Utrecht Law Review

Economic Security and Higher Education: The Rise of Research Securitisation

ARTICLES

BRENDAN WALKER-MUNRO

ABSTRACT

In the last two decades, universities have undertaken a drastic re-engagement with their agendas of conducting of research in the national interest. Yet the historical independence of universities has been modified by geopolitics, with these institutions collaborating more frequently with arms of government (such as the military, intelligence agencies or law enforcement) on their research endeavours. Further, the commonality of research partnerships with overseas individuals and entities – crucial to the development of diversity in opinions and views – is being challenged in the face of subordination, manipulation or interference by malicious actors.

In response, one of the principal features of the European Commission's package on economic security was embedding 'research security' – the practice of protecting university-led research from interference, co-option or diversion by foreign powers for reasons of national interest. Whilst the link between economic security and national security is maturing and becoming clearer, the precise forms and mechanisms by which economic security is advanced by research security remains simultaneously contested and poorly explored.

One recent trend in research security protections has been the emergence of, or uptick in, the use of economic sanctions and controls to limit engagements or partnerships between universities and foreign entities. For that reason, this paper will focus on examining two specific examples of economic sanctions frameworks through the research security lens: the policy on Sensitive Technology Research and Affiliations of Concern of Canada, and the National Security and Investment Act 2021 of the United Kingdom. The paper will argue for the proper place of such economic controls typified in both regimes, as well as exploring the general utility and drawbacks associated with the use of economic sanctions and controls in the institution of research security. It will also develop several key suggestions that could be adopted by the Member States of the European Union as they begin to comply with the new requirements.

CORRESPONDING AUTHOR:
Dr Brendan Walker-Munro

Associate Professor, Faculty of Business, Law & The Arts, Southern Cross University, Coolangatta Queensland 4225, AU

brendan.walker-munro@scu.edu.au

KEYWORDS:
higher education; national security; research security; foreign interference

TO CITE THIS ARTICLE:
Brendan Walker-Munro, 'Economic Security and Higher Education: The Rise of Research Securitisation' (2026) 22(1) Utrecht Law Review 28–46. DOI: https://doi.org/10.36633/ulr.1178

DOI: 10.36633/ulr.1178

1 INTRODUCTION

If Baldwin was right in saying redefining security was 'something of a cottage industry' back in 1997,[1] then dealing with contemporary emerging notions of economic security must be like the dot-com boom of the 2000s: everybody is either getting on board or getting left behind. States around the world are overwhelmingly linking the broadening concept of national security to the protection of domestic bases of economic prosperity, technological advantage and market dominance.[2] The very notion of economic security – which could rationally cover everything from 'the ability of economies to weather risks and shocks, withstand economic pressure and coercion, manage strategic dependencies, protect critical infrastructure, [and] deter cyber-attacks and disinformation' – simultaneously describes the same hallmarks of countries at the forefront of shifts in international power dynamics.[3] Thus, economic dynamics are driving security dynamics. Economic security has gained an increased foothold in geopolitical debates, diplomatic and political statecraft is taking on an economic flavour and the rules-based global order is increasingly functioning according to the rules of the market.[4]

There are some obvious benefits to nation-States that can successfully protect their economies from externalities whilst also making, marketing or producing something of value. In the United States (US), economic dominance has come through semi-conductors and the tech 'pseudo-monopoly' constituted by Meta, Alphabet, Apple and others; whilst in the People's Republic of China (PRC) it has been telecommunications, commercial drones and electric vehicles.[5] So-called 'middle power' economies – Australia, Japan, India – leverage aspects of their technology-focused economies for political and strategic advantage, even against economically or militarily superior allies and adversaries.[6] Equally, when nation-States inevitably come to disagreement or even conflict – usually over the very fuel that their economies need to run like rare minerals or trade routes[7] – these matters are progressively resolved by tools of economic statecraft. Economic tools also have the benefit that they can be applied to allies and friends, allowing an implementing nation-State to remain on good political or diplomatic terms even whilst throttling competing economies.[8] As fictional Hollywood corporate raider Gordon Gekko would have it, 'greed is good'.[9] On this highly contested economic battleground, innovative research and development has become a prominent weapon. Novel technologies that are exploitable offer the country that hosts them a game-changing advantage. This has often involved the 'weaponisation of interdependence', the 'exploitation of economic links for geopolitical advantage' and using 'economic interdependence as leverage to achieve political liberalisation and countering foreign influence'.[10] Unsurprisingly, countries can (and have) resorted to illicit and semi-licit tactics to supplement their economic security, prompting complaints about the unfairness of economic dynamics driving security dynamics.[11] In some cases, it might be sour grapes because it appears the PRC (as one example) has proven far more adept at the game

1 David A Baldwin, 'The Concept of Security' (1997) 23(1) Review of International Studies 5, 5.

2 Joel Slawotsky, 'Conceptualizing National Security in an Era of Great Power Rivalry: Implications for International Economic Law' (2025) 42(3) East Asia 279.

3 Federico Steinberg and Guntram Wolff, 'Dealing with Europe's Economic (In-)Security' (2024) 15 Global Policy 183.

4 Henry Farrell and Abraham Newman, 'The New Economic Security State: How De-Risking Will Remake Geopolitics' (2023) 102(6) Foreign Affairs 106.

5 Danielle Cave and others, *ASPI's Critical Technology Tracker* (Australian Strategic Policy Institute 1 March 2023) <www.aspi.org.au/report/critical-technology-tracker> accessed 10 April 2025.

6 Clinton Fernandes, *Sub-Imperial Power* (Melbourne UP 2022).

7 Michael Renner, *The Anatomy of Resource Wars* (WorldWatch Paper No 162, October 2002) 10.

8 For example, consider President Donald Trump's imposition of tariffs on Canada, Australia and the EU in the first quarter of 2025: James Corera, 'Economic Security and Geostrategic Competition: Tariffs Don't Equal Coercion' (*The Strategist*, 25 March 2025) <www.aspistrategist.org.au/economic-security-and-geostrategic-competition-tariffs-dont-equal-coercion/> accessed 30 March 2025.

9 'Wall Street' (1987) 20th Century Fox.

10 Conor McCaffrey and Niclas Frederic Poitiers, 'Instruments of Economic Security' in Jean Pisani-Ferry, Beatrice Weder di Mauro and Jeromin Zettelmeyer (eds), *Paris Report 2: Europe's Economic Security* (CEPR Press 2024) 181–209 <https://cepr.org/publications/books-and-reports/paris-report-2-europes-economic-security> accessed 7 April 2025.

11 Zeba Siddiqui, 'Five Eyes Intelligence Chiefs Warn on China's "Theft" of Intellectual Property' (*Reuters*, 18 October 2023) <www.reuters.com/world/five-eyes-intelligence-chiefs-warn-chinas-theft-intellectual-property-2023-10-18/> accessed 30 March 2025.

DOI: 10.36633/ulr.1178

than the West.[12] Such pundits suggest that this leaves 'the rest of us … to choose a third option. We are allowing China to play by its own rules while we remain committed to the old game and expect the US to do the same'.[13]

Of centrality to this paper, in May 2024 the Council of the European Union (EU) accepted a Recommendation on Research Security (Council Recommendation).[14] Tellingly, the Council Recommendation was issued in January 2024 as part of the EU's package on economic security, consisting of 'promoting the EU's competitiveness … [p]rotecting the EU's economic security through a range of existing policies and tools … [and p]artnering with the broadest possible range of partners to strengthen economic security'.[15] The specific controls in the package included proposed revisions to the Foreign Direct Investment Screening Regulation, white papers on security risks in investment and dual-use goods, as well as the exposure draft of the Council Recommendation.[16] Article 9 of the Council Recommendation then asks Member States to '[p]ay specific attention to international cooperation in domains involving critical knowledge and technology, including those identified by the Commission Recommendation (EU) 2023/2113',[17] which sets out the Council's economic security strategy.[18]

This recommendation is just one example of an observable trend in the emergence of, or uptick in, economic sanctions to limit partnerships between universities and foreign entities on grounds relating to 'research security' (ie, the US, Canada and the EU) or the slightly less pejorative 'trusted research' (the term *du jour* in the United Kingdom (UK), New Zealand and South Korea). Laws and policies which enact these programmes differ between jurisdictions, but all of them seek to shield research and development – usually in universities or institutions associated with them – from national security threats such as espionage, foreign interference and trade secret theft. The very bedrock of research security in the EU has been framed by reference to economic securitisation; but the precise mechanisms by which Member States of the EU can enact the types of controls set forth in the Council Recommendation remains largely unexplored and under-theorised.

This paper will use the EU Recommendation as a prompt to explore the notion that economic dynamics are driving security dynamics, especially in the context of research security controls in higher education. The paper will explore two specific examples of economic sanctions frameworks in research security as instructive case studies: the policy on Sensitive Technology Research and Affiliations of Concern (STRAC) of Canada and the National Security and Investment Act 2021 (NSI Act) of the UK.[19] Canada and the UK are widely regarded as being world leaders in research security, having adapted strong protective measures in response to several academic misconduct and espionage scandals over the past five years.[20] Therefore, these frameworks are of increasing relevance to the EU both in terms of understanding the research security

12 John C Gannon, Richard A Meserve and Maria T Zuber, 'Reconsidering Research Security' [2025] Issues in Science and Technology 90.

