's AI Research Ecosystem*.
156 Author's interviews with research security professionals and academics.
157 Vogel and Ben Ouagrham-Gormley (2023), 'Scientists as spies?'; Universities UK (2025), 'Managing risk and developing responsible transnational education (TNE) partnerships', last updated 18 February 2025, https://www.universitiesuk.ac.uk/universities-uk-international/insights-and-publications/uuki-publications/managing-risk-and-developing-responsible.
158 Author's interviews with academics; UK-China Transparency (2023), 'China Scholarship Council 'Rules' – translation and notes', 15 November 2023, https://ukctransparency.org/data/media/2023/11/China-Scholarship-Council-Rules-translation-and-notes-1.pdf.
159 Parton (2025), *China, science and technology*.
160 Author's interviews with research security professionals.

engage in informal knowledge exchange, or collaborate across overlapping projects in ways that fall outside the scope of initial risk assessments. These risks are not limited to the movement of researchers into the UK; UK-based researchers may also transfer strategically significant expertise through participation in foreign talent programmes, consultancy arrangements, visiting appointments, or involvement in academic conferences or other forms of engagement overseas. This creates structural blind spots in oversight, particularly in fast-moving fields where knowledge is embedded in individuals rather than formal research outputs.[161]

The challenge for policymakers is not to reduce international collaboration, but to differentiate between valid scientific exchange among trusted partners and higher-risk activities that may contribute to the transfer of strategically significant capabilities.

In this context, effective mitigation depends not only on formal screening mechanisms such as ATAS, but also on sustained, ground-up research security awareness and the embedding of a risk-aware culture within universities themselves, ensuring that researchers understand risk pathways and can identify and escalate concerns as collaborations evolve.[162]

At the same time, the UK's research excellence depends upon attracting international researchers. The British government has rightly recognized this through initiatives such as the Global Talent Fund and the Global Talent visa, which seek to attract leading researchers in strategically important fields. However, Britain struggles to compete for STEM talent because of relatively low salaries compared with those available in competing markets, and because of the widely held perception among potential applicants that UK visa processes are cumbersome. The challenge for policymakers is therefore not to reduce international collaboration, but to differentiate between valid scientific exchange among trusted partners and higher-risk activities that may contribute to the transfer of strategically significant capabilities. Research security measures must strengthen the UK's resilience without making Britain a less attractive destination for world-leading researchers.

Recommendations

— The UK government should do more to incentivize trusted international STEM talent to locate to the UK. The government should expand the Global Talent Fund to support the work of leading researchers in key technologies, and should align recruitment with national S&T priorities. Funding should extend beyond individual fellowships to support research teams, laboratory capability and commercialization of research, ensuring that world-class talent can establish long-term research programmes.

161 Author's interviews with academics and a research security professional.
162 Author's interviews with research security professionals.

- The UK should address potential research security gaps in the Global Talent visa route by ensuring the scheme adopts proportionate screening standards equivalent to those in other STEM visa pathways – including, where appropriate, using ATAS-style checks. Where possible, STEM-relevant visas should be prioritized for fast-tracked processing.
- The government and university sector should require enhanced disclosure and risk assessment for researchers who will be funded through foreign state-sponsored scholarships, talent programmes and other in-kind arrangements when these applicants will be working in sensitive STEM fields. Necessary safeguards should include:
  - Ensuring foreign government sponsorship, talent programme participation and associated contractual obligations are appropriately captured and assessed through relevant visa screening mechanisms, including ATAS.
  - Revising UKRI's standard terms and conditions to require mandatory disclosure of collaborators' foreign affiliations, appointments, associations and sources of funding.
  - Universities ensuring that staff conducting due diligence have routine access to conflict-of-interest disclosures, with processes in place to periodically review these records throughout the life cycle of research activity. Where feasible, institutions should develop centralized systems capable of identifying and flagging high-risk indicators. Where elevated risks are identified, universities should apply proportionate safeguards and consider referring such cases to RCAT.

