Research Papers

October 2025

UK National Security Advantage from Disruptive Technologies

Understanding UK Assets, Needs and Dependencies

Pia Hüsch and Natasha Buckley

RUSI

Disclaimer

The content in this publication is provided for general information only. It is not intended to amount to advice on which you should rely. You must obtain professional or specialist advice before taking, or refraining from, any action based on the content in this publication.

The views expressed in this publication are those of the authors, and do not necessarily reflect the views of RUSI or any other institution.

To the fullest extent permitted by law, RUSI shall not be liable for any loss or damage of any nature whether foreseeable or unforeseeable (including, without limitation, in defamation) arising from or in connection with the reproduction, reliance on or use of the publication or any of the information contained in the publication by you or any third party. References to RUSI include its directors and employees.

RUSI Research Papers, October 2025

ISSN 2977-960X

Publications Team

Editorial

Director of Publications: Alice Trouncer

Managing Editor: Sarah Hudson

Assistant Editor: Sophie Boulter

Design

Graphic Designer: Zenab Hotelwala

Research Editorial

Head of Research Governance and Editorial: Elias Forneris

Cover image: Created with Canva AI

Get in touch

www.rusi.org

enquiries@rusi.org

+44 (0)207 747 2600

The Royal United Services Institute for Defence and Security

61 Whitehall, London

SW1A 2ET

United Kingdom

Follow us on

Contents

Acronyms and Abbreviations

AISI – AI Security Institute

ARIA – Advanced Research and Innovation Agency

ARPA – Advanced Research Projects Agency

DARPA – Defense Advanced Research Projects Agency

DASA – Defence and Security Accelerator

DBT – Department for Business and Trade

DSIT – Department of Science, Innovation and Technology

EDI – equality, diversity and inclusion

FCDO – Foreign, Commonwealth & Development Office

IP – intellectual property

IRR – Integrated Review Refresh

ISO – International Organization for Standardization

ITU – International Telecommunications Union

MoD – Ministry of Defence

NCA – National Crime Agency

NCSC – National Cyber Security Centre

NIF – NATO Innovation Fund

NQCC – National Quantum Computing Centre

NSIA – National Security and Investment Act

NSTIx – National Security and Innovation Exchange

NSSIF – National Security Strategic Investment Fund

PPP – public–private partnership

RCAT – Research Collaboration Advice Team

R&D – research and development

REF – Research Excellence Framework

RIO – Regulatory Innovation Office

SBIR – Small Business Innovation Research

SME – small and medium-sized enterprise

STTR – Small Business Technology Transfer

SIN – Science and Innovation Network

STN – Science and Technology Network

S&T – science and technology

STEM – science, technology, engineering and maths

ST&I – science, technology and innovation

UKIC – UK Intelligence Community

VC – venture capital

Acknowledgements

The authors are grateful to the UK government for providing funding for this paper and for their support throughout the research process. A great deal of thanks must go to the team that helped to guide and shape the paper. Conrad Prince, Hugh Oberlander, James Sullivan, Elias Forneris and Sophie Boulter all provided valuable support and editing. Thank you to Zenab Hotelwala for the visuals in this paper. Thanks also go to the peer reviewers, as well as to the various individuals from the national security community, wider UK government and the science, tech and innovation ecosystem who provided insightful feedback on different stages of the paper and the recommendations. A final thank you goes to all the participants in this research, particularly individuals who work in the national security community and challenged themselves to break siloes and silence and spoke with us about their work. We appreciate everyone's time and input.

Executive Summary

- Countries are accelerating efforts, including in a national security context, to gain an advantage from the opportunities that disruptive technologies present. The interconnectivity of science, technology and innovation (ST&I) ecosystems has taken technology competition to an international level.
- The UK government has set an ambitious tech agenda over the past five to seven years. It has repeatedly increased spending to improve its reputation for the R&D, commercialisation and adoption of technologies. Yet, the global race for technological supremacy primarily takes place between the US and China. Against this backdrop, how can the UK navigate this international competition for technological advantage to its national benefit, both in terms of economic growth and national security?
- Over a 12-month period, RUSI explored the UK's pursuit of strategic advantage for national security in disruptive technologies. RUSI interviewed 57 research participants. These interviewees work at the intersection of technology and national security and were drawn from the broader UK innovation ecosystem. The findings of this paper identify a series of existing assets that have put the UK in a strong position and highlight some gaps and risks for UK policymakers to consider.
- Participants revealed that the UK government's ambitions for disruptive technologies for national security purposes remain largely undefined. While UK policy language often remains aspirational, little detail is typically provided to set a strategic direction, such as identifying specific priority areas or use cases. Participants had varied understandings of the exact relationship between the objectives of 'securing strategic advantage' and securing UK economic growth.
- To enable a strategic approach to UK ST&I policy, participants called for a cultural shift on transparency and information sharing within the national security community.
- UK assets, gaps and risks remain poorly understood by members of the UK ST&I ecosystem, even though they are a prerequisite to a strategic approach to technology policy. The paper identifies several non-exhaustive factors that shape the UK's position. These include key assets such as the academic sector and tech diplomacy, and limitations such as the absence of large technology companies and sufficient venture capital (VC) to scale up the otherwise strong UK start-up ecosystem.

- This research demonstrates that there is still a limited comparative international understanding of best practice in technology policy. Comparisons between the UK's economic resources and political system, and those of other countries (for example, the US and China) are often imperfect. Meaningful lessons from the policy interventions of other countries remain rare and require deeper research.
- The UK brings strong assets to the global race for technology, but these must not be taken for granted. The historical strength of the UK academic community is at risk due to financial constraints on universities, a lack of domestic students studying ST&I subjects and the high cost of living in the UK. Participants also identified the need for greater trust between the national security community and UK-based academics to balance the desire for international collaboration with national security concerns.
- The UK has an impressive start-up environment and has launched initiatives, such as funding for risk-taking research. However, risk appetite among policymakers, civil servants and investors remains low. Start-ups and individual talents are often attracted to locations with larger VC funding than the UK or cannot attract enough funding to scale. They therefore become victim to the 'valley of death', without access to further UK (or trusted international) funding.
- UK public–private partnerships benefit from the UK government acting as a first investor or the 'customer of first resort' for technology products. Research participants revealed that this model successfully leads to greater strategic direction from the national security community and attracts significant subsequent private investment. However, much of this relies on personal relationships, individual networks and continued government funding.
- The paper makes detailed policy recommendations linked to three overarching priority areas:
    - Maintaining and investing in existing assets – such as the UK's leading academic sector, tech diplomacy initiatives and standard-setting work – while attracting top talent.
    - Overcoming hurdles for transparency and collaboration between the UK national security community and the wider technology ecosystem.
    - Scaling up early success for wider economic, strategic and societal benefits.