13 Corera (n 9).

14 Council of the European Union, Council Recommendation of 23 May 2024 on enhancing research security [2024] OJ C/2024/3510 <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C_202403510> accessed 30 March 2025.

15 European Commission, 'Commission Proposes New Initiatives to Strengthen Economic Security' (Press release, 24 January 2024) <https://ec.europa.eu/commission/presscorner/detail/en/ip_24_363> accessed 30 March 2025.

16 European Commission, 'Memo on European Economic Security' (24 January 2024) <https://europa.eu/newsroom/ecpc-failover/pdf/qanda-24-364_en.pdf> accessed 30 March 2025.

17 Council of the European Union (n 15) art 9.

18 Commission of the European Union, Commission Recommendation (EU) 2023/2113 of 3 October 2023 on critical technology areas for the EU's economic security for further risk assessment with Member States [2023] OJ L2023/2113, C/2023/6689 <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202302113> accessed 13 January 2026.

19 It is worth noting that Canada has not only a federal government, but also provincial governments that have legislative authority for their regions and have passed their own laws relating to research security. Provincial laws relating to research security are out of scope for this paper, but more can be read here: Government of Canada, 'Protect Your Research – Regional Factsheets' (11 July 2021) <https://science.gc.ca/site/science/en/safeguarding-your-research/general-information-research-security/protect-your-research-regional-factsheets> accessed 29 March 2025.

20 Alex Wilner and others, 'Research at Risk: Global Challenges, International Perspectives, and Canadian Solutions' (2022) 77(1) International Journal 26, 27–28; Brendan Walker-Munro, 'National Security, Foreign Investment & Research Security: The Current State of Art' (2024) 33(2) Griffith Law Review 167, 169–71.

DOI: 10.36633/ulr.1178

approaches of two of their strongest research collaborators,[21] but also understanding the barriers to collaborative research (whether imposed for economic security or otherwise) are emerging as a crucial enabler for innovation and responsible internationalisation.[22] The paper will argue for the proper place of such economic controls typified in both regimes, as well as explore the general utility and drawbacks associated with the use of economic sanctions and controls in the institution of research security. It will also develop several key lessons that could be learned by the EU Member States as they begin to comply with the new requirements of the Council's recommendation.

2 THE THREAT

The definition of research security – for this paper at least – can be found in recitals to the Council Recommendation:

> anticipating and managing risks related to: (a) the undesirable transfer of critical knowledge and technology that may affect the security of the Union and its Member States, for instance if channelled to military or intelligence purposes in third countries; (b) malign influence on research where research can be instrumentalised by or from third countries in order to inter alia create disinformation or incite self-censorship among students and researchers infringing academic freedom and research integrity in the Union; (c) ethical or integrity violations, where knowledge and technologies are used to suppress, infringe on or undermine Union values and fundamental rights, as defined in the Treaties.[23]

Another useful addition can be drawn from a recent report into Australian research security, which held that the term meant:

> A set of actions taken by governments or other public or funding bodies, usually in collaboration with academia and research institutes, to safeguard against the risk of undesired technology transfers, interference in or misuse of research, and threats to research integrity.[24]

However, each nation-State often adopts a view of 'threat' to research security that is reflective of its broader economic security policies and position in the market. As an example, the US – a world leader not only in research and development but specifically in the development of semiconductors and information technologies – passed the CHIPS and Science Act of 2022 to protect that economic advantage.[25] The Act amended the William M (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021[26] to permit the listing of 'countries of concern',[27] which included:

- Any 'covered country'– namely the PRC, North Korea, Russian and Iran;[28] and
- Any country that the Secretary, in consultation with the Secretary of Defense, the Secretary of State and the Director of National Intelligence, determines to be engaged in

21 Marek Kwiek, 'What Large-Scale Publication and Citation Data Tell us About International Research Collaboration in Europe: Changing National Patterns in Global Contexts' (2021) 46(12) Studies in Higher Education 2629.

22 Kirstin RW Matthews and others, 'International Scientific Collaborative Activities and Barriers to Them in Eight Societies' (2020) 27(8) Accountability in Research 477, DOI: 10.1080/08989621.2020.1774373.

23 Council of the European Union (n 15) art 18(1).

24 Brendan Walker-Munro, *Shifting the Needle: Making Australia's Research Security Ecosystem Work Smarter* (Australian Strategic Policy Institute July 2025) <www.aspi.org.au/report/shifting-the-needle-making-australias-research-security-ecosystem-work-smarter/> accessed 7 August 2025.

25 CHIPS and Science Act of 2022 (Pub L 117–67).

26 § 9901; codified at 15 USC 4651.

27 This is to be contrasted with a 'foreign entity of concern', which is generally any entity listed by other US departments, including foreign Chinese military companies (the '§1237(b) list': 50 USC 1701; Pub L 105–261), Chinese military companies in the US (the '§1260H list': 10 USC 113; Pub L 116–283), the 'Entity List' maintained by the Bureau of Industry (15 CFR 744, Supplement No 4) or the Uyghur list (Uyghur Human Rights Policy Act of 2020, §9(b)(3); Pub L 116–45; 134 Stat 656).

28 10 USC § 4872(d)(2).

DOI: 10.36633/ulr.1178

conduct that is detrimental to the national security or foreign policy of the US: currently Burma, Cuba, Eritrea, Pakistan, Saudi Arabia, Tajikistan and Turkmenistan.[29]

Yet what is perhaps more important from a research security perspective is a focus on 'behaviours of concern', as this is largely the threat which underpins a basis for holding such countries to account for their illicit and quasi-licit activities. The G7 published a non-exhaustive list of such behaviours in late 2024, precisely for the purposes of articulating the 'risk' to which modern research practices amongst the Member States ought to be directed.[30] These included cyber threats (both indirect threats in the form of phishing or social engineering attempts, as well as direct threats such as ransomware and hacking), physical access breaches to steal research data or results, poor security hygiene, insider threats (including those 'self-motivated or supported or pressured by others to access or steal research for their own gain, or the gain of others'[31]) as well as partnering with outside parties (for 'undisclosed purposes or benefits with security implications'[32]) as well as offers of funding 'as an incentive to access or transfer research data, processes and outcomes, potentially without the transparent disclosure of the intended purpose or end user'.[33]

The targets of research security – that is, the specific threats to research that security controls are enacted to protect against – are often framed as entities including foreign nation-States but also organised crime groups, cybercrime organisations, right down to 'lone-wolf' or motivated opportunists (who may also be domestic in nature) that seek to infiltrate, subordinate and exfiltrate research programmes or institutions for the economic benefits that can be realised from such appropriated research. Once again, we see economic dynamics driving security dynamics: the threat of exfiltration of economically valuable research results in a securitisation of the research environment.

The PRC features heavily in complaints regarding breaches of research security.[34] Shadowy activities of other autocratic nations – largely Russia, Iran and North Korea – are occasionally referenced, although their activities are usually curtailed by their involvement in broader international wrongdoing.[35] For example, in April 2022 the EU suspended all funded cooperation with Russia owing to the invasion and war in Ukraine,[36] whilst both North Korea and Iran have been sanctioned by the EU for development of weapons of mass destruction.[37]

Collectively then, research security seeks to identify, proscribe and/or mitigate those behaviours of concern which more generally pose economic risk – whether engaged in by friend or foe – but with a recognition that certain countries and entities 'of concern' may utilise (or preferentially utilise) such behaviours to advance their own economies.

3 THE RESPONSE

Precise mechanisms of regulation in research security takes different forms, but all contemporary frameworks generally involve:

29 Preventing the Improper Use of CHIPS Act Funding 88 Fed Reg 65,600 (codified at 15 CFR § 231).

30 G7, 'Best Practices for Secure and Open Research Security and Integrity of the Global Research Ecosystem' (SIGRE Working Group February 2024) <www.science.gc.ca/site/science/sites/default/files/documents/1136-g7-best-practices-for-secure-and-open-research-october-2024.pdf> accessed 15 March 2025.

31 ibid 5.

32 ibid.

33 ibid.

34 Wilner and others (n 21); Richard Lester and others, 'Managing United States–China University Relations and Rrisks' (2023) 380(6642) Science 246, DOI: 10.1126/science.adg5619; Jeffrey Stoff, Leslie McIntosh and An Chi Lee, *Transparency and Integrity Risks in China's Research Ecosystem* (Center for Research Security & Integrity, September 2024); Tommy Shih and Caroline Wagner, 'The Trap of Securitizing Science' (2024) 41(1) Issues in Science and Technology 100.

35 Walker-Munro, 'National Security, Foreign Investment & Research Security' (n 21).

36 European Commission, 'Statement on Research by Commissioner Mariya Gabriel' (Media release, 3 March 2022) <https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_22_1528> accessed 29 March 2025.

37 European Commission, 'EU Sanctions Tracker' (January 2026) <https://data.europa.eu/apps/eusanctionstracker/> accessed 14 January 2025.