Complexity of the security environment

Universities are increasingly required to operate in a rapidly evolving and contested geopolitical environment, in which both regulatory expectations and underlying threat dynamics are in flux. This challenge is compounded by resource constraints within institutions, and is likely to intensify as highly motivated hostile actors adapt their methods in order to circumvent existing safeguards.[163]

One of the critical difficulties remains assessing the risk posed by the research itself. Emerging domains such as AI, quantum technologies and engineering biology are inherently dual-use. In many cases, the strategic significance of research may not become apparent until years after the initial discovery, particularly in early-stage or fundamental science where downstream applications remain uncertain. While academic researchers are typically best placed to understand the technical implications of their work, translating specialized scientific knowledge into forms usable for risk assessment is often difficult. Professional services staff responsible for research governance may lack the expertise to evaluate rapidly evolving technologies.[164] The design of existing regulatory tools can add to this challenge. For instance, export control regimes were largely designed for industrial contexts involving tangible goods and defined end-users, and are poorly

163 Marwaha et al. (2023), *Complex Collaborations.*
164 Author's interviews with academics and a research security professional.

adapted to capturing the security implications of the transfer of cutting-edge, intangible research. This makes the relevant administrative processes particularly burdensome for academia.[165]

Furthermore, institutions face increasing difficulty in accurately assessing the risks associated with international research collaborations. This challenge is particularly acute in relation to China, where the boundaries between civilian, military and security actors are often opaque and difficult to distinguish. As a result, ostensibly low-risk Chinese universities, research institutes or companies may have links to wider defence and national security networks that are not immediately apparent. Consequently, due diligence based primarily on formal institutional affiliation or publicly available information is often insufficient to provide a complete picture of risk.[166]

These challenges create uncertainty regarding what constitutes an acceptable level of risk and how existing research security guidance should be interpreted and put into practice. While RCAT and campaigns such as the UK government's Trusted Research guidance framework, together with a more proactive approach by the security agencies to raise public awareness of emerging threats, have strengthened institutional awareness and capability, many universities continue to face challenges in translating high-level principles into practical and consistent decision-making. This has generated growing demand within the university sector for more detailed, practical and actionable support from government.[167]

Universities often express frustration that RCAT is unable to provide sufficiently clear or definitive judgments regarding complex collaborations, or to explain in detail why particular entities, technologies or partnerships may present elevated risks.[168] To a significant extent, these limitations are unavoidable. RCAT advice and many related regulatory decisions are often informed by classified intelligence that cannot readily be disclosed, while RCAT itself has no regulatory authority to direct institutional decision-making.

Nevertheless, there remains considerable scope to improve the specificity, consistency and utility of government support, particularly in areas where universities face repeated uncertainty.[169] More broadly, generalized or country-agnostic guidance is increasingly viewed as inadequate for addressing the distinctive characteristics of China's political, legal and institutional system.[170]

In response to similar challenges, jurisdictions such as Canada have adopted 'list-based' approaches, naming entities of concern. Proponents of such mechanisms argue that these provide universities with clarity and reduce the burden on researchers to interpret complex geopolitical and institutional risks independently. However, list-based approaches present limitations. Organizations linked to military or state security systems may conceal their connections through subsidiaries, affiliated institutes, joint ventures or alternative naming structures, making static lists inherently incomplete and quickly outdated. There is also

---

165 Author's interviews with academics.
166 McFaul, Bresnick and Chou (2025), *Pulling Back the Curtain on China's Military-Civil Fusion.*
167 Marwaha et al. (2023), *Complex Collaborations*; author's interviews with research security professionals.
168 Author's interviews with research security professionals.
169 Marwaha et al. (2023), *Complex Collaborations.*
170 Author's interviews with research security professionals and an academic.

a danger that over-reliance on designated lists may create a false sense of security. This may encourage institutions to assume that unlisted entities are low-risk, thereby weakening due diligence and preventing rigorous risk assessment that would consider all aspects of a collaboration.[171]

Ultimately, the challenge of navigating the complex threat environment cannot be resolved through static compliance mechanisms alone, and a purely list-based approach is unlikely to be appropriate for the UK. The pace of technological change, the evolving nature of geopolitical competition and the growing integration of civilian and military S&T ecosystems require more adaptive, intelligence-informed and institutionally embedded approaches to research security.[172] Despite certain calls from within the university sector for prescriptive and granular guidance from the government, the realities of risk management in the context of ever-evolving state threats mean that universities must accept a certain level of ambiguity. The long-term objective of policy should therefore focus on cultivating durable security awareness, institutional resilience and agile risk-management capabilities. Achieving this may require government to explore more structured mechanisms for sharing appropriately declassified threat information with trusted university personnel.