Introduction

Countries are accelerating efforts to capitalise on the opportunities – including those in a national security context – that are presented by 'disruptive technologies' such as AI and quantum technologies. Countries aim to provide greater funding for research, build supportive infrastructure, position themselves as close allies of the private sector and attract global talent to work at their universities, start-ups and technology companies.[1]

Gains in national advantage in technology are relative to progress made by – and reliance on – other countries. Advancement in national innovation is merely one measure of progress. A fuller assessment is needed as the interconnectivity and complexities of science, technology and innovation (ST&I) ecosystems and supply chains make technology competition inherently international. The need for cooperation on R&D, the role of multinational corporations in advancing civilian and dual-use technologies, and intertwined global supply chains require an international approach. The growing need for countries to back technological innovation, such as AI technologies, through costly infrastructure projects further necessitates joint funding from multiple stakeholders.

Strategic competition for technological supremacy primarily occurs between the US and China. The US has long demonstrated its global technology power and has been world-leading in the development and implementation of many technologies. However, China's advancing technological capabilities – especially in fields such as AI – increase pressure on the US and its allies to ramp up their R&D programmes, de-risk supply chains and include ST&I in their foreign and national security policies.

1. See, for example, European Commission, 'Commission Launches Ambitious Strategy to Make Europe a Startup and Scaleup Powerhouse', <https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1350>, accessed 15 September 2025; Cliff Saran, 'London Tech Week: More Funding, Fellowships and Skills', ComputerWeekly, <https://www.computerweekly.com/news/366625836/London-Tech-Week-More-funding-fellowships-and-skills>, accessed 15 September 2025; Clare Duffy, 'Trump Announces a $500 Billion AI Infrastructure Investment in the US', CNN, 21 January 2025, <https://edition.cnn.com/2025/01/21/tech/openai-oracle-softbank-trump-ai-investment>, accessed 15 September 2025.

The UK's 2023 Integrated Review Refresh (IRR) committed £500 million 'in new and existing funding', and all UK governments have since repeatedly pledged additional funding for further ST&I.[2] However, ambitious aims and budget declarations alone are insufficient to secure the strategic advantage that these technologies may offer. The UK's ST&I ecosystem has a high number of stakeholders, each driven by different motivations. These range from economic incentives or academic pursuits to national security concerns. The successful interplay of these stakeholders, paired with the right strategic and regulatory landscape, can advance technology innovation in the UK.

The UK cannot lead the world in all technologies. It, alone, is also unlikely to lead in any single technology: the realities of globalisation and the complexities of supply chains make this challenging. Instead, key alliances and partnerships with other countries, sectors and institutions are critical. Some technologies are more relevant to the UK national security community. These include AI, quantum technologies, space technologies and future telecommunications. The right priorities (and the relevant partners) need to be paired with the necessary budget to achieve the UK's ambitious aim of securing a strategic advantage in science and technology (S&T), including in the realm of national security.

This paper is part of a 12-month research project examining the UK's position and progress in securing a national security advantage from disruptive strategic technologies. The overall aim of the project is to develop an understanding of the UK's current approach to enhancing technological innovation for national security purposes, to identify gaps in this work, and to set out options for future policy levers to develop and enhance UK disruptive technology capabilities.

The research outlines the UK's assets, needs and dependencies in the global race for technology, and identifies what should be the UK's priorities in the next three to five years. These priorities would reinforce existing strengths and compensate for current shortcomings and dependencies.

This paper comprises five chapters. The first chapter sets out the UK context to government efforts of securing a strategic advantage from disruptive technologies. The second chapter addresses the international dimension of competition for technology and securing technological advantage. The third chapter dives into the UK domestic asset of a strong academic sector. The fourth chapter examines the critical role of the private sector and its partnership with the public sector, especially for funding opportunities. The fifth chapter suggests strategies to leverage public–private partnerships (PPPs), with a focus on the UK government as an early customer, start-ups, intellectual property (IP) and patents. The conclusion provides comprehensive policy recommendations.

2. HM Government, *Integrated Review Refresh: Responding to a More Contested and Volatile World*, CP 811 (London: The Stationery Office, 2023), p. 56.

The paper addresses the following research questions:

1. What factors contribute to the UK's positioning in the international competition for technology advantage? What are the assets, limitations and risks that determine the UK's position?
2. What is the role of the UK national security community within the UK ST&I ecosystem? How does it interact with other stakeholders?
3. What issues do UK policymakers need to address in the next three to five years to secure strategic advantage from these technologies in a national security context? Who are the key partners in implementing solutions to these issues?

Methodology

The research conducted for this paper used a mixed methods approach.

An initial rapid evidence assessment was conducted between February and May 2024. This used open source online desk-based research into the ST&I ecosystem. This included exploring the funding environment, available government programmes and departments, academic hubs and centres of excellence, and independent expert institutions. Research was conducted into the four key technology clusters addressed within this project: AI, quantum, space, and future telecommunication technologies. In this paper, the term 'disruptive technologies' primarily refers to these four technologies. It also includes other rapidly emerging technologies and the technology that sits at the intersections of the four technologies. This research included UK national strategy documentation, open source technology briefs and academic research outputs.

In addition, 57 semi-structured interviews were conducted with key experts and stakeholders in the ST&I ecosystem, including: members of the UK Intelligence Community; the UK government and academics specialising in disruptive technologies or UK ST&I policy; public and private sector funding bodies; and experts in international innovation ecosystems. Interviewees were selected for their expertise at the intersection of national security and technology, or were selected from within the wider UK ST&I ecosystem. Interviewees also made introductions to experts in non-public roles. The subsequent conversations explored technology topics and UK agency strategies, allowing for more detailed insights than standard interviews or surveys. All interviewees voluntarily consented to the interviews and on the condition of anonymity. Table 1 provides an overview of the interviewees.

Table 1: Number of Interviewees and Their Sector Affiliation

Sector	Number
Public Sector	30
Academia	14
Private Sector	10
Think Tanks/Civil Society	3
Total	57

Source: The authors.

In addition, a roundtable with private sector stakeholders shaping the UK ST&I ecosystem was conducted in December 2024 to explore the relationships and partnerships between the private sector and the UK government. The roundtable was designed to explore the success of mechanisms and levers in ST&I policy in enabling the private sector to deliver strategic advantage from disruptive technologies.

The interviews and roundtable were held at the unclassified level. Comments shared by participants were anonymous and non-attributable.

Limitations and Scope

The following limitations and scope should be noted in relation to the project:

- The primary focus areas of the project are AI, quantum technologies, space and future telecommunications. While other priority technologies are referred to in UK ST&I, and defence and security policies (for example, semiconductors and engineering biology in the 2023 IRR), reference to these is only made where appropriate.
- This research focuses on the intersection of disruptive technologies and the 'national security community'. For the purposes of this research project, the 'national security community' refers to: the Security Service (MI5); the Secret Intelligence Service (MI6); the Government Communications Headquarters (GCHQ); the Ministry of Defence (MoD); the Home Office; and the National Crime Agency.
- The research does not refer to any classified materials or capabilities and has been conducted at an unclassified level. Other classified information may be relevant to the research questions raised in this paper but cannot be discussed due to project parameters.