> the Government, along with non-departmental public bodies … [c]ontrolling who can perform research … [p]roducing guidance on how sensitive research should be performed, stored and disseminated … [and] [r]estricting how research and research outputs are funded and acquired.[38]

In concordance with those principles, many states looking to protect their economic security have framed controls applying to 'the "who", the "what" and the "how" of involvement in … research in the age of decaying, vulnerable or volatile geopolitical relationships'.[39] Such controls are usually present but scattered across numerous statutes: for example, laws that protect the rights to creative and intellectual property,[40] prohibit unauthorised dealings with trade secrets and espionage[41] or maintain high standards of research integrity (ie, enforcing existing obligations of disclosure around funding, conflicts of interest, etc).[42] The effectiveness of these controls might remain open to serious debate, but they have nevertheless appeared without fail in numerous jurisdictions with high-performing higher education institutions (HEIs) in the US,[43] followed quickly by Canada,[44] the PRC,[45] the UK[46] and the EU.[47]

3.1 DOMAINS OF RESEARCH SECURITY

A recent report by Universities UK International suggested that the government and institutions should focus on six domains where the risk of economic interference was highest: 'financial, reputational, academic freedom and freedom of speech, security, relationship and personnel management, and cyber, intellectual property (IP) and data management'.[48] A similar report in Australia likewise pointed to six domains, but from the perspective of the security measures enacted to protect economically valuable research: export controls, autonomous and multilateral sanctions, criminal law, foreign investment, travel and migration, and intellectual property.[49] In both cases, controls have evolved from the economic utility of the technology in question, such that the 'value' of the research becomes worthwhile protecting as a matter of domestic national security.

As an example of how economic dynamics drive security dynamics, one can consider federally funded research in the US. In 2009, a doctoral student at Duke University Ruopeng Liu allegedly took millions of dollars of metamaterials research back to the PRC, establishing a 'shadow laboratory' to replicate US advancements.[50] Now, university researchers must make disclosure statements relating to their employment, any engagement in foreign 'talent recruitment

38 Alexis Brown, 'What's Next for National Security and Research?' (Final report, Higher Education Policy Institute, February 2022) 15–16.

39 Brendan Walker-Munro, 'A Missed Opportunity: Amending the Defence Trade Controls Act 2012 (Cth) and Research Security' (2024) 2 Journal of Strategic Trade Control 1, 3, DOI: 10.25518/2952-7597.144.

40 Melissa Flagg, Autumn Toney and Paul Harris, *Research Security, Collaboration, and the Changing Map of Global R&D* (CSET Policy Brief, Center for Security and Emerging Technology, 2021).

41 Kathleen M Vogel and Sonia Ben Ouagrham-Gormley, 'Scientists as Spies?: Assessing US Claims About the Security Threat Posed by China's Thousand Talents Program for the US Life Sciences' (2023) 42(1) Politics and the Life Sciences 32.

42 Tommy Shih, 'The Role of Research Funders in Providing Directions for Managing Responsible Internationalization and Research Security' (2024) 201 Technological Forecasting and Social Change 123253.

43 US National Science Foundation, 'Research Security' (2024) <https://new.nsf.gov/research-security> accessed 2 April 2025.

44 Government of Canada, 'Safeguarding Your Research' (2022) < https://science.gc.ca/site/science/en/safeguarding-your-research> accessed 9 February 2025.

45 Ingrid d'Hooghe and others, 'Assessing Europe-China Collaboration in Higher Education and Research' (Leiden Asia Centre, 2018); Samantha Hoffman, 'The Hong Kong National Security Law and UK Academic Freedom' (Report commissioned for the British Association of China Studies, 2021).

46 National Protective Security Authority, 'Trusted Research' (2023) <www.npsa.gov.uk/trusted-research> accessed 4 April 2025.

47 Council of the European Union (n 15).

48 Universities UK International, 'Managing Risk and Developing Responsible Transnational Education (TNE) Partnerships' (Final report, 27 June 2024). See also Gordon Long, 'Safeguarding the Research Enterprise' (Report commissioned by JASON for the NSF, 21 March 2024) 2.

49 Walker-Munro, *Shifting the Needle* (n 25).

50 Cynthia McFadden, Aliza Nadi and Courtney McGee, 'Education or Espionage? A Chinese Student Takes his Homework Home to China' (*NBC News*, 24 July 2018) <www.nbcnews.com/news/china/education-or-espionage-chinese-student-takes-his-homework-home-china-n893881> accessed 1 March 2025.

programmes', as well as supplying information to the government to permit due diligence on contracts, collaborative partners and funding bodies for all research they conduct.[51] Thus, the expansion of broad 'security concerns' is premised on the potential loss of economic value in research, even in a university where research may be done for the 'public good'. Money that the US government invests in research is inevitably linked to service the interests of the US and must not go towards underwriting the economic development of a foreign country.

Internationally, the linkage of economic dynamics and security dynamics is resulting in growing calls for funding bodies to play a greater role in the secure administration of university research. Indeed, the Council Recommendation refers to the principles of 'responsible internationalisation' which concluded '[r]esearch funders that support international cooperation should also be able to request … risk assessments to ensure that the necessary measures are taken to ensure responsible internationalisation'.[52] These principles continue to highlight the need for the incorporation of 'reciprocity' – the notion that researchers should enjoy mutual benefits, influence and protections as outcomes of the research (as opposed to one-sided or uneven benefits for the parties).[53] Export controls are usually mentioned in research security contexts, but are considered blunt tools totally unsuited to the 'generally' fundamental research occurring in universities and higher education institutions.[54] Researchers likewise will give short shrift to economic security concerns relating to their work, often raising the arguments of open science,[55] non-discrimination in the face of academic inquiry[56] and academic freedom (which may or may not be protected by statute or constitutional provisions).[57]

There are significant benefits to allowing economic dynamics to drive security dynamics. First, it resolves the contentious notion of 'dual use' technology – those classes of technologies said to have both military and civilian end-uses, as distinct from those with purely civilian applications. Dual use as a concept becomes entirely untenable where almost every critical technology currently being researched can support or augment military capabilities (even if not regulated by arms control instruments[58]). If dual use is discarded in favour of controls based on economic security, technologies can be more easily identified and regulated based on a quantifiable assessment of their economic value to the domestic defence, manufacturing or industrial base of the state in question.

Moving on from that, other dichotomous regulatory lists with similar issues – such as technology-focused export control lists or lists of 'security relevant' (ie, high risk) biological agents[59] – can be gradually replaced or phased out. Given that these lists are generally adopted in the form of subordinate legislation or governmental declarations, they cannot adapt and react to research and developments at the speed at which the underlying tech markets operate.

51 National Science and Technology Council, 'Guidance for Implementing National Security Presidential Memorandum 33 (NSPM-33) on National Security Strategy for United States Government-Supported Research and Development' (Subcommittee on Research Security, Joint Committee on the Research Environment, January 2022) <https://bidenwhitehouse.archives.gov/wp-content/uploads/2022/01/010422-NSPM-33-Implementation-Guidance.pdf> accessed 17 March 2025.

52 Tommy Shih, Albin Gaunt and Stefan Östlund, *Responsible Internationalisation: Guidelines for Reflection on International Academic Collaboration* (STINT 2020) 5.

53 Shih, 'The Role of Research Funders' (n 43).

54 Claire Stalenhoef, Machiko Kanetake and Marijk van der Wende, *The Implications of the EU's Dual-Use Export Control Regulation 2021/821 for Universities and Academics* (Utrecht Centre for Regulation and Enforcement in Europe Working Papers, October 2022).

55 E William Colglazier, 'The Precarious Balance Between Research Openness and Security' (2023) 39(3) Issues in Science and Technology 87; Marcus Smith and Patrick Walsh, 'Security Sensitive Research: Balancing Research Integrity, Academic Freedom and National Interest' (2023) 45(5) Journal of Higher Education Policy and Management 495.

56 Wilner and others (n 21) 48; Diarmuid Cooney-O'Donoghue, 'The Politics of STEMM Collaboration between Australia and China: National Security, Geopolitics, and Academic Freedom' (2024) 48 Asian Studies Review 745, DOI: 10.1080/10357823.2023.2294800.

57 Samuel AW Evans and Walter D Valdivia, 'Export Controls and the Tensions Between Academic Freedom and National Security' (2012) 50 Minerva 169; Erin N Grubbs, 'Academic Espionage: Striking the Balance Between Open and Collaborative Universities and Protecting National Security' (2019) 20(5) North Carolina Journal of Law & Technology 235.

58 Lauren Sanders, 'Australia's Defense Export Control Regime and Critical Technologies' (2024) 2 Journal of Strategic Trade Control 7, DOI: 10.25518/2952-7597.93.

59 ibid; Piers Millett and others, 'Beyond Biosecurity by Taxonomic Lists: Lessons, Challenges, and Opportunities' (2023) 21(6) Health Security 521; Brendan Walker-Munro, 'Virtual Labs and Designer Bugs: Generative AI, Synthetic Biology and National Security' (2024) 31(2) Journal of Law and Medicine 353.

DOI: 10.36633/ulr.1178

Identifying research into specific areas or technologies on the basis of their economic value to the controlling state permits a more nuanced and accurate form of regulatory intervention.