Recommendations

- The UK government should assess the feasibility of extending security clearances to key personnel in universities. This would allow the sharing of classified intelligence assessments with research security teams to support informed decision-making.[173] Given delays in security clearance processing by UK Security Vetting[174] – the unit in the Cabinet Office that provides vetting for all government departments and many public bodies – such efforts should be accompanied by commensurate resourcing to ensure appropriate clearances are issued in a timely manner.
- The UK government should provide more detailed and actionable research security guidance.[175] Rather than maintaining a public list of prohibited or restricted entities, the government should expand the volume of information available for research organizations and academics.
    - Where possible, existing intelligence and analysis should be sanitized and declassified for wider dissemination. Awareness of research risks could be improved across the academic sector by publishing more official assessments on priority S&T fields and their dual-use risks, as well as by issuing country-specific advice outlining how different state actors may seek to acquire, transfer or exploit sensitive S&T research.

171 Author's interviews with research security professionals.
172 McFaul, Bresnick and Chou (2025), *Pulling Back the Curtain on China's Military-Civil Fusion*.
173 Cabinet Office, Department for Science, Innovation and Technology, The Rt Hon Michelle Donelan and The Rt Hon Oliver Dowden CBE MP (2024), 'Government to launch new consultation to protect UK universities from security threats'.
174 House of Commons Committee of Public Accounts (2023), *The performance of UK Security Vetting*, Fifty-Third Report of Session 2022–23, HC 994, 12 May 2023, https://publications.parliament.uk/pa/cm5803/cmselect/cmpubacc/994/report.html.
175 Marwaha et al. (2023), *Complex Collaborations*.

  - More detailed assessments could be provided at a higher level of classification to cleared key university personnel on the risks associated with particular categories of foreign-linked organizations, such as military-affiliated universities, state-owned enterprises, defence-industrial entities and government-sponsored research institutes.

- Existing regulatory mechanisms should be adapted to the realities of academic research. In particular, export licensing application processes should be reformed to help academics articulate the plausible dual-use implications and realistic downstream applications of their work in terms accessible to non-specialist assessors.
- The UK government should increase funding to expand and empower RCAT.[176] While RCAT plays a vital advisory role, its function should be strengthened to enable the agency to operate with a more proactive research security and risk management capability. In particular:
  - RCAT should be granted clearer authority to request structured information and records from higher education institutions on their sensitive research programmes. This would help to identify cumulative and cross-cutting risks that may not be visible at the initiation of individual formal arrangements. To support these efforts, universities should be encouraged and assisted to develop and maintain central records of such research activities.

Limitations of self-regulation

Building resilience in an evolving threat environment requires more than nominal or token compliance at the point of funding or collaboration. It increasingly depends on three mutually reinforcing capabilities: (i) credible external validation of institutional risk assessments; (ii) ongoing monitoring across the life cycle of research activity; and (iii) proportionate enforcement mechanisms where risks or areas of non-compliance are identified.[177]

At present, the UK system is comparatively weak across all three dimensions, creating a structural reliance on institutional self-assessment that is increasingly difficult to sustain given the scale and complexity of international research collaboration.

Furthermore, the question of where regulatory oversight should reside within the UK framework remains unresolved, given that assigning such functions to RCAT would risk undermining its role as a trusted source of advice and guidance.