I. Securing Strategic Advantage from Disruptive Technologies: The UK Context

The UK is yet to carve out its position in the global competition for technology. Except for the US and China, most countries – including the UK – cannot realistically hope to lead the world in several of the most high-profile emerging technologies. How can smaller countries, especially the UK, identify and deliver a compelling approach to technology and innovation that makes effective use of their limited resources with a focus on securing both economic growth in a fiscally challenging period, and delivering national security objectives in light of heightened geopolitical tensions?

Globally, countries are expanding their efforts to enhance technological capabilities for their national advantage. They are allocating significant resources to foster innovation and to bolster a thriving tech ecosystem – including investing in dual-use technologies, which are highly relevant to national security and defence. Allies and adversaries have made high-profile announcements of ambitious strategies, new spending measures, and additional funding for research and innovation hubs or infrastructure projects. Measures extend beyond financial resources; they include a wide range of levers to enhance ST&I ecosystems, such as measures to attract talent or remove regulatory red tape.

The UK is no exception to this trend. Especially since 2020 – with the rise of heightened geopolitical tensions and supply chain challenges experienced during the Covid-19 pandemic – the UK has pushed to harness technological advancements for national security purposes. Key individuals within the Boris Johnson government, such as Dominic Cummings, publicly advocated for a stronger link between technology and national security. This was reflected in a number of key strategies at the time: the 2023 IRR spoke of 'strategic advantage in science and technology as a core national priority',[3] and the 2023 UK's International Technology Strategy set out a vision for becoming a 'science and technology superpower'.[4]

The UK benefits from key assets that positively contribute to its position in this international competition: a strong quantum technologies ecosystem; thought leadership on AI safety; an excellent academic sector; and convening power on technology issues. Conversely, critical gaps in the UK's position remain. These include: few large technology companies; a lack of sufficient capital to scale up its start-ups; minimal manufacturing capabilities; and a lack of an innovation-friendly ecosystem which embraces risks. The UK remains dependent on foreign suppliers for key technologies with crucial national security implications, namely semiconductors,[5] launch capabilities, telecommunication infrastructure[6] (including radios)[7] and critical minerals.[8]

3. HM Government, *Integrated Review Refresh*, p. 14.
4. HM Government, *UK International Technology Strategy*, CP 810 (London: The Stationery Office, 2023), p. 4.
5. Interview with participant P12, online, 17 July 2024; interview with participant P20, online, 16 December 2024; interview with participant P26, online, 30 January 2025.
6. Interview with participant P18, London, 12 November 2024.
7. Interview with participant P25, online, 30 January 2025.
8. Interview with participant P29, online, 3 February 2025.

Table 2 provides a more detailed overview of the UK's assets, needs, risks and dependencies based on the interview data.

Table 2: UK Assets, Needs, Risks and Dependencies in the International Competition for Technological Advantage

Assets	Needs	Risks and Dependencies
World-leading education ecosystem	Grow the venture capital (VC) community	Foreign students paying tuition fees which fund academic research
Strong university and other early research	More trusted capital to scale up UK tech start-ups	Semiconductor supply chain and manufacturing
Flourishing tech start-up scene	More UK tech 'unicorns' and ability to keep UK companies	US tech leadership and demands
Smaller, agile public sector	Tech giants	Foreign capital to scale UK start-ups
UK government as international technology convener	An innovation-friendly regulatory landscape (testing environments and copyright regime)	Individual champions for tech innovation across sectors and government departments
Strong quantum technology ecosystem	A braver risk culture	Radio manufacturers and supply chains
Thought leadership on AI safety	Better understanding of partners' strengths	Batteries
Influential work on tech standards	Better understanding of adversaries' progress and ecosystem	High housing costs around start-up areas (Oxford, Cambridge, London)
Track record in chip design	Launch capabilities	High energy costs
Large global telecoms operators	More large AI tech companies	Cloud providers
Strong base in life sciences	More manufacturing capabilities	Critical minerals
Talent and ideas		

Source: The authors.

'Strategic Advantage' as the UK's Objective

Doubts remain over what constitutes success in UK S&T, and there are multiple shortcomings and dependencies which will never be completely overcome. This raises questions about what the UK is trying to achieve with existing interventions. If, unlike the US and China, the UK cannot be the world's leader in technology, what is a more realistic aim for the UK to pursue?

Securing a 'strategic advantage' from disruptive technologies has been commonly used to describe the need to enhance the UK's technology track record and its capabilities, including for national security purposes. From the onset of this project, the term was used by many working at the intersection of national security and technology.

The phrase is in the 2021 Integrated Review but was used prior to its release.[9] Still, there is no agreed definition of 'strategic advantage' within UK government policy. This makes assessing its successful achievement inherently complex, despite its centrality to national security objectives. RAND has previously proposed that a position of strategic advantage 'is one in which an actor is more likely than others (whether hostile or friendly) to achieve their objectives in a given contest, crisis, or conflict'.[10]

A key challenge in assessing strategic advantage under this definition lies in first defining the UK's objectives – a step that has proven difficult during this period of shifting political agendas, and when considering the vast field of ST&I. For example, it is unclear whether the advantage sought refers to R&D, commercialisation or the adoption of technologies. Over the course of this research project, the UK has also experienced considerable political changes, including in government, party leadership and national priorities. Within the UK's ST&I ecosystem, these priorities have moved from viewing the UK as a tech superpower and securing a strategic advantage from disruptive technologies under Conservative leadership, to embracing 'mission driven economic growth' under Labour.[11]

Despite the differences in narrative terminology under current and previous governments, and challenges on the exact definition of strategic advantage, securing strategic advantage from disruptive technologies remains a strong objective for national security. These technologies underpin the UK's ability to achieve its core interests, even if those interests change over time. Investing in disruptive technologies can ensure cutting-edge defence capabilities, economic resilience and international

9. HM Government, *Global Britain in a Competitive Age: The Integrated Review of Security, Defence, Development and Foreign Policy* (London: The Stationery Office, 2021), p. 35.
10. James Black et al., 'Strategic Advantage in a Competitive Age: Definitions, Dynamics and Implications', RAND, 6 March 2023, p. x, <https://www.rand.org/randeurope/research/projects/2023/strategic-advantage-in-a-competitive-age.html>, accessed 27 March 2025.
11. Labour Party, 'Missions', <https://labour.org.uk/missions/>, accessed 1 August 2025.

influence, and are a multiplier for existing asymmetric strengths. This is a realistic ambition for the UK given its current strengths in certain areas of technology.