There are also contemporary changes in both the funding and manpower of research and development to consider. The commercialisation of universities has pushed most research 'closer to the "D-end" of the R&D spectrum', thus there has emerged a growing and more insistent need to protect the economic benefits of the work occurring at these institutions.[60] Researchers have always had impacts in the geopolitical arena; after all, it should be remembered that during the Cold War, the Soviet-Union and the US engaged in tit-for-tat intellectual property theft as a form of State-sanctioned espionage.[61] Instead, when economic dynamics are permitted to drive security dynamics – especially where the geopolitical environment has become both vertically and horizontally more volatile – research security becomes easier to accept because it is ensuring economic viability as an arm of the national interest.[62]

3.2 CALLING OUT BAD ACTORS: CANADA'S SENSITIVE TECHNOLOGY RESEARCH AND AFFILIATIONS OF CONCERN

The Canadian definition of research security is arguably less inclusive than that of the Council Recommendation, with the former referring solely to 'the ability to identify possible risks to your work through unwanted access, interference, or theft and the controls that minimize these risks and protect the inputs, processes, and products that are part of scientific research and discovery'.[63] Originally circulated in 2015 by Public Safety Canada, Canada's federal public safety ministry, as a roadmap of 'safeguarding science',[64] clarity in that definition has been largely supplied in response to a series of research scandals where knowledge has been compromised because of the actions of foreign entities.

The most infamous of these scandals was the quiet suspension, and then termination, of the employment of medical researchers Dr Xiangguo Qiu and Keding Cheng at the Winnipeg-based National Microbiology Lab (NML).[65] Qiu and Cheng, both Chinese nationals, had been the subject of a Canadian Security Intelligence Service (CSIS) investigation that resulted in the cancellation of their security clearances to work with highly infectious diseases at NML, including the Ebola virus. The CSIS report – originally classified and only tabled in Canada's federal Parliament following a lengthy row between Prime Minister Justin Trudeau and the opposition[66] – documented significant research security failures over two years:[67]

(i) Qiu's collaboration with a Major-General in the People's Liberation Army and a top virologist at the Academy of Military Medical Sciences in the PRC;

(ii) Travel to the Wuhan Institute of Virology (paid by the PRC) to train Chinese scientists in the development of monoclonal antibodies;

60 John Krige, 'Regulating the Academic "Marketplace of Ideas": Commercialization, Export Controls, and Counterintelligence' (2015) 1 Engaging Science, Technology, and Society 1, 10.

61 Mario Daniels and John Krige, 'Beyond the Reach of Regulation? "Basic" and "Applied" Research in the Early Cold War United States' (2018) 59(2) Technology and Culture 226; Mario Daniels and John Krige, *Knowledge Regulation and National Security in Postwar America* (University of Chicago Press 2022).

62 Eugene Skolnikoff, 'Research Universities and National Security: Can Traditional Values Survive?' (MIT Working Paper MIT-IPC-02-005, April 2002); Tommy Shih, Andrew Chubb and Diarmuid Cooney-O'Donoghue, 'Scientific Collaboration Amid Geopolitical Tensions: A Comparison of Sweden and Australia' (2024) 87(5) Higher Education 1339.

63 Government of Canada, 'Why Safeguard Your Research?' (5 May 2022) <https://science.gc.ca/site/science/en/safeguarding-your-research/general-information-research-security/why-safeguard-your-research> accessed 17 March 2025.

64 Public Safety Canada, 'Research Security Information Update' (May 2021) <www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2021-rsi-psr-ma/index-en.aspx> accessed 17 March 2025.

65 House of Commons Special Committee on the Canada-People's Republic of China Relationship, 'The Nexus Between Science and National Security in Canada: The Case of the National Microbiology Laboratory in Winnipeg' (Final report, 44th Parliament, November 2024) <www.ourcommons.ca/documentviewer/en/44-1/CACN/report-8> accessed 28 March 2025.

66 The opposition actually passed a motion which held the Liberal government in contempt of Parliament, with the government responding by suing the Speaker of the House of Commons to force a judge to rule on the legal authority for Parliament to withhold the documents: see Catharine Tunney, 'Lies and Scandal: How Two Rogue Scientists at a High-Security Lab Triggered a National Security Calamity' (*CBC*, 2 March 2024) <www.cbc.ca/news/politics/winnipeg-lab-firing-documents-released-china-1.7130284> accessed 28 March 2025.

67 Special Committee (n 66) 8–13.

DOI: 10.36633/ulr.1178

(iii) The filing of a patent for an inhibitor of the Ebola virus with the Chinese National Institutes for Food and Drug Control, in which Dr Qiu was named as a contributor;

(iv) The shipping of live samples of Ebola and Henipah viruses to the Wuhan Institute of Virology.

Around the same time as the NML incident was occurring, Canada was stepping up its research security protections. Public Safety Canada published the document 'Building Security Awareness in the Academic Community'[68] which put universities on notice of both the threat and possible risk mitigations, whilst ministerial statements made clear that research security was emerging as a political imperative.[69] In 2023, the U15 Group (representing Canada's most research intensive universities) published a collation of practices they had identified as 'best practice' in research security.[70] At the same time, Canada's Liberal government established the National Security Guidelines for Research Partnerships (NSGRP), obligating applicants for federal funding to complete a risk assessment and propose risk mitigations as a condition of that funding.[71] In a report published last year assessing the impact of the NSGRP, Public Safety Canada identified that only 4% of applications had required more significant scrutiny, with 32 applications (out of 1,158 total applications received) refused on national security grounds.[72]

Following the NML incident, research security protections in Canada were strengthened again in 2024 with the launch of the Policy on STRAC. STRAC made clear that researchers in so-called 'sensitive technology areas' would not be eligible to receive federal funding if they were affiliated with, or received funding or in-kind support from, 'a university, research institute or laboratory connected to military, national defence, or state security entities that could pose a risk to Canada's national security'.[73] The STRAC was essentially comprised of two components – the Sensitive Technologies Research Areas (STRA) list,[74] and the Named Research Organisations (NRO) list.[75] Research into any area on the STRA list could not be conducted with federal funding if the researcher was affiliated with, or receiving funding or in-kind support from, an entity on the NRO list.

Although the STRA list is relatively well established, entities can be added to the NRO list at any time, if and when the federal government forms the view that the entity will 'pose the highest risk to Canada's national security due to their direct, or indirect connections with military, national defence, and state security entities'.[76] In this way, the STRAC is highly adaptable and reactive to emerging or changing geopolitical realities by 'calling out' threats – an important aspect of providing security to economies that move at speed and scale. It is also important to note that both the STRA list and the NRO list are considered non-exhaustive. The STRAC clearly articulates that collaboration with any research partner involving a technology on the STRA list,

68 Public Safety Canada, *Building Security Awareness in the Academic Community* (2019) <https://publications.gc.ca/site/eng/9.885586/publication.html> accessed 28 March 2025.

69 Innovation, Science and Economic Development Canada, 'Research Security Policy Statement – Spring 2021' (Media release, 24 March 2021) <www.canada.ca/en/innovation-science-economic-development/news/2021/03/research-security-policy-statement--spring-2021.html> accessed 28 March 2025.

70 U15 Group of Canadian Research Universities, 'Safeguarding Research in Canada: A Guide for University Policies and Practices' (June 2023) <https://science.gc.ca/site/science/sites/default/files/documents/2024-01/1173-safeguarding-research-in-canada-a-guide-for-university-policies-and-practices.pdf> accessed 28 March 2025.

71 Government of Canada, 'National Security Guidelines for Research Partnerships' (6 October 2022) <https://science.gc.ca/site/science/en/safeguarding-your-research/guidelines-and-tools-implement-research-security/national-security-guidelines-research-partnerships> accessed 29 March 2025.

72 Government of Canada, 'Progress Report on the Implementation of Canada's *National Security Guidelines for Research Partnerships* and Supporting Research Security Efforts' (January 2024) <https://science.gc.ca/site/science/en/safeguarding-your-research/general-information-research-security/additional-resources/annual-reports/progress-report-2021-2023> accessed 14 January 2025.

73 Government of Canada, *Named Research Organizations* (September 2024) 3 <https://science.gc.ca/site/science/sites/default/files/documents/2024-01/1082-named-research-organizations-list-09Jan2024.pdf> accessed 7 April 2025.

74 Comprised of 11 emerging or disruptive technology areas with potential use cases for military, intelligence or security purposes contrary to Canadian national security, like artificial intelligence, life sciences, aerospace technologies, robotics and quantum: ibid.

75 Most of the entities on the NRO are in the PRC, but several are also located in Russia and Iran, and the list itself is considered non-exhaustive.

76 Government of Canada, *Named Research Organisations* (n 74).

DOI: 10.36633/ulr.1178

or any other collaboration with an entity on the NRO list (ie, not involving an STRA technology), may still present risks to research security. Researchers continue to be encouraged to utilise the NSGRP for all forms of research collaboration, to underpin a deeper understanding of the partners to their research.