The system places primary responsibility for identifying and managing research security risk on universities themselves. This means that there is limited external validation of whether assessments are consistently or robustly applied. In practice, institutions act as both risk owners and principal assessors of their own compliance. While this model can be effective in environments characterized by full disclosure and good-faith behaviour, it creates inherent vulnerabilities when risks fall outside

176 Cabinet Office, Department for Science, Innovation and Technology, The Rt Hon Michelle Donelan and The Rt Hon Oliver Dowden CBE MP (2024), 'Government to launch new consultation to protect UK universities from security threats'.
177 Walker-Munro (2025), '(Professor) Hadrian's Wall'.

institutional visibility or are not captured by regulatory frameworks. It also depends heavily on complete and accurate disclosure of foreign affiliations, funding sources and collaborative arrangements. Where disclosure is incomplete, inconsistent or deliberately withheld, there is limited external capacity to detect or correct gaps in assurance.[178]

Furthermore, there is no systematic mechanism for ongoing review or cumulative risk assessment once research activity is under way. Existing instruments, and internal due diligence functions, largely function as point-in-time assessments at the initiation of formal funding or partnership agreements, without much in the way of structured reassessment as projects evolve. This is a significant weakness given the dynamic nature of research collaboration. Personnel move between institutions and projects, new sub-awards and parallel funding streams emerge, and research trajectories shift over time.

If not identified by institutions at the beginning of an arrangement, risks are often only identified after they have materialized, rather than being managed proactively across the life cycle of research activity.[179] At the strategic policy level – once the government's forthcoming research security strategy is released and implemented – attention must turn to how the new strategy's effectiveness will be measured, how success will be evaluated, and how the framework can be adapted as the threat environment, technological landscape and geopolitical context evolve.

Finally, these gaps are reinforced by a reliance on what can be considered 'soft compliance' mechanisms, where adherence to research security expectations is largely voluntary and mediated through institutional interpretation of risk appetite rather than through consistent external verification or enforcement. While preserving institutional autonomy and avoiding unnecessary bureaucracy remain important, the absence of meaningful external assurance creates a governance gap. Compliance cannot be reliably tested and may drift towards 'compliance formalism', whereby procedural adherence to broadly defined expectations substitutes for substantive risk management.[180]

A useful approach to these challenges is emerging in non-UK jurisdictions. It involves sharing responsibility for research security more explicitly between universities, public funding bodies and government, with funders playing a greater role in scrutinizing and validating institutional risk assessments.[181] While progress has been made on embedding research security principles and expectations within UKRI funding frameworks, the UK's current assurance mechanisms remain limited in their ability to ensure independent verification of risk. UKRI terms and conditions require institutions to undertake due diligence supported by standardized due diligence questionnaires. However, these instruments primarily test whether appropriate policies and processes exist, rather than how they have been applied to a specific project.[182]

---

178 Author's interview with research security professionals and academics.
179 Author's interviews with academics and a research security professional.
180 Walker-Munro (2025), *Shifting the needle*.
181 Walker-Munro (2025), '(Professor) Hadrian's Wall'.
182 Marwaha et al. (2023), *Complex Collaborations.*

Furthermore, institutions are not currently obligated to disclose to UKRI specific high-risk indicators – such as external consultancy arrangements, participation in foreign talent programmes or overlapping institutional affiliations – that would enable funders to assess risk independently.[183] As a result, UKRI has limited capacity to test whether institutional assessments fully reflect underlying exposure to risk. While some observers may be concerned that expanding UKRI's role could position the research funder as a *de facto* regulator, public funders already possess significant leverage through grant eligibility criteria and funding conditions. This creates a strong case for strengthening their assurance function as a complementary layer of oversight alongside institutional due diligence, rather than relying on universities as the primary mechanism of control.[184]

Recommendations

- UKRI should strengthen its 'trusted research and innovation' principles and expectations so that they become more of a core component of the research security system, complementing university governance and wider government regulation. In particular, UKRI should:
  - Revise its standard terms and conditions so that these expressly require mandatory disclosure of collaborators' foreign affiliations, appointments, associations and sources of funding.
  - Revise and update UKRI's 'trusted research and innovation' principles and accompanying due diligence guidance so that these align more explicitly with the evolving national security context of internationalized research. UKRI should draw on comparable international approaches such as the Australian Research Council's Research Security Framework, which articulates structured principles for assessing risk in relation to national security, defence and international relations.
  - Bolster capacity for conducting post-award monitoring and targeted spot checks in relation to higher-risk grants, to confirm that mitigation protocols remain effective and that emerging risks are identified over the life cycle of the research in question.
- The UK government should ensure UKRI is adequately resourced and empowered to undertake timely and proportionate risk assurance. This should include the capacity to undertake independent checks on applicant disclosures and validate information where necessary.