This research also demonstrates that the UK ecosystem, sitting at the intersection of technology and national security, needs to be guided by more concrete aims and objectives. These must be reflected in the UK's technology strategies. Under the current approach – largely advanced by previous governments – existing strategies set out grand ambitions but often fail to clarify which specific technologies or applications are UK priorities, and who is accountable for implementing them. For example, not all AI technologies or use cases can be priorities. Instead, identifying several use cases or subsets of technologies would provide useful strategic guidance to those in the ecosystem – and make the UK ecosystem more resilient to being guided by technology 'hypes' or fears of missing out. Clearly, identifying such priorities also requires input from the national security community. That said, it is also important for the UK to clearly state which technologies are not priorities. Countries such as the Netherlands already do this. However, in the UK, it can seem that every technology is a priority. This makes it harder for people and organisations to coordinate their work and resources.

> **The UK ... must acknowledge the limitations to the role it can play in this race for global tech supremacy**

The UK must set concrete priorities and objectives based on a realistic assessment of its current strengths and limitations, and must identify where it should cooperate with others. Such assessment is methodologically challenging (see the section titled 'The Challenge of Measuring the Success of UK Efforts'). It also requires a cultural shift in the UK, and it must acknowledge the limitations to the role it can play in this race for global tech supremacy. That is not to say that the UK cannot be ambitious in this space; on the contrary, it has developed some core strengths in this ecosystem – particularly around early research – and should confidently pursue its aims. Like other smaller countries, particularly those in Europe, the UK needs to come to terms with its economic and political weight and radically prioritise its limited resources. This includes a shift from a self-perception or ambition of being a 'global tech superpower', to being a medium-sized partner that plays a critical role in some (but not all) tech areas. Otherwise, the UK risks stretching itself thin across many areas, without developing a strong track record in specific technologies, commercialising technologies or enabling applications – and may neither have strong sovereign capabilities nor be an attractive partner to allies, with whom it could jointly develop sovereign capabilities.

The National Security Community: From Secrecy to Strategy

Setting these priorities clearly requires strategic input from the national security community. While there are some examples of the national security community successfully feeding into UK technology strategies – most notably, the UK Quantum Strategy[12] – wider challenges remain on the interaction between the national security community and the ST&I ecosystem.

Many interviewees continue to perceive that the UK national security community operates in siloes and is reluctant to feed into, or engage with, the wider ecosystem. Genuine concerns over classification and security considerations are warranted. However, the impression remains that the national security community over-relies on classification as an argument not to engage with members outside its own bubble. Decades of working separately, and a culture of secrecy, are being challenged in the UK national security community. Experts are now realising the need to engage with external tech innovation developments that might support national security missions. These same technologies are also a priority for the wider UK government from an economic growth and innovation perspective. The need for the UK national security community to overcome its reluctance to engage with others has been confirmed by its own members, including one who argued that 'we need to get over ourselves'.[13]

Numerous research participants stressed a need for a cultural shift that welcomes greater transparency between the national security community and other members of the ST&I ecosystem.[14] Yet, cultural change in established ways of working is challenging. The UK national security community has launched initiatives that seek to engage others, both within UK government and outside it. Externally, this includes communicating key technological challenges for national security agencies. For example, problem books aim to reduce mission challenges to technological problems without using sensitive information. This is a successful way to communicate outside classification needs and engage academic and technical problem-solvers in a language that appeals to them. Internally, this includes formalised work of organisations such as the National Security and Innovation Exchange (NSTIx), a government organisation established to coordinate technology and innovation activities across government stakeholders.[15]

12. Interview with participant P10, online, 10 July 2024.
13. Interview with participant P35, online, 13 February 2025.
14. Interview with participant P14, online, 20 September 2024; interview with participant P33, 11 February 2025, online; interview with participant P35, online, 13 February 2025.
15. National Security Technology and Innovation Exchange, <https://www.gov.uk/government/organisations/national-security-technology-and-innovation-exchange>, accessed 27 March 2025.

However, as of early 2025, NSTIx has been decommissioned and considerable work remains to be done on coordinating and communicating with stakeholders outside the national security community. Individuals, their personal connections and motivation to engage beyond departmental borders are critical. However, barriers to mobility remain across branches of the civil service, and for the private sector. Individual champions such as Dominic Cummings and Peter Knight – who have championed cross-sectoral work at the intersection of technology and national security – remain the exception. It is crucial that where these champions exist, or where individuals engage across silos, they are supported by adequate resources and formal recognition – allowing them to prioritise this joined-up work. For example, a degree of personal engagement exists between key governmental stakeholders investing in and funding dual-use innovation, including the Defence and Security Accelerator (DASA), the National Security Strategic Investment Fund (NSSIF), the Department for Business and Trade (DBT) and others. However, such engagement needs to be sustainable beyond personal appointments and to receive adequate formalisation and prioritisation to effectively avoid duplication of scarce resources. Exchanging knowledge on best practices and on the levers that UK government departments are already deploying would create further value for taxpayers.

The Challenge of Measuring the Success of UK Efforts

It is a challenge to understand which existing measures offer the best value for money. The ecosystem is large and interconnected, and success must consider both economic output and national security.

Economic growth may be easier to measure than the complex notion of 'strategic advantage'. Traditional quantitative measures, such as the size of armed forces or economic capacity, offer an incomplete view; rather, strategic advantage is often determined by qualitative factors such as political legitimacy, leadership, technological innovation and the ability to leverage asymmetric advantages across multiple domains.[16] The Integrated Review highlighted the role of S&T as a key enabler of strategic advantage.[17] Yet the absence of a robust theoretical framework and concrete aims makes it difficult to measure the success of related initiatives. Strategic advantage is highly relational and depends both on national potential and the ability to translate that potential into real-world outcomes. The success of real-world outcomes, in turn, is highly context-dependent and must consider evolving threats, technological disruptions and geopolitical shifts. Consequently, any meaningful evaluation must

16. Black et al., 'Strategic Advantage in a Competitive Age', pp. 15, 55.
17. HM Government, *Global Britain in a Competitive Age,* p. 35.

recognise that references to 'strategic advantage' do not have a fixed meaning across technologies, sectors and communities. Moreover, the extent of such an advantage often remains unclear.[18]

This does not mean that it is impossible to identify successful and unsuccessful measures. Yet, the national security community's lack of transparency on the activities that have been undertaken and what it considers successful further complicates any assessments of 'success' in enhancing the UK's track record at the intersection of technology and national security.

Several government departments continue to track the UK's standing in the global competition for technology and in different national R&D ecosystems. The standing of other countries is also tracked. They rely on classified or commercial data, often to assess quantitative indicators such as numbers of patents, publications or funding budgets. Most of these assessments are not publicly available, either due to classification or data-sharing limitations. This is a significant impediment to public policy debates and risks duplication of efforts, as several government departments work on mapping the same ecosystems without a central repository of key information (for instance, on the track record of other stakeholders).