3.3 CALLING IN BAD ACTORS: THE UK'S NATIONAL SECURITY INVESTMENT ACT 2021

Turning now to the UK's NSI Act, this piece of legislation – which came into force on 4 January 2022 – ties both inbound and outbound foreign direct investment (FDI) to concerns around national security. Entities that would gain control of either a 'qualifying entity' or 'qualifying asset' are required to notify the UK Secretary of State prior to gaining control by giving a 'mandatory notice'[77] or, as part of due diligence, seek the Secretary's consideration of the transaction by issuing a 'voluntary notice'.[78] The Secretary is permitted 30 days to consider such notices, before concluding that either no action will be taken, or that the transaction will be 'called-in' for further review.[79] Qualifying entities or assets differ slightly in that:

(i) A qualifying entity includes any natural person, corporation, partnership, not-for-profit or other legal entity, if they 'carry on an activity' as set out in the Schedules of the Regulations.[80]

(ii) A qualifying asset includes 'land, tangible, moveable property, and ideas, information or techniques which have industrial, commercial or other economic value ("intellectual property")' and 'trade secrets, databases, source code, algorithms, formulae, designs … [and] software'.[81]

Call-ins can also be exercised by the Secretary at any time where either 'a trigger event has taken place in relation to a qualifying entity or qualifying asset' or 'arrangements are in progress or contemplation which, if carried into effect, will result in a trigger event taking place in relation to a qualifying entity or qualifying asset', and the relevant trigger event 'may give rise to a risk to national security'.[82] According to the Secretary's statement on the use of the call-in power – made under section 3 of the NSI Act[83] – call-ins are 'not a system for screening all acquisitions in the economy' and intended to operate in relation to only a 'small number of investments that could be harmful to national security, whilst leaving the vast majority of deals unaffected'.[84] Principal acquisitions that threaten UK economic security are those that 'may lead to disruption, erosion or degradation to critical national infrastructure', 'present risks to governmental and defence assets', 'undermine the UK's military, intelligence or security capabilities' or permit foreign actors to build their own such capabilities.[85]

Irrespective of the exercise of a call-in, the NSI Act imposes significant barriers to investment that does not conform with its terms. Where an entity moves to acquire any entity or asset that would ordinarily require consideration under the NSI Act, they not only commit a criminal

77 NSI Act, ss 14(1) and (3).

78 ibid s 18(2).

79 ibid ss 14(8)(b)(i)–(ii) and 18(8)(b)(i)–(ii).

80 ibid s 6(2); National Security and Investment Act 2021 (Notifiable Acquisition) (Specification of Qualifying Entities) Regulations 2021 (UK) (NSI Regulations), schs 1–17.

81 NSI Act, ss 7(2) (but subject to s 7(3)) and 8(2)–8(8). See also Cabinet Office, 'National Security and Investment Act: Guidance for the Higher Education and Research-Intensive Sectors' (21 May 2024) <www.gov.uk/government/publications/national-security-and-investment-act-guidance-for-the-higher-education-and-research-intensive-sectors/national-security-and-investment-act-guidance-for-the-higher-education-and-research-intensive-sectors> accessed 28 March 2025.

82 NSI Act, s 1(1).

83 ibid s 3; Cabinet Office, 'National Security and Investment Act 2021: Statement for the purposes of section 3' (21 May 2024) <www.gov.uk/government/publications/national-security-and-investment-statement-about-exercise-of-the-call-in-power/national-security-and-investment-act-2021-statement-for-the-purposes-of-section-3--2> accessed 28 March 2025.

84 Cabinet Office, 'National Security and Investment Act: Guidance for the Higher Education and Research-Intensive Sectors' (n 82) [5] and [8].

85 ibid [11]–[13].

DOI: 10.36633/ulr.1178

offence but also any contract or act in furtherance of the acquisition is annulled by law.[86] The Secretary may also issue various orders if he or she is satisfied a risk to national security 'has arisen or would arise',[87] which can compel both positive and negative actions including orders of divestment of some part of the acquiring entity or cancellation of the transaction.[88] The terms, scope and breadth of the NSI Act is considered a critical aspect of UK research security; firstly because universities have been overwhelmingly targeted by call-in notices[89] and secondly because the NSI Act:

> a.) permits the Executive to examine what are ordinarily opaque research activities by universities that may have national security implications, and b.) grants the Executive power to interfere in ordinarily lawful research collaborations if the Executive concludes such collaborations pose a threat to national security.[90]

In this manner, the NSI Act is largely concerned with identifying aspects of 'foreign ownership, control or influence' (FOCI), a US concept traditionally applied to defence contracting and the protection of classified information.[91] Any entity 'under FOCI' could risk access to classified information or contract because a foreign interest could 'decide or direct … the entity's management or operations', or alternately a foreign government could exercise some power over the entity, either directly (ie, contractual means) or indirectly (ie, by appointment to the governing board).[92] In both cases, the independence and autonomy of the contractor is, or could be, compromised by a foreign actor.

4 SYNTHESIS: WHERE DOES THE EU GO FROM HERE?

Considering these two case studies, one can readily identify the fallacy identified by Shultz, who infamously suggested that the use of these kinds of sanctions exemplified 'light switch diplomacy',[93] ie, geopolitical actors become classified as either 'good' or 'bad', and the light switch of their economic development and support is switched on or off accordingly. Indeed, one of the principal challenges inherent in the above case studies is that they typify the use of 'negative' economic security controls – penalties, sanctions or pecuniary punishments designed to coerce foreign actors to conduct themselves in a manner conducive to the imposing state. Problematically, these approaches to research security tend to ignore 'positive' economic security measures, such as non-discriminatory treatment, favoured partner status, tariff reductions or R&D/investment incentives.[94] Negative economic security controls can also result in the creation or exacerbation of security externalities, meaning that their attempted linkage to matters of 'high politics' and the security of the state can in fact backfire, weakening or threatening the security of the imposing state.[95] This was recognised by the League of European Research Universities (LERU) and Central European Universities (CE7) in October 2024 through the publication of their joint statement 'Improving research security in European

86 NSI Act, ss 13(1)–(3) and 32(1)–(2).

87 ibid ss 25(1), 25(2) and 26(1).

88 ibid ss 25(4) and 26(5).

89 Cabinet Office, 'Report on the National Security and Investment Act 2021 (Notifiable Acquisition) (Specification of Qualifying Entities) Regulations 2021' (December 2024) <https://assets.publishing.service.gov.uk/media/676403314e2d5e9c0bde9bad/Report_on_the_National_Security_and_Investment_Act_2021__Notifiable_Acquisition___Specification_of_Qualifying_Entities__Regulations_2021.pdf> accessed 28 March 2025.

90 Walker-Munro, 'National Security, Foreign Investment & Research Security' (n 21) 174.

91 For example, see the US National Industrial Security Program Operating Manual (NISPOM) 32 CFR 117; Melvin Rishe, 'Foreign Ownership, Control, or Influence: The Implications for United States Companies Performing Defense Contracts' (1990) 20(2) Public Contract Law Journal 143.

92 32 CFR § 117.1(a)(1).

93 Gary Clyde Hufbauer and Euijin Jung, 'What's New in Economic Sanctions?' (2020) 130 European Economic Review 103572.

94 Nanyoung Kwon, 'A Study on Japan's Economic Security Promotion Act from the Perspective of Economic Statecraft' (Master's Thesis, Seoul National University, February 2024) 13.

95 Steve Chan and A Cooper Drury, *Sanctions as Economic Statecraft: Theory and Practice* (St Martin's Press 2000).

DOI: 10.36633/ulr.1178

universities'.[96] In that joint statement it was recognised that approaches across the EU needed to be consistent, joined-up and properly funded, without distracting from the fundamental objectives of university research.

From the EU's perspective, there are also challenges with implementing regulatory regimes, both generally in an economic sense but in relation to research security specifically, especially in a geopolitically charged economic security environment.[97] This is the case for several reasons exposed in the literature. Firstly, the EU itself is premised on the notion of openness in which every foundational document – from the Treaty of Paris to the Treaty of Lisbon – has articulated freedoms of trade, investment and finance as well as concepts like the Single Market that bely economic autonomy.[98] The result is that economic security measures can result in contraventions or conflicts with the loosely 'constitutional' documents that underpin the EU's legislative and executive mandate. Even so, the level and meaning of openness differs depending on the parties to the economic or research agreement in question. For example, 'openness' in the context of the Single Market applies only within and between EU Member States, continuing to treat non-EU countries as 'outsiders'.[99] Research between 'insiders' of the EU is obviously preferred.[100] Further, scholarly critiques have long suggested that 'loosening up the Treaty objectives to encourage contestation about the Union's objectives and direction' is necessary because the EU is functionally pre-empted from proper economic autonomy by its Treaty framework.[101] Put another way, the choice Member States have to pursue *how* they wish to achieve a normative economic goal (such as securing technologies of economic value) will be constrained by sheer virtue of their membership in the Union.[102]

Secondly, despite the apparent unity of the overarching legislature, the EU is still a polity that comprises numerous nation-states with diverse agendas, political aims and security priorities, and who may fundamentally disagree on economic security outcomes and aims.[103] Security and foreign affairs policy is a particularly contested domain where – even despite a consistent theme of 'otherness' in approaching non-EU countries has existed since the 1992 Treaty of Maastricht – the EU's approach to security and foreign policy remains paradoxical. States want to ensure (as a collective bloc and common market) they are both physically safe and economically secure from outside interference; however, they also want to retain autonomy to derive nationalistic benefits from unrestricted trade, diplomacy and exchange.[104] Thus, the setting of geopolitical standards and matters of security may be cast at an institutional level but still involve practical devolution to each nation-State, meaning the European Parliament and Council of the EU can be challenged translating economic security policy into actions (especially compared to unilaterally hegemonic states like the US and the PRC).[105]

Thirdly, the EU remains significantly reliant, both in terms of financing and materiel support, on the US and other Western allies for the achievement of its local and international security

96 LERU, 'Improving Research Security in European Universities' (14 October 2024) <www.leru.org/news/improving-research-security-in-european-universities> accessed 14 April 2025.