183 UK Research and Innovation (2025), 'UKRI Trusted Research and Innovation: principles and expectations', 13 June 2025, https://www.ukri.org/publications/ukri-trusted-research-and-innovation-guidance/ukri-trusted-research-and-innovation-principles-and-expectations; UK Research and Innovation (2026), 'Terms and conditions for research grants', published 5 April 2021, last updated 1 April 2026, https://www.ukri.org/publications/terms-and-conditions-for-research-grants.
184 Cabinet Office, Department for Science, Innovation and Technology, The Rt Hon Michelle Donelan and The Rt Hon Oliver Dowden CBE MP (2024), 'Government to launch new consultation to protect UK universities from security threats'; Marwaha et al. (2023), *Complex Collaborations*.

07 Conclusion

Improving UK universities' resilience in the face of rising research security threats will require closer integration between academic, industrial, defence and national security objectives. It will also require a cultural shift across government and the university sector.

Research security is ultimately about preserving the UK's capacity to generate prosperity, maintain national security, and sustain strategic advantage in an increasingly contested geopolitical environment. The challenge is to avoid retreating from international collaboration, which remains essential to scientific excellence and innovation, yet to ensure that openness is accompanied by appropriate safeguards. As this paper has argued, current vulnerabilities stem not only from specific high-risk actors or technologies, but also from structural features of the research system itself.

Addressing these challenges requires an integrated approach that aligns research security with the UK's broader S&T, industrial, defence and national security objectives. This is important given financial pressures that risk undermining the resilience of higher education institutions. As universities remain central to the government's long-term ambitions for economic growth, technological leadership and strategic advantage, research security policy must be designed to strengthen – rather than inadvertently weaken – the sector's capacity to deliver these objectives.

This means enhancing universities' capability to manage risk, improving government support and intelligence-sharing, adapting regulatory mechanisms, and strengthening the role of public funders as providers of supplementary assurance. It also means ensuring that the incentives shaping university behaviour are consistent with national priorities. Equally important is fostering a durable culture of research security across the university sector, in recognition of the reality that many of the most significant risks emerge through people and evolving collaborative networks rather than through discrete transactions or formal arrangements alone.

Looking ahead, the UK's research security framework should be designed not only for today's threat environment but for a range of plausible geopolitical futures. While more intrusive measures may not currently be necessary,

proportionate or feasible, the government should nevertheless establish clear trigger points and contingency plans for how the research security framework should adapt if threats to the UK's research base intensify. Such measures could include: enhanced enforcement powers; a centralized, intelligence-led clearing house for risk assessments and due diligence; expanded security reviews of patent filings and research publications; reform of the National Security and Investment Act to include mandatory notification of the acquisition of assets such as IP in sensitive S&T fields; and dedicated regulatory oversight of research security practice.

Enhanced measures could include the establishment of secure research zones, where access would be restricted to appropriately security-vetted researchers. Participation could be subject to additional conditions, such as requirements (where justified on national security grounds) for researchers to notify or obtain approval from the UK government for travel to higher-risk jurisdictions. Building this flexibility now will help ensure that the UK can continue to protect its research system – and with it, the national security, prosperity and strategic advantage on which the UK's future depends.

Annex 1

Table 2. UK government legislative and policy instruments relevant to research security