> **The lack of a comprehensive understanding of the UK's own strengths in the ST&I ecosystem is a significant limitation**

This research acknowledges the challenges of mapping these efforts. Understanding what success looks like – including establishing a causal link between government initiatives and rewards in the technological ecosystem – is an extremely difficult process, especially without access to classified information. The lack of a comprehensive understanding of the UK's own strengths in the ST&I ecosystem is a significant limitation to ongoing work in this area. An understanding of UK assets is essential for identifying what the UK can offer in its tech partnerships and remaining areas of weakness. This reveals the dependencies and capabilities that can be further leveraged or developed.

While this project does not exhaustively map UK assets, needs, risks and dependencies, its findings will nevertheless be communicated through this lens to contribute to a better understanding of the state of the UK's ST&I ecosystem at the intersection of national security.

18. Interview with participant P29, online, 3 February 2025.

II. The International Dimension to Securing a Strategic Advantage from Disruptive Technologies

Both allies and adversaries often enact similar measures to make the most of technological inventions. It is therefore critical to not only reflect on the UK's position, but also learn from international best practice.

This chapter considers interviewees' reflections on UK performance – compared with allies and adversaries – in this technological competition, and what the UK can learn from other countries, including the US, China and European partners. This chapter also examines key UK assets and priorities in this international competition, such as international tech diplomacy, technological standard-setting and the role of the Science and Innovation Network (SIN) in supporting these efforts.

The UK's Position in International Competition for Strategic Advantage

Mixed assessments emerged when interviewees considered whether the UK has maintained its technological edge over 'the adversary' or whether it has been outpaced by the adversary in securing a strategic advantage from disruptive technologies. Interviewee responses primarily focused on China, and their assessments varied widely – pointing to UK strengths,[19] such as niche technical capabilities,[20] or to the UK's

19. Interview with participant P20, online, 16 December 2024; interview with participant P22, online, 23 January 2025.
20. For example, chip design, radar and sensing, or software development. Interview with participant P23, online, 23 January 2025; interview with participant P25, online, 30 January 2025.

alliance with the US.[21] Others felt that the UK only maintained a marginal technological edge,[22] with a poor outlook for maintaining it.[23] In general, the majority of interviewees were less confident of the UK's capabilities compared with China's progress on technology and innovation.[24] Instead, the sentiment was that the UK 'cannot compete with China'[25] as 'China is way and above the UK'.[26] Even where the UK seeks to catch up[27] or can position itself as 'the best of the rest',[28] the race for cutting-edge technologies primarily takes place between the US and China,[29] with the UK 'becoming increasingly irrelevant in these conversations'.[30] Interviewees frequently stressed that the UK cannot ensure that the adversary does not outpace the UK.[31]

> **The UK cannot ensure that the adversary does not outpace the UK**

Not all participants bought into the premise of strategic advantage, nor did all participants agree that the UK is involved in a race for technology. Some participants questioned what constituted a 'strategic advantage',[32] while others disagreed with the framing of a 'race',[33] as it tenuously assumes that the UK has the option of not being left behind.[34] One academic stressed that the notion of a race overlooks how science and innovation depend on collaboration, not competition, and dismissed the framing as a 'nationalistic argument that misunderstands how science works'.[35] Another participant

21. Interview with participant P22, online, 23 January 2025; interview with participant P32, online, 10 February 2025; interview with participant P26, online, 30 January 2025, describing the relationship with the US as the UK's 'strongest asset'.
22. Interview with participant P26, online, 30 January 2025; also, interview with participant P31, online, 7 February 2025.
23. Interview with participant P19, online, 6 December 2024.
24. Interview with participant P15, online, 30 September 2024, stating 'China is outpacing most'; interview with participant P7, online, 4 July 2024; interview with participant P14, online, 20 September 2024.
25. Interview with participant P17, online, 14 October 2024.
26. Interview with participant P18, London, 12 November 2024.
27. Interview with participant P33, online, 11 February 2025.
28. Interview with participant P18, online, 12 November 2024.
29. Interview with participant P17, online, 14 October 2024. This participant argued that the UK had already lost out on the innovation wave before Chat GPT: interview with participant P12, online, 17 July 2024.
30. Interview with participant P19, online, 6 December 2024.
31. Interview with participant P12, online, 17 July 2024.
32. Interview with participant P23, online, 23 January 2025.
33. Interview with participant P8, online, 4 July 2024; authors' interview with participant P2, online, 17 June 2024. Interviewee P2, for example, was less concerned about winning a race than in UK investment in technology being stolen by the adversary.
34. Interview with participant P4, online, 1 July 2024.
35. Interview with participant P8, online, 4 July 2024.

warned that 'the fear of missing out should not be a motivation to put in more resources'.[36]

Based on the interview data and the limitations of this research project, there are no clear factors that determine why participants arrive at positive or negative conclusions on the UK's perceived advantage over the adversary. The assessments might, at times, be based on factors including personal political views or knowledge of classified material. There was also no detailed indication of which aspects of the ST&I ecosystem were decisive to secure 'strategic advantage' for the UK, and whether it is more important to enhance early research, commercialisation or adoption of technology.

The same unknowns apply to the question of whether the UK is doing enough to understand China; this question provoked similarly divided responses. Interviewees considered the understanding of one's own strengths and those of the adversary to be key.[37] Some interviewees made reference to how UK intelligence agencies[38] and other government departments seek to understand the adversary.[39] The coordination with Five Eyes partners was considered especially important to understanding adversarial progress on technologies, and to temper expectations of certain technologies, such as quantum radar.[40] While some interviewees considered British understanding of adversarial technologies, such as Chinese AI advancements, to be strong,[41] others felt that 'China knows a lot more about us and our research than we do about theirs'.[42] Interviewees made reference to the need to outline basic R&D structures and map relevant stakeholders of the UK ST&I ecosystem – a highly complex task, of which results are often not publicly accessible.

The reasons for the interviewees' assessment of the UK's position in the international competition for technological supremacy cannot be conclusively identified. A comparative assessment contrasting UK assets, needs, risks and dependencies against those of its allies and adversaries is, however, key to understanding the UK's technology track record and to informing its policies.

36. Interview with participant P5, online, 3 July 2024.
37. Interview with participant P8, online, 4 July 2024, pointing to the paradox of needing to work together to understand competition.
38. Interview with participant P5, online, 3 July 2024; interview with participant P32, online, 10 February 2025.
39. Interview with participant P18, London, 12 November 2024.
40. Interview with participant P5, online, 3 July 2024.
41. Interview with participant P34, online, 11 February 2025.
42. Interview with participant P4, online, 1 July 2024.