97 See generally Chad Brown, 'Trade policy, Industrial Policy, and the Economic Security of the European Union' in Jean Pisani-Ferry, Beatrice Weder di Mauro and Jeromin Zettelmeyer (eds), *Paris Report 2: Europe's Economic Security* (CEPR Press 2024) 135–80 <https://cepr.org/publications/books-and-reports/paris-report-2-europes-economic-security> accessed 14 April 2025.

98 Finn Laursen, 'The Founding Treaties of the European Union and Their Reform' in William R Thompson (ed), *Oxford Research Encyclopedia of Politics* (Oxford Research Encyclopedias 2016).

99 Thomas Prosser, 'Insiders and Outsiders on a European Scale' (2017) 23(2) European Journal of Industrial Relations 135.

100 Marina Cino Pagliarello, 'Higher Education in the Single Market Between (Trans) National Integration and Supranationalisation: Exploring the European Universities Initiative' (2022) 44(1) Journal of European Integration 149.

101 Marija Bartl, 'The Way We Do Europe: Subsidiarity and the Substantive Democratic Deficit' (2015) 21(1) European Law Journal 23; Mark Dawson and Floris de Witte, 'From Balance to Conflict: A New Constitution for the EU' (2016) 22(2) European Law Journal 204.

102 Gareth Davies, 'Democracy and Legitimacy in the Shadow of Purposive Competence' (2015) 21(1) European Law Journal 2.

103 Steinberg and Wolff (n 4) 186.

104 Ramses A Wessel, 'Integration and Constitutionalisation in EU Foreign and Security Policy' in Robert Schütze (ed), *Globalisation and Governance: International Problems, European Solutions* (CUP 2018) 339–75.

105 Mark Leonard and others, 'Securing Europe's Economic Sovereignty' (2019) 61(5) Survival 75–98, DOI:10.1080/00396338.2019.1662148.

priorities,[106] ie, resisting military advances from Russia. At the same time, Russia forms valuable investment and trading partnerships with EU nations (on energy and high technology respectively), meaning policy responses *need* to be shaped and delivered at the EU level to avoid individual nation-states becoming complicit in Sino-Russian avoidance of broader measures of Western economic statecraft.[107] Concerns of regulatory arbitrage (ie, the movement of transactions away from jurisdictions with high scrutiny to ones of lower scrutiny) are writ large in the management of such foreign relations.

From the perspective of research security, the EU is also itself being challenged. Having established a clear pathway in the Council Recommendation and embedded it inside a broader package of economic security controls, the EU was then blindsided in December 2024 by the adoption of UN General Resolution A/79/416 DR.[108] First proposed by the PRC and supported by much of the Latin American and African Member States, the Resolution '*urges* all Member States, without prejudice to their non-proliferation obligations, to take concrete measures to promote international cooperation on materials, equipment and technology for peaceful purposes, in particular not to maintain any restrictions incompatible with the obligations undertaken'. The language of the resolution is no mistake – it suggests a much more politicised or diplomatic response aiming to counter emerging notions of research security (and tied into economic security) beginning to be implemented across the EU. The December 2024 resolution of the UN therefore seems to be a precisely targeted piece of Chinese diplomatic statecraft, designed to push back on the increasing threat of research security controls to the broader evolution and enhancement of Chinese economic advantage.

So where does the EU go from here? Ironically, the UN resolution provides that succinct response: EU nations need to deepen and mature the linkage between economic dynamics and security dynamics, by focusing their legal and policy measures on protecting economic security as a state interest.

In doing so, there are three areas that EU Member States should consider when putting the Council Recommendation into practice using the research security lens:

(i) Engaging in 'selective fortification', ie, the adoption of the 'small yard, high fence' strategy, by enacting strong legislative controls are enacted around a reasonably small but internationally defensible subset of critical economic activities, technologies and research (such as how the US approached its dominance in the semi-conductor market by enacting the CHIPS and Science Act);[109]

(ii) Ensuring that positive measures are enacted alongside negative interventions tied to or aimed at economic security; and

(iii) Adopting a blended approach of both law and policy, with flexibility to support individual approaches reflective of the unique context of higher education and research institutions.

4.1 SELECTIVE FORTIFICATION OF THE RESEARCH ENTERPRISE

The notion of selective fortification has arisen by scholars examining the previous policy approaches from the establishment of the EU, where views of economic policy were largely divided into camps of 'Atlantic Europe' (collaborative policy, openness by default) or 'Fortress Europe' (nationalist policy, protective of municipal interests). The current literature suggests

106 Hugo Meijer and Stephen G Brooks, 'Illusions of Autonomy: Why Europe Cannot Provide for its Security if the United States Pulls Back' (2021) 45(4) International Security 7.

107 Referring to the PRC as a 'circumvention hub' for Western sanctions against Russia: Tauno Tohk, 'More Than a Systemic Rival: China as a Security Challenge for the EU' (International Centre for Defence and Security Brief, March 2025) 1 <https://icds.ee/en/more-than-a-systemic-rival-china-as-a-security-challenge-for-the-eu/> accessed 12 April 2025.

108 United Nations General Assembly, 'Promoting international cooperation on peaceful uses in the context of international security' (25 October 2024) 79th Session UN Doc A/C.1/79/L.53/Rev.1 <https://documents.un.org/doc/undoc/ltd/n24/317/40/pdf/n2431740.pdf> accessed 12 April 2025.

109 Asif H Qureshi, 'The US Chips and Science Act of 2022: A Self-Interested Indulgence in Foreign Trade and Science or a Model for Future Development?' (2023) 51(1) Syracuse Journal of International Law & Commerce 89. Of course, these nationalistic endeavours can be undone by changes in government – see for example the changes wrought by the second Trump administration: Jeff Tollefson Witze and Max Kozlov, 'Science Under Trump 2.0: The Likely Winners and Losers' (2025) 637 Nature 533.

that such models can no longer survive the modern geopolitical environment.[110] 'Selective fortification' – that is, the 'develop[ment of] targeted instruments and institutional capacities that aim to insulate European firms from new patterns of international competition'[111] – is itself a rebranded version of the 'high fence, small yard' strategy (which focuses on targeted economic interventions rather than sweeping reform[112]). Put another way, research security as economic security should focus on 'identifying and mitigating the security vulnerabilities that accrue from open, globally integrated markets'.[113] This requires EU Member States to embrace the notion of economic dynamics driving security dynamics, and adopting specific and targeted legislation like the US CHIPS and Science Act to both incentivise domestic manufacturing/research, whilst discouraging and penalising foreign actions which threaten that domestic base.

Selective fortification aligns with practical observation of research security practices emerging in the wake of the Council Recommendation. Germany for example has published a Position Paper in response to the *Zeitenwende* (turning point in history),[114] Italy has published a National Action Plan on research security,[115] and Latvia and Estonia have seen the emergence of their security services as valued stakeholders in academic settings.[116] They join well-established research security nation-states in the EU, such as France (which has recognised threats to research security in its Criminal Code since at least 2012[117]) and the Netherlands (where the National Contact Point has long coordinated discussions between academia and the national intelligence body, the AIVD[118]). Scholars in the field have also demanded that policies adopt principles of 'responsible internationalisation', involving a recognition of risk in international collaborations but advocating for heavy-handed governmental interference in only the direst of cases.[119] These principles also recognise and accord with academic autonomy, substantial dips and rises in the sector's homogeneity across the EU, as well as the 'academic norms advocating international exchange, openness, and transparency'.[120] Selective fortification clearly incorporates these principles, invoking many states to engage in a marked 'increase [in] state intervention in the emerging economies, the growth of state-owned enterprises and sovereign wealth funds, and the return of industrial strategy in the West'.[121]

110 Steinberg and Wolff (n 4). See also Catherine Hoeffler, 'Arming Fortress Europe?: Spaces and Instruments of Economic Patriotism in EU Armament Policy' (2023) 11 Politics and Governance 154; Timo Seidl and Luuk Schmitz, 'Moving on to not Fall Behind? Technological Sovereignty and the "Geo-Dirigiste" turn in EU Industrial Policy' (2024) 31(8) Journal of European Public Policy 2147, DOI: 10.1080/13501763.2023.2248204; Floor Doppen, Antonio Calcara and Dirk De Bièvre, 'Balancing Security and Economics: Domestic State-Firm Relations and Investment Screening Mechanisms in Europe' (2024) 31(6) Review of International Political Economy 1637.

111 Scott Lavery, 'Rebuilding the Fortress? Europe in a Changing World Economy' (2023) 31(1) Review of International Political Economy 330, DOI:10.1080/09692290.2023.2211281.

112 Steinberg and Wolff (n 4) 185.

113 Sarah Bauerle Danzman and Sophie Meunier, 'The EU's Geoeconomic Turn: From Policy Laggard to Institutional Innovator' (2024) 62(4) Journal of Common Market Studies 1097, DOI: 10.1111/jcms.13599.

114 See for example Federal Ministry of Education and Research, 'Positionspapier des Bundesministeriums für Bildung und Forschung zur Forschungssicherheit im Lichte der Zeitenwende' [Position paper of the German Federal Ministry of Education and Research on research security considering the Zeitenwende] (Report, 2025) < https://www.bmftr.bund.de/SharedDocs/Downloads/DE/2024/position-paper-research-security.pdf > accessed 1 April 2025.

115 Decode39, 'How Italy Plans to Tackle Foreign Interference in Research' (7 November 2024) <https://decode39.com/9677/how-italy-plans-to-tackle-foreign-interference-in-research/> accessed 14 January 2026.