Legislation/ regulatory instrument/ guidance	Responsible government entity	Summary
Export Control Act 2002 and Export Control Order 2008; UK Strategic Export Control Lists (known as the consolidated list)[185]	Export Control Joint Unit, DBIST	Export controls regulate the transfer or sharing of certain controlled goods, software and technology (including technical expertise and knowledge) from the UK to overseas recipients or destinations. These controls apply not only to the export of physical items, but also to transfers of intangible assets via email or file-sharing systems, in virtual meetings, or through verbal disclosures or other forms of communication. The 'consolidated list' designates goods, software and technology subject to export controls, including dual-use items with both civilian and military applications. Controls may also apply under 'end-use' provisions where there are concerns that an item or system could be used for military purposes, in relation to weapons of mass destruction or for human rights violations. Where a transfer falls within the scope of export controls, an export licence may be required. Criminal penalties may apply in the event that an export licence is not obtained where applicable.[186]
National Security Investment Act 2021[187]	Investment Security Unit (formerly Cabinet office; now DBIST)	The Act provides the government with powers to investigate acquisitions deemed potentially detrimental to national security, and to require an acquisition to meet certain conditions. The Act also provides for the potential prohibition or reversal of a transaction where this is needed. The legislation applies to legal entities and assets, meeting certain criteria, that are termed 'qualifying entities' and 'qualifying assets' respectively. Acquisitions of qualifying entities or assets are called 'qualifying acquisitions'. Mandatory notification applies to acquisitions involving qualifying entities in one of the 17 sensitive areas[188] of the UK economy deemed to be critical to national security. The acquisition of entities in other areas of the economy, as well as the acquisition of assets (i.e. transfer of IP), does not fall under mandatory notification. However, entities may submit a voluntary notification of such acquisitions. The government may also require acquisitions to undergo scrutiny if they are deemed sensitive to the UK economy. Completing a mandatory notifiable acquisition without approval voids the acquisition and can result in civil or criminal penalties.

185 legislation.gov.uk (undated), 'Export Control Act 2002', https://www.legislation.gov.uk/ukpga/2002/28/contents; legislation.gov.uk (undated), 'The Export Control Order 2008', https://www.legislation.gov.uk/uksi/2008/3231/contents/made; Export Control Joint Unit and Department for Business and Trade (2025), 'Consolidated list of strategic military and dual-use items that require export authorisation', published 10 April 2013, last updated 16 December 2025, https://www.gov.uk/government/publications/uk-strategic-export-control-lists-the-consolidated-list-of-strategic-military-and-dual-use-items-that-require-export-authorisation.
186 Export Controls Joint Unit, Department for Business and Trade, and Department for International Trade (2024), 'Export controls applying to academic research', published 31 March 2021, last updated 2 August 2024, https://www.gov.uk/guidance/export-controls-applying-to-academic-research#exemptions.
187 legislation.gov.uk (undated), 'National Security and Investment Act 2021', https://www.legislation.gov.uk/ukpga/2021/25/contents; Universities UK (2022), *The National Security and Investment Act: Guidance for universities*, February 2022, https://www.universitiesuk.ac.uk/sites/default/files/uploads/Reports/national-security-and-investment-act-guidance-for-universities.pdf.
188 The 17 areas are: advanced materials, advanced robotics, artificial intelligence, civil nuclear, communications, computing hardware, critical suppliers to government, cryptographic authentication, data infrastructure, defence, energy, military and dual-use, quantum technologies, satellite and space technologies, suppliers to emergency services, synthetic biology and transport.

Legislation/ regulatory instrument/ guidance	Responsible government entity	Summary
Academic Technology Approval Scheme (ATAS); Immigration Rules[189]	FCDO	ATAS obligates certain foreign students and researchers to obtain approval from the FCDO as part of the visa application process to study or conduct research in sensitive technology-related fields in the UK. The relevant fields include academic subjects and occupation types listed in the Immigration Rules. Nationals of specified countries are exempt from the requirement to obtain an ATAS certificate. In addition, holders of certain visa types, including the Global Talent visa, are not required to obtain an ATAS certificate.
National Security Act 2023[190]	Home Office; MI5	The legislation expands the definition of criminal offences relating to espionage, sabotage, theft of trade secrets and foreign interference, and includes conduct that supports or facilitates hostile activity by a foreign power against the UK. Offences may apply even where the relevant conduct takes place partly or entirely outside the UK.
'Trusted Research' guidance	MI5 (NPSA) and GCHQ (NCSC)	The label 'Trusted Research' refers to a collection of guidance and advice developed by NPSA and the NCSC. According to NPSA documentation, 'Trusted Research supports the integrity of the system of international research collaboration' and its 'advice has been produced in consultation with the research and university community'.[191] The guidance and advice are intended to support researchers, university staff and funders in managing risks and protecting sensitive material from theft, misuse or other unauthorized/malign exploitation. The initiative includes bespoke advice for academia,[192] senior university leaders and industry, and includes guidance on risks presented by researchers travelling overseas for conferences or academic work and shared workspaces. As part of the initiative, NPSA and the NCSC developed the Trusted Research Evaluation Framework (TREF),[193] intended to provide academic institutions with a common tool to self-assess the maturity of their research security protocols.
Research Collaboration Advice Team	RCAT (formerly part of DSIT; now DBIST)	RCAT, launched in 2022 as part of the now-defunct DSIT, provides guidance to research institutions on national security risks associated with international collaboration. It is designed to help universities and academics understand emerging security threats and implement appropriate safeguards. RCAT offers advice on UK laws and regulatory requirements, delivers tailored risk-management support, and seeks to strengthen sector-wide capability and improve engagement between government and academia. RCAT is formed of regionally based advisers who are responsible for engaging directly with universities within their respective geographical areas.[194]