What the UK Can Learn from International Best Practice

Although many countries are seeking to secure advantages from disruptive technologies, the interviews point to a poor understanding within the UK ST&I community of what constitutes international best practice to achieve these advantages. Interviewees were often unsure about how to assess the UK against other countries, or what the UK can learn from them – even when interviewees were encouraged to share anecdotal evidence rather than comprehensive assessments. Similarly, the existing academic and policy literature only offers limited comparative insights of ecosystems, particularly concerning the intersection of technology and national security – which remains a sensitive area that has only recently regained a wider, more public interest.

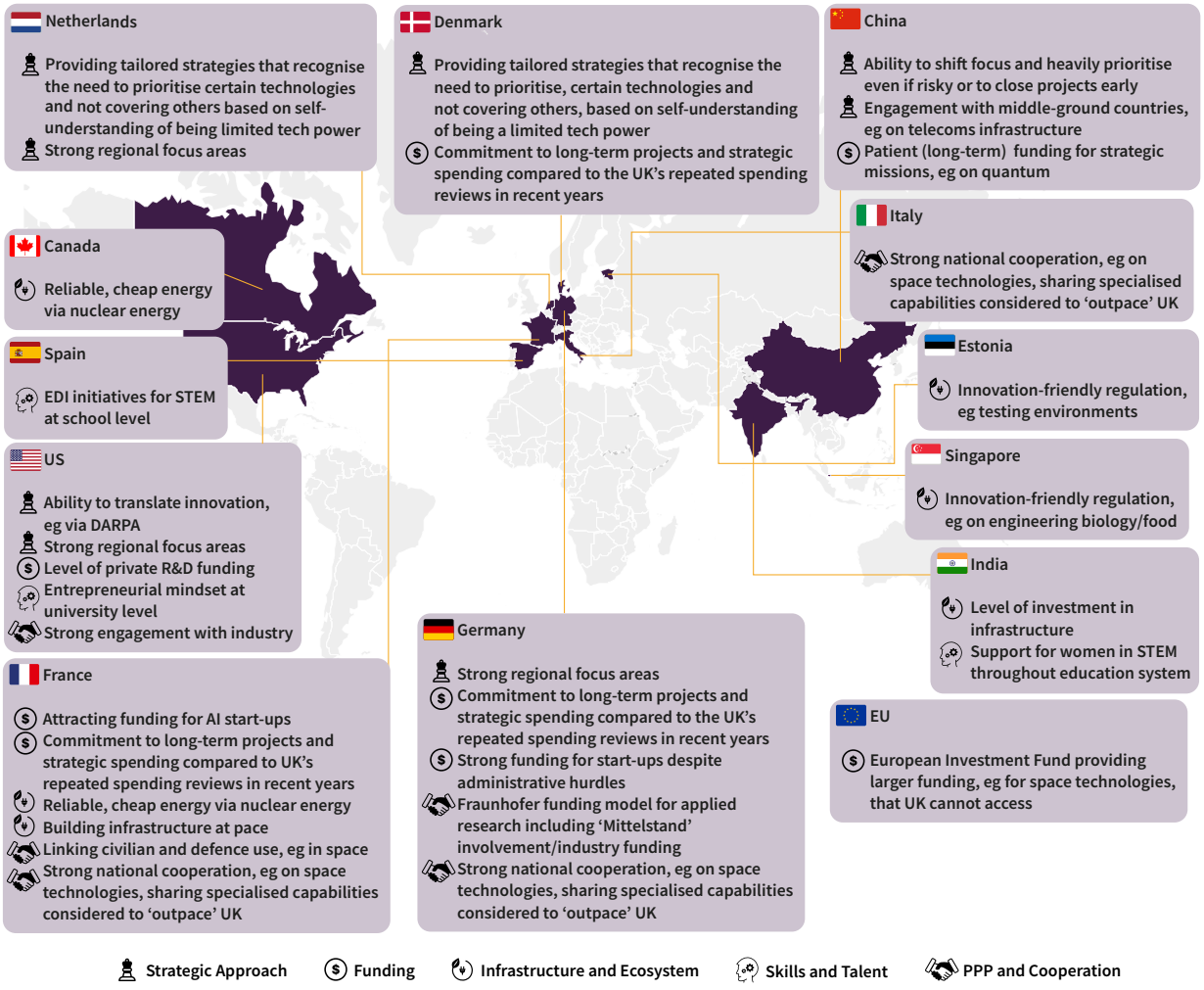
> **[There is] a limited understanding in the broader UK ST&I community … about what best practice in the field looks like**

Another limitation was that some interviewees from the ST&I ecosystem did not work in roles requiring a strong international outlook and were therefore less confident to speak on international comparisons. Nevertheless, the data indicates there is a limited understanding in the broader UK ST&I community – including on the part of mid- to senior level civil servants – about what best practice in the field looks like. Numerous stakeholders were not aware of the comparative strengths of certain Five Eyes partners or European counterparts. Some referenced the scale of other ST&I ecosystems, primarily in the US and China, or the size of smaller governmental counterparts, namely Australia[43] or Denmark.[44] Still, the comparative comments offered by interviewees often remained superficial – offering no analytical insights on whether countries which operate on another economic scale achieve proportionally greater advances, or to whether the UK could learn from them.

43. Interview with participant P33, online, 11 February 2025.
44. Interview with participant P1, online, 19 April 2024; interview with participant P18, London, 12 November 2024.

As the UK's ST&I ecosystem is highly nuanced, comparative remarks – especially for countries of different sizes – naturally risk drawing invalid analogies. Furthermore, such remarks cannot exhaustively consider the underlying structural, political and economic factors at play in each country. The following findings (Figure 1) must therefore not be seen as conclusive by themselves; rather, they are based on the interviewees' perceptions. These findings can be considered a starting point for further in-depth research that could challenge and test these findings.

Figure 1: Perceived International Best Practice



Source: The authors.

Learning from US Technology Leadership Through Scale and Private Sector Backing

Undoubtedly, the US is world-leading in many, if not most, cutting-edge technologies. If breadth of technological strength – rather than a niche capability – is decisive in being 'world leading', the scale of the US ecosystem constitutes a clear advantage. The US ecosystem benefits from the 'sheer force of numbers, the invested capital and the number of skilled people'.[45] This difference of scale – in terms of the US economy, its domestic demand and the power that comes with it – makes the US stand out. These characteristics also make it hard for the UK to compete with, or compare itself to, the US. [46]

Other interviewees also considered that the UK's smaller ecosystem offered advantages over that of the US. The large US public sector was perceived as 'slow to move',[47] while the UK's public sector was seen as 'agile in comparison'[48] and running at a lower cost than its US counterpart.[49] Nonetheless, the US was repeatedly admired for its risk culture for founding start-ups and for its acceptance of failure as part of the outcome – two attributes the UK is often seen as lacking, with its ST&I ecosystem considered 'risk averse'.[50] The UK, in contrast, was seen as having more appetite for political risk, particularly with respect to support of Ukraine[51] (a country where certain emerging technologies that are critical to national security are being developed, tested and refined).[52]