116 Solvita Denisa-Liepniece and Dmitri Teperik, 'Enhancing Research Security in Latvia and Estonia: Potentials for Mitigating China-related Risks in Academic Collaboration' (Sandia National Laboratories March 2025).

117 Secrétariat général de la défense et de la sécurité nationale, 'Protéger le potentiel scientifique et technique de la nation' [Protecting the nation's scientific and technical potential] (2025) <www.sgdsn.gouv.fr/nos-missions/proteger/proteger-le-potentiel-scientifique-et-technique-de-la-nation> accessed 1 April 2025.

118 Government of the Netherlands, 'National Contact Point for Knowledge Security' (2025) <https://english.loketkennisveiligheid.nl/> accessed 1 April 2025.

119 Tommy Shih, 'We Cannot Adopt a Blanket Approach to Research Security' (*University World News*, 2 October 2024) <www.universityworldnews.com/post.php?story=20241001140316637> accessed 14 January 2026; Hans de Wit and Chris Glass, '"Responsible Internationalisation": How Responsible is it?' (*University World News*, 8 January 2025) <www.universityworldnews.com/post.php?story=20250108083213848> accessed 14 January 2026.

120 Andrea Braun Střelcová, 'Guardians of Knowledge: Why the EU's New Research Security Approach Puts European Universities in a Bind' (*China Observers EU*, 7 March 2024) <https://chinaobservers.eu/guardians-of-knowledge-why-the-eus-new-research-security-approach-puts-european-universities-in-a-bind/> accessed 4 April 2025.

121 Lavery (n 112) 332.

DOI: 10.36633/ulr.1178

Thus, each of the Member States could enact – in consultation with their domestic higher education providers and the Commission – domestic protections reminiscent of the US CHIPS and Science Act and protect domestic manufacturing and research bases. Obviously, this would require Member States of the EU to have a deep understanding of what areas of technology they specialise or lead the market in, or at least wish to develop a stronger sovereign capability in. Research into technologies or concepts outside of those considered 'critical' to the economy of the relevant Member State should be regulated lightly (if at all). Not only would this meet the overarching language of the UN General Resolution A/79/416 DR but is also defensible as an exercise of the sovereign interests of the relevant Member State. Alternately, such Member States could use existing or new laws (or economic value instruments) to disincentivise their domestic research and innovation markets from foreign inputs – noting that this not only has significant economic implications that would need to be accounted for but may also put individual Member States out of lockstep with the wider EU.

4.2 BALANCING POSITIVE AND NEGATIVE INTERVENTIONS

Provisions of economic security across the EU – including those enacted for the purposes of research security – have also largely been focused on banning/limiting potential risky collaborations, and thus been devoid of *positive* economic security measures.[122] For example, Hahn and Reinhold write extensively on the EU's 'promoting', 'protecting' and 'partnering' measures under economic security declarations, to consider whether those are compliant with broader international trade laws under the auspices of the World Trade Organization.[123] The point here is not to consider whether these measures are *sine qua non* compliant with international obligations generally or in a particular case – more to observe that punitive measures in the EU economy security strategy ought to be combined with incentives.

For example, the two case studies examined above – the STRAC of Canada and NSI Act of the UK respectively – do not of themselves contribute positive measures in an economic security sense. But these policies *do* exist in a broader legal and policy network that can be marshalled for the purposes of regulating national security threats to the research enterprise. Canada administers around CAD$450 million in the Research Support Fund to help domestic institutions with programmes to 'secure research from threats',[124] whilst the UK operates the Research Collaborative Advice Team, a government agency designed to provide advice to researchers and institutions on methods for managing their research security risks.[125] Yet even these regulatory factors may still incorporate further negative measures:

> Other 'strands' in that regulatory network will include migration or visa approval processes, export controls, criminal laws relating to national security … and contractual conditions which may applying to specific types of research funding or funding more generally (i.e., requiring document or information security, security clearances for researchers, etc.).[126]

To be truly viable, economic security measures that apply to research security should feature *positive* counterparts – tax or investment incentives, favoured trading status and tariff reductions. Returning to our earlier example where economic dynamics have driven security dynamics, one tranche of the CHIPS and Science Act of the US[127] provides US$52.7 billion in financial incentives for domestic production of semiconductors under the CHIPS Program Office (whilst simultaneously limiting overseas supply of semiconductors to foreign nations) as well as supplying funding to the National Science Foundation and US universities to strengthen

122 Kwon (n 95).

123 Michael Hahn and Philipp Reinhold, 'International Economic Relations as a Risk: The EU's Economic Security Strategy and the World Trading System' (2025) 20(2) Global Trade and Customs Journal 110.

124 Government of Canada, 'Research Support Fund' <www.rsf-fsr.gc.ca/home-accueil-eng.aspx> accessed 2 April 2025.

125 UK Government, 'Research Collaboration Advice Team' <www.gov.uk/government/organisations/research-collaboration-advice-team> accessed 2 April 2025.

126 Walker-Munro, 'National Security, Foreign Investment & Research Security' (n 21) 174.

127 Pub L 117–67, at 136 Stat 1366.

DOI: 10.36633/ulr.1178

research security.[128] EU Member States would do well to incentivise the pursuit of research security measures with financial benefits (recalling that LERU and CE7 called for exactly this in late 2024).

Aspects of the AUKUS Agreement between the US, UK and Australia serves as yet another exemplar of positive incentivisation of economic (and research) security – Australia and the UK became members of a licence-free environment from some of the more draconian provisions of the US International Traffic in Arms Regulations.[129] The excision of both Australian and UK environments serves as a powerful incentive for defence researchers, innovators and contractors to supply their knowledge and materiel in ways that support the broader achievement of US foreign and industrial policy. The EU Member States could also learn from the experiences of the US in forging these crucial pieces of legislative enablement of their domestic capabilities, by examining the export control regimes (especially as they apply to university research) for ways to exempt 'trusted' partners from permit obligations and thus incentivising the sharing of research with partners in ways that achieve their national security objectives.[130]

4.3 BLENDING HARD AND SOFT LAW: WHAT ROLE FOR FLEXIBILITY?

Where economic security measures are already written into the legislative restrictions ('hard law'), Member States should also be contemplating whether such measures have articulated circumstances of flexibility or exemption to permit each institution to set some aspect of their research security policy settings ('soft law'). Economic security from both the position of the EU and its individual Member States will increasingly come to rely on 'more common and integrated policy action', and this in turn requires that 'the need to pool more sovereignty to achieve economic security needs to be recognised'.[131] This is in fact one of the significant benefits of the EU legislative environment: each Member State must consider for themselves the law and policy settings applicable within its jurisdiction (subject to compliance with other EU or transnational legal instruments or treaties). On the other hand, Member States also need to cleave to the principles established *inter alia* by the European Parliament and Council of the EU, to ensure that no gaps in regulatory or legislative coverage can arise which might permit regulatory arbitrage – that is, the avoidance of onerous or restrictive regulation in one state by basing their operations in another, to the detriment of the wider market.[132]

The UK NSI Act outlined earlier is a positive exemplar for the blend of hard and soft law. For example, the rigid provisions of the NSI Act are supported by a 'section 3' statement issued by the Secretary of State.[133] Whilst a section 3 statement is a policy document, it is both required by law and must be informed by both national and international policy considerations. The Secretary of State may seek to amend a section 3 statement at any time to change (for example) the scope of 'areas of the economy' to which the call-in power might relate, the purposes for which the Secretary of State might exercise the call-in power and the diverse factors which the Secretary has committed to taking into account when considering whether to exercise a call-in. In doing so, the NSI Act and accompanying Secretarial statement impose two forms of economic security regulation. The first is a 'gatekeeping function' that invokes a security interest to establish a clear threshold for State intervention, ie, research *requiring* protection

128 Victoria Cooper, 'Explainer: The CHIPS and Science Act 2022' (*United States Studies Centre*, 11 August 2022) <www.ussc.edu.au/explainer-the-chips-and-science-act-2022> accessed 4 April 2025.

129 William Greenwalt and Tom Corben, 'AUKUS Enablers? Assessing Defence Trade Control Reforms in Australia and the United States' (United States Studies Centre Report, 21 August 2024) <www.ussc.edu.au/aukus-assessing-defence-trade-control-reforms-in-australia-and-the-united-states> accessed 4 April 2025.

130 Stalenhoef, Kanetake and van der Wende (n 55).

131 Fabian Zuleeg, 'Economic Security: A New EU Paradigm?' (European Policy Centre Discussion, Paper 8 June 2023) 7.

132 Lars Gjesvik and Johann Ole Willers, 'Beyond Control? The Political Economy of Private Interception, Intrusion, and Surveillance Markets' (2024) 31(6) Review of International Political Economy 1840.

133 NSI Act, s 3; Cabinet Office, 'National Security and Investment Act 2021: Statement for the purposes of section 3 – 2021 version' (21 May 2024) <www.gov.uk/government/publications/national-security-and-investment-statement-about-exercise-of-the-call-in-power/national-security-and-investment-act-2021-statement-for-the-purposes-of-section-3> accessed 4 April 2025.

DOI: 10.36633/ulr.1178

from foreign manipulation or interference will incur economic security consequences.[134] A second function of the NSI Act with relevance to economic security is the provision of 'virtue signals' to the market. Transactions which fall outside the NSI Act or Secretarial statement are not considered relevant for economic or national security purposes and can be used to signal or communicate confidence that such transactions are viewed as a low security priority.[135] Both the threshold for intervention and the virtue signals to the market are entirely scalable and changeable, and may be amended by the Secretary of State to take account of changes in the prevailing market or shifting geopolitical conditions.