189 Foreign, Commonwealth and Development Office (2026), 'Academic Technology Approval Scheme (ATAS)', published 25 March 2013, last updated 24 March 2026, https://www.gov.uk/guidance/academic-technology-approval-scheme.
190 legislation.gov.uk (undated), 'National Security Act 2023', https://www.legislation.gov.uk/ukpga/2023/32/contents.
191 National Protective Security Authority (2025), *Trusted Research: Guidance for Academics*
192 Ibid.
193 National Protective Security Authority and National Cyber Security Centre (2024), *Trusted Research Evaluation Framework*.
194 Research Collaboration Advice Team (2026), 'Research Collaboration Advice Team: 2026 update'.

Legislation/ regulatory instrument/ guidance	Responsible government entity	Summary
UKRI terms and conditions for research grants;[195] UKRI Trusted Research and Innovation principles and expectations	UKRI (formerly part of DSIT; now DBIST)	UKRI sets terms and conditions for research grants and fellowships awarded by its subsidiary councils. These terms and conditions include obligations that recipients of grants adhere to UK research security-relevant legislation, ensure appropriate risk management policies are in place, and carry out appropriate due diligence on collaborative partners. Grant applicants must adhere to the principles on 'trusted research and innovation'.[196] These principles set out UKRI's approach to grant applicant assessment, noting that assessors may carry out a range of checks and may request further information from a proposed recipient before an award is made. This includes providing evidence of due diligence. In the event of non-compliance with its terms and conditions, UKRI may suspend, terminate or recover the grant. UKRI may also mandate that protective mitigations be put in place as a condition of the grant. UKRI has compiled supporting questionnaires and documents intended to provide guidance to research organizations on conducting due diligence on overseas partners.[197] Nevertheless, compliance with this material is not compulsory. UKRI notes that research organizations may develop their own policies commensurate with their risk appetite and the particulars of the research project in question.
Intellectual property laws – Patents Act 1977; Trade Secrets (Enforcement etc.) Regulations 2018[198]	Intellectual Property Office	Intellectual property law provides protection for creations of the mind, including inventions, designs and information of commercial value.[199] With regard to S&T, two forms of IP are most relevant: • **Patents:** novel inventions can be protected through a registered patent. By registering a patent, the creator is granted the exclusive right to the IP of the invention in exchange for making the invention public. This means patent holders can stop others making, selling or using their invention without a licence. However, in order to register a patent, the filer must provide adequate information about the invention. • Under s. 22 of the Patents Act 1977, the Intellectual Property Office has the power to give 'directions' prohibiting disclosure of a patent application if publication of the patent would be prejudicial to national security. While the office examines all filings for potential security risks, in practice the imposition of a secrecy direction is extremely rare and only applied to defence-related technology (not merely dual-use technology). • **Trade secrets:** this form of IP provides legal protection against the unauthorized acquisition, use or disclosure of secret trade information. To meet the definition of a trade secret, the information must be commercially valuable, known only to a limited group of persons, and subjected to reasonable steps to ensure its confidentiality.[200] In the UK, trade secrets are protected through a combination of statutory, common law and contractual measures.[201]