Consensus emerged among interviewees that one key strength of the US, which the UK should seek to replicate, is the engagement of large industry partners and the private sector more generally – evident in the Silicon Valley and Boston ecosystems.[53] While caveats of scale remain, this is particularly the case for private spending on R&D. One interviewee argued that while the UK's public spending on quantum technologies exceeds that of the US, US private spending is more substantial; in the UK, there are

45. Interview with participant P2, online, 17 June 2024.
46. Interview with participant P6, online, 3 July 2024; interview with participant P18, London, 12 November 2024.
47. Interview with participant P1, online, 19 April 2024.
48. *Ibid.*; similarly noted by P14, online, 20 September 2024; interview with participant P13, London, 22 July 2024. P13 describes the UK public sector as 'more nimble'.
49. Interview with participant P13, London, 22 July 2024.
50. According to the Communications and Digital Committee, the 'UK risks becoming an "incubator economy" if we don't take action to support our tech companies to scale up'. See UK Parliament, Communications and Digital Committee, 3 February 2025, <https://committees.parliament.uk/committee/170/communications-and-digital-committee/news/205059/uk-risks-becoming-an-incubator-economy-if-we-dont-take-action-to-support-our-tech-companies-to-scale-up/>, accessed 28 March 2025.
51. Interview with participant P14, online, 20 September 2024.
52. Joyce Hakmeh, 'What Ukraine Can Teach Europe and the World About Innovation in Modern Warfare', 5 March 2025, <https://www.chathamhouse.org/2025/03/what-ukraine-can-teach-europe-and-world-about-innovation-modern-warfare>, accessed 27 March 2025.
53. Interview with participant P5, online, 3 July 2024; interview with participant P1, online, 19 April 2024.

major companies that would benefit from quantum technologies but they need to be more collaboratively and strategically engaged.[54] Arguably, however, such private funding needs to be driven (or, at least, stimulated early on) by public demand, especially strategically, as is already the case in the US, where departments such as the Department of Defense send signals to the market that 'crowd-in' private R&D funding.[55]

The US also succeeds in its deliberate approach to ensuring that innovation is translated and commercialised.[56] DARPA is considered an exemplary model to provide funding for risky research.[57] The UK has taken note of this approach and founded the Advanced Research and Invention Agency (ARIA).[58] Unlike its US counterpart, however, ARIA is not defence-focused, and the common – but often superficial – comparison to DARPA is therefore misleading. Comparing it to the Advanced Research Projects Agency – Energy (ARPAe), a US funding body focused on energy technologies, is more accurate.[59] ARIA is still in its early stages, which makes it difficult to assess its success. It is already uniquely placed to fund cutting-edge, high-risk research with a strong emphasis on commercialisation. This includes the ability to fund promising individuals as opposed to only academics embedded in a university ecosystem. ARIA also provides critical training and hosts activities directed at enhancing an entrepreneurial mindset among researchers, for instance through so-called 'activation partners'. These partners support start-ups by upskilling founders or by providing funding for demonstration devices.[60] However, it is still unclear whether it is well-suited to fund research for dual-use or defence technologies, when compared with other funding mechanisms that have a direct customer, such as DARPA or DASA.[61]

Interviews for this project were conducted throughout a period of considerable change, including a change of government both in the UK and in the US. While still considered a key partner to the UK in the race for technology,[62] the US is also a competitor,[63] especially for talent and capital.[64] One participant noted that 'the UK exports skills and

54. Interview with participant P5, online, 3 July 2024.
55. Gianluca Pallante, Emanuele Russo and Andrea Roventini, 'Does Public R&D Funding Crowd-In Private R&D Investment? Evidence from Military R&D Expenditures from US States', *Research Policy* (Vol. 52, No. 8, 2023).
56. Interview with participant P2, online, 17 June 2024.
57. *Ibid*.
58. UK Government, 'Advanced Research and Invention Agency (ARIA): Statement of Policy Intent', 19 March 2021, <https://www.gov.uk/government/publications/advanced-research-and-invention-agency-aria-statement-of-policy-intent>, accessed 28 March 2025.
59. Interview with participant P39, London, 19 February 2025.
60. *Ibid*. See also ARIA, 'Activation Partners', <https://www.aria.org.uk/about-aria/activation-partners>, accessed 28 March 2025.
61. Interview with participant P39, London, 19 February 2025.
62. Interview with participant P26, online, 30 January 2025; interview with participant P32, online, 10 February 2025.
63. Interview with participant P23, online, 23 January 2025.
64. Pia Hüsch and Natasha Buckley, 'What Does Trump 2.0 Mean for UK Tech Ambitions?', Binding Hook, 14 January 2025, <https://bindinghook.com/articles-binding-edge/what-does-trump-2-0-mean-for-uk-tech-ambitions/>, accessed 28 March 2025.

companies to [the] US'.[65] Yet, current geopolitical tensions raise key questions on how to navigate this fine line dividing partnership and competition. Although the 'constant and unique partnership with the US' was considered 'resilient to changes', the competition between the two countries is now more prominent.[66] This raises key questions, including whether there are circumstances in which the UK would not sell key technologies to the US,[67] or would block US buyouts of UK firms. President Donald Trump's transactional approach to diplomacy further constitutes a challenge for the UK, which may now face new demands and trade-offs. On UK involvement for US-led AI programmes, one participant therefore noted that to hold leverage in negotiations with the US, the UK must do so from a position of strength and with its own investment, noting that 'the more we can bring to the table, the more leverage we have'.[68] This approach also resonates for other technologies beyond AI, but others viewed this with scepticism.

China's Strategic Approach to Achieving Technological Dominance

It is challenging to compare a country such as China with the UK due to differences of scale and political systems. Nevertheless, interviewees identified some beneficial practices that China uses to advance its technology ambitions, from which the UK can learn. China, most notably, can leverage a 'closely coordinated system'[69] for a strategic approach to technology development. This is guided by its explicit aspiration to become a technology superpower and achieve market dominance.[70] In contrast, the UK was considered 'not as good at joining up talk'.[71] China's ability to align academic, industrial and military missions 'mean[s] significant advantages'.[72]

These aspirations are backed by considerable resources, both in terms of skilled people and finance. Interviewees saw this long-term funding and patient approach as beneficial, stating that 'if you want to be a superpower … you need to think beyond the span of an individual government'.[73] One interviewee felt that what distinguishes China from other states is its ability to have long-term plans (over 20 years), taking national security considerations into account. These plans have enabled China to become 'good

65. Interview with participant P1, online, 19 April 2024.
66. Interview with participant P23, online, 23 January 2025.
67. Interview with participant P13, online, 22 July 2024.
68. Interview with participant P22, online, 23 January 2025.
69. Interview with participant P5, online, 3 July 2024.
70. Interview with participant P3, online, 26 June 2025. Similarly noted in the interview with participant P33, online, 11 February 2025.
71. Interview with participant P28, online, 3 February 2025.
72. Interview with participant P14, online, 20 September 2024.
73. Interview with participant P31, online, 7 February 2025.

at identifying technologies and enabling investments that allow them to move at scale'.[74] For example, areas such as quantum technologies have benefitted from Chinese long-term funding.[75] In contrast, UK strategies often change in line with new governmental priorities and reference five-year programmes. The 10-year funding period advanced for the UK Quantum Strategy is a positive exception. China's 'willing[ness] to aggressively prioritise and build up capacity and then let the market do its work' was considered a core strength,[76] as was the ability to build large-scale infrastructure.[77] Interviewees also credited China's high tolerance for risky projects and the ability to fail,[78] as well as its ability to (easily) shift focus, including a willingness to let go of projects[79] – aspects that are weaknesses in the UK system.

China operates at a remarkable scale. However, it is not clear how much the UK can learn from its example. One participant explained that 'China throws money and people at challenges, but it is not clear whether they deliver results to the scale and quality that you would expect proportionally'.[80] Instead, the interviewee cautioned against the perceived dominance of China in areas such as AI and quantum technologies. They pointed out that actual results continued to rely on IP theft and that the number of publications was based on 'dummy research … without actual research'.[81] Other interviewees added that while China's practices currently secured it significant advantages, its ability to innovate remained limited compared with the US in the short term. They saw the possibility for this to change in the medium to long term, particularly if China were able to compensate for current US dominance in semiconductors.[82]

Finally, participants looked to China for its strong presence in standard-setting bodies[83] and its engagement with middle-ground countries, notably in telecommunications infrastructure and space programmes.[84]

74. Interview with participant P5, online, 3 July 2024.
75. Antonia Hmaidi et al., 'Chinese LLMs + Weight-Loss Drugs + Chinese Telcos Build AI Models', 26 September 2024, <https://merics.org/en/chinese-llms-weight-loss-drugs-chinese-telcos-build-ai-models>, accessed 28 March 2025.
76. Interview with participant P22, online, 23 January 2025.
77. *Ibid.*
78. Interview with participant P29, online, 3 February 2025.
79. Interview with participant P22, online, 23 January 2025.
80. Interview with participant P2, online, 17 June 2024.
81. *Ibid.*
82. Interview with participant P14, online, 20 September 2024.
83. Interview with participant P3, online, 26 June 2024. See also Tim Rühlig, 'Chinese Influence Through Technical Standardization Power', *Journal of Contemporary China* (Vol. 32, No. 139, 2022), pp. 54–72.
84. Interview with participant P13, London, 22 July 2024. See also César Eduardo Santos, 'China's "People-to-People" Diplomacy Targets the Global South', *The Diplomat*, 29 November 2024, <https://thediplomat.com/2024/11/chinas-people-to-people-diplomacy-targets-the-global-south/>, accessed 15 September 2025; Tin Hinane El Kadi, 'How Huawei's Localization in North Africa Delivered Mixed Returns', Carnegie Endowment for International Peace, 14 April 2022, <https://carnegieendowment.org/research/2022/04/how-huaweis-localization-in-north-africa-delivered-mixed-returns?lang=en>, accessed 28 March 2025.

Learning from European Partners' Priorities

Apart from China and the US, interviewees had an overall limited understanding of how other countries steer competition for innovation. This is a missed learning opportunity for the UK, since many likeminded countries in Europe and further abroad face similar budget limitations and a need to focus on some technologies. Similarly, they are unable to compete across the board.

Some participants openly acknowledged their lack of comparative knowledge[85] while others stressed the need to better understand other ecosystems and to undertake an in-depth comparison.[86] The following section does not provide such in-depth analysis; rather, it identifies useful areas that could constitute a starting point for future research. It offers suggestions of thematic areas of best practice that could form hypotheses for future research.

Germany

Many participants identified Germany's Fraunhofer Society for the Advancement of Applied Research and its collection of 76 world-leading research institutes across the country as an exemplary model for advancing applied S&T.[87] The Fraunhofer funding model – based on a combination of significant industrial revenue, publicly funded research and funding from federal and state governments – was considered particularly successful.[88] The close link to universities[89] – especially to Germany's strong *Mittelstand* (medium-sized industry partners) – ensures a market-driven approach to applied research.[90] The position of the Fraunhofer institutes, which are at the intersection of industry and research, means that 'companies who work [with these institutes] have access to the latest technology'.[91] The Fraunhofer model was also perceived to be providing societal benefits, as Germany's strong manufacturing base supports widespread, high-quality employment. By contrast, well-paid technology roles in the UK tend to be concentrated within early-stage development, with fewer benefits to the broader workforce.[92]

85. Interview with participant P23, online, 23 January 2025; interview with participant P39, London, 19 February 2025; interview with participant P42, online, 21 February 2025.
86. Interview with participant P6, online, 3 July 2024; interview with participant P4, online, 1 July 2024.
87. Fraunhofer, 'About Fraunhofer', <https://www.fraunhofer.de/en/about-fraunhofer.html>, accessed 28 March 2025.
88. Interview with participant P7, online, 4 July 2024; interview with participant P8, online, 4 July 2024; interview with participant P41, online, 21 February 2025.
89. Interview with participant P7, online, 4 July 2024.
90. Fraunhofer, 'About Fraunhofer'.
91. Interview with participant P8, online, 4 July 2024.
92. Interview with participant P1, online, 19 April 2024.

British efforts to recreate a similar model that linked research and industry received public praise.[93] However, interviewees found that such efforts were not successful.[94] For example, the Catapult Network[95] lacks government or other mid-tier regional funding. The UK also lacks the equivalent of a strong manufacturing *Mittelstand*, on which the success of Fraunhofer relies on.[96] Catapults do not have this close link to industry or academia.[97] These contextual and structural differences make it challenging to transplant successful funding models from one country to another, even if they are envied.[98]

Despite the praise for the Fraunhofer model, one participant pointed out that the model is successful in linking established technologies to existing industry, but not effective for emerging ones, such as AI.[99]

Participants also highlighted Germany's strong spinout and start-up scene and the considerable amount of funding available to spinouts and start-ups – provided they can jump through the necessary bureaucratic hoops.[100] Like the UK, Germany has many strong early research centres and universities that result in start-ups and spinouts. However, reputable data to compare the success of start-ups is scarce. Some sources indicate a higher five-year survival rate of German start-ups (60%[101]) compared with UK start-ups (42.4%[102]). Other statistics see a higher failure rate among German start-ups (75%) than UK equivalents (70%).[103] Further research would need to explore the comparability and quality of these statistics. Given the recent surge in policy levers to support technology start-ups, new data is necessary. Such data should also capture sectoral differences and reasons for survival. German start-ups primarily listed personal, rather than financial, reasons for discontinuation.[104]

93. Catapult Medicines Discovery, 'House of Lords Recognises