5 CONCLUSION

This paper has examined the field at the intersection of economic security and research security, where I suggest that economic dynamics have driven security dynamics, especially in the emergence of research security across the EU. As the full force of the Council Recommendation comes into conflict with the UN General Assembly's resolution on 'concrete measures', Member States will need to regulate the national security risks inherent in different forms of research in more nuanced and mature ways. It is important to recall that, whilst both universities and governments have responsibilities and obligations in this space, those same responsibilities and obligations inevitably overlap and cause friction. Emerging research is already showing that to continue international collaborations in contested or volatile geopolitical settings will require universities to:

> develop guidelines that consider the increasingly multipolar research landscape amid geopolitical tensions. The research sector's inability to handle matters related to data security, multiple affiliations, or ethics dumping can mean that national political forces are likely to use additional compliance.[136]

Simultaneously, the EU is likely to continue its clarion call on research institutions across the Union to safeguard their national research enterprises. The European Commission will no doubt continue to claim competitiveness and sovereign capability is at the centre of its legislative agenda, yet this continues to require tact and nuance in handling 'a process teeming with dilemmas related to autonomy, implementation, and coordination'.[137] In many respects, economic security measures implemented today will still take several years to achieve their full impact (even if early signs are positive that '[e]fforts to target foreign interference have already spurred better knowledge-sharing and coordination inside the EU'[138]).

Nor have all strategies of economic securitisation been successful, and Member States need to remain live to the significant challenges presented by the higher education system. The Dutch government has at the time of writing opened consultation into the Knowledge Screening Act,[139] a piece of legislation that would obligate the 68 Dutch knowledge institutions (including scientific institutes and universities of applied sciences) to conduct background screening on foreign-based researchers, to refuse collaborations with those who pose too high a risk. However, the scheme has been widely pilloried by the academic community.[140] Further, the

134 J Benton Heath, 'The New National Security Challenge to the Economic Order' (2020) 129 The Yale Law Journal 1020; citing Oren Gross and Fionnuala Ní Aoláin, *Law in Times of Crisis: Emergency Powers in Theory and Practice* (CUP 2006) 283.

135 ibid.

136 Shih, Chubb & Cooney-O'Donoghue (n 63) 1353.

137 Střelcová (n 121).

138 ibid.

139 Overheid.nl, 'Internetconsultatie' [Consultation on the Knowledge Screening Act] <www.internetconsultatie.nl/screeningkennisveiligheid/b1> accessed 12 December 2025.

140 Annabelle de Bruin, 'New Knowledge Security Screening is Counterproductive' (*Delta*, 30 May 2023) <https://delta.tudelft.nl/en/article/new-knowledge-security-screening-counterproductive> accessed 12 April 2025; Jos Wassink, 'A Knowledge Security Law? Then Screen Everyone' (*Delta*, 9 June 2023) <https://delta.tudelft.nl/en/article/knowledge-security-law-then-screen-everyone> accessed 12 April 2025; KNAW, 'Royal Netherlands Academy of Arts and Sciences (KNAW) Warns Against Proposed Knowledge Security Act' (Media release, 10 October 2023) <www.knaw.nl/en/news/royal-netherlands-academy-arts-and-sciences-knaw-warns-against-proposed-knowledge-security-act> accessed 12 April 2025; Ben Upton, 'Dutch Research Security Rules "Virtually Impossible to Implement"' (*Times Higher Education*, 18 October 2023) <www.timeshighereducation.com/news/dutch-research-security-rules-virtually-impossible-implement> accessed 12 April 2025; Hanne Cokelaere, 'Dutch Government Plans to Screen Scientists for National Security Risks' (*POLITICO*, 7 April 2025) <www.politico.eu/article/dutch-government-scientists-tech-national-security-espionage/> accessed 12 April 2025.

DOI: 10.36633/ulr.1178

logistics of the scheme may prove its downfall: public reporting on Dutch research security suggests hundreds of academic collaborations have already been refused – with up to 30% of proposals receiving negative advice[141] – and the Knowledge Screening Act anticipated to apply to 8,000 such collaborations every year.[142] On those estimates alone, nearly 2,400 researchers a year will be barred from collaboration in the Netherlands.

More broadly, the global notion of research security as an academic discipline is almost entirely under-theorised. What little has been written about the subject usually prioritises the notion of academic freedom rather than identifying its boundaries and engaging with co-design to guide institutional governance approaches that appropriately manage risk.[143] At the same time, preventing researchers or institutions from seeking funding (or banning those that cannot maintain their compliance) on the basis of economic security concerns could just as easily exacerbate problems, not solve them. Empirical studies on the influences for university funding are rare, but one such study in the US showed that temporary shocks or cuts in federal funding results in universities actively prioritising higher-risk sources of private funding, whether from foreign governments or corporations.[144] Current moves by the Trump administration to defund research containing diversity, equity and inclusion terms – even for projects funded outside the US – have further reminded the global higher education sector of the danger of not diversifying research income streams.[145]

Finally, the ongoing trend of securitisation of higher education (including their contributions to the economy) will require ongoing, committed and nuanced conversations across both EU Member States and the broader EU leadership. Imposing regulatory or legal restrictions will not only hamper European institutions from competing on the global market but may also impede domestic scientific capability or even constitute interferences with international obligations (which may create concomitant reputational and financial cost). Economic security controls need to be paired with incentives – 'sticks' need to be properly counterbalanced with 'carrots'. Implicit in that conversation needs to be a proper accounting for who assesses, deals with and then carries the risk associated with a certain collaboration. Governments cannot be everywhere or expected to do everything, but they do possess skills, resources and sources that universities cannot match. In the words of Professor Rory Medcalf – the head of Australia's National Security College – 'when it comes to the security landscape, the gap between what government knows and what it says in public must become narrower, not widen'.[146] Accordingly, the EU's best role in economic security is as a promoter of shared needs, 'to unite actors with divergent long-term interests behind an intermediate agenda for policy change'.[147] By promoting and partnering (as well as penalising) conduct critical to ensuring economic security, the EU can ensure the research institutions of its Member States recognise the benefits of protective research security, rather than yet another security hurdle that stifles their creativity, autonomy and innovative contributions to society as a whole.

141 Bas de Vries and Milo Hornstra, 'Universiteiten wijzen honderden buitenlandse onderzoekers en samenwerkingen af' [Universities reject hundreds of foreign researchers and collaborations] (*NOS News*, 24 March 2025) <https://nos.nl/artikel/2560912-universiteiten-wijzen-honderden-buitenlandse-onderzoekers-en-samenwerkingen-af> accessed 4 April 2025.

142 Alexander Martin, 'To Tackle Espionage, Dutch Government Plans to Screen University Students and Researchers' (*The Record*, 8 April 2025) <https://therecord.media/netherlands-plan-vetting-researchers-students-espionage> accessed 15 April 2025.

143 William G Tierney, 'The Idea of Academic Freedom and Its Implications for Teaching and Learning' in N V Varghese and Sayantan Mandal (eds), *Teaching Learning and New Technologies in Higher Education* (Springer 2020) 17–28; Ross McLennan, 'Balancing Collaboration and Security: A High-Wire Challenge for Australia's Universities' (Speech to the Australian Institute of International Affairs, 8 June 2021) <https://www.youtube.com/watch?v=avgzy496o94> accessed 14 January 2026; Kirsten Lyons, 'Universities' Relevance Hinges on Academic Freedom' (*The Conversation*, 2 June 2021) <https://theconversation.com/universities-relevance-hinges-on-academic-freedom-160346> accessed 4 April 2025.

144 Tania Babina and others, 'Cutting the Innovation Engine: How Federal Funding Shocks Affect University Patenting, Entrepreneurship, and Publications' (2023) 138(2) The Quarterly Journal of Economics 895, DOI:10.1093/qje/qjac046.

145 Brendan Walker-Munro, 'Trump is Surveying Australian Academics About Gender Diversity and China – What Does This Mean for Unis and Their Research?' (*The Conversation*, 17 March 2025) <https://theconversation.com/trump-is-surveying-australian-academics-about-gender-diversity-and-china-what-does-this-mean-for-unis-and-their-research-252282> accessed 4 April 2025.

146 Rory Medcalf, 'Why We Need a Different Conversation About National Security' (Securing Our Future Conference Keynote, Canberra, 8 April 2024).

147 Seidl and Schmitz (n 111) 2150.

COMPETING INTERESTS

I have consulted for the Australian Strategic Policy Institute and the Office of the Independent National Security Legislation Monitor.

AUTHOR AFFILIATIONS

Dr Brendan Walker-Munro orcid.org/0000-0001-5484-1145
Associate Professor, Faculty of Business, Law & The Arts, Southern Cross University, Coolangatta Queensland 4225, AU

TO CITE THIS ARTICLE:
Brendan Walker-Munro, 'Economic Security and Higher Education: The Rise of Research Securitisation' (2026) 22(1) Utrecht Law Review 28–46. DOI: https://doi.org/10.36633/ulr.1178

Published: 19 May 2026

Utrecht Law Review is a peer-reviewed open access journal published by Utrecht University School of Law.