195 UK Research and Innovation (2026), 'Terms and conditions for research grants'.
196 UK Research and Innovation (2025), 'UKRI Trusted Research and Innovation: principles and expectations', 13 June 2025, https://www.ukri.org/publications/ukri-trusted-research-and-innovation-guidance/ukri-trusted-research-and-innovation-principles-and-expectations.
197 UK Research and Innovation (2022), 'Due diligence guidance and supporting documents'.
198 legislation.gov.uk (undated), 'Patents Act 1977', https://www.legislation.gov.uk/ukpga/1977/37/contents; legislation.gov.uk (undated), 'The Trade Secrets (Enforcement, etc.) Regulations 2018', https://www.legislation.gov.uk/uksi/2018/597/made.
199 Intellectual Property Office, https://www.gov.uk/government/organisations/intellectual-property-office.
200 'The Trade Secrets (Enforcement, etc.) Regulations 2018', s. 2 (Interpretation).
201 World Intellectual Property Organization (undated), 'OVERVIEW OF NATIONAL AND REGIONAL TRADE SECRET SYSTEMS: UNITED KINGDOM', https://www.wipo.int/documents/d/trade-secrets/docs-overview-country-sheets-uk-final.pdf.

Legislation/ regulatory instrument/ guidance	Responsible government entity	Summary
Sanctions and Anti-Money Laundering Act 2018	FCDO; HM Treasury (Office of Financial Sanctions Implementation)	The UK government defines sanctions as financial controls put in place 'to achieve a specific foreign policy or national security objective'.[202] Sanctions impose legal limitations on 'the provision of certain financial services',[203] and can 'restrict access to financial markets, funds and economic resources'.[204] This means that universities and research institutes may not enter any financial arrangements with sanctioned entities. Breach of sanctions may result in civil or criminal liability.[205]

202 Office of Financial Sanctions Implementation (2026), 'UK financial sanctions general guidance', updated 12 May 2026, https://www.gov.uk/government/publications/financial-sanctions-general-guidance/uk-financial-sanctions-general-guidance#overview-of-financial-sanctions.
203 Ibid.
204 Ibid.
205 Ibid.

About the author

Tahlia Peterson is a research fellow at the Royal United Services Institute (RUSI), focused on technology and national security. She is a former Richard and Susan Hayden Academy Fellow with the Queen Elizabeth II Academy for Leadership and the Next Generation at Chatham House, where she worked as part of the UK in the World Programme. Her research at Chatham House examined the UK's strategic approach to managing the risks and harnessing the opportunities posed by intensifying technological competition between the United States, China and the European Union, with a particular focus on emerging fields such as artificial intelligence, quantum computing and biotechnology.

Prior to joining Chatham House, Tahlia served as a strategic analyst for the Australian government, where she delivered high-level assessments and advice on security issues and geopolitical threats across the Asia-Pacific to senior decision-makers in government, partner governments and the private sector.

She holds a bachelor's degree in international and global studies and a bachelor of laws degree, both from the University of Sydney, and a master's degree in national security policy from the Australian National University.

Acknowledgments

The author would like to thank Olivia O'Sullivan for her mentorship and supervision on this project. Special thanks are due to all those who contributed their time, expertise and insights to this research, especially to the people the author interviewed and consulted across the UK government, the university sector and industry bodies, as well as experts from comparative jurisdictions. The perspectives and engagement of all these individuals were invaluable in shaping the findings of this paper.

The author is grateful to the UK in the World Programme and the Queen Elizabeth II Academy for Leadership and the Next Generation for their guidance and mentorship throughout the research process and her fellowship at Chatham House.

The author would also like to acknowledge Andrew Payne and the peer reviewers for their thoughtful and constructive feedback on earlier drafts, as well as Jake Statham for his careful editing and support in bringing this paper to publication.

This project was made possible due to funding provided by the Richard and Susan Hayden Academy Fellowship.

ISBN 978 1 78413 688 8
DOI 10.55317/9781784136888

Cite this paper: Peterson, T. (2026), *How the UK should protect its science and tech research from foreign state threats: A case for a more systemic approach to research security*, Research Paper, London: Royal Institute of International Affairs, https://doi.org/10.55317/9781784136888.

This publication is printed on FSC-certified paper.
designbysoapbox.com

Independent thinking since 1920

CHATHAM HOUSE

The Royal Institute of International Affairs
Chatham House
10 St James's Square, London SW1Y 4LE
T +44 (0)20 7957 5700
contact@chathamhouse.org | chathamhouse.org

Charity Registration Number: 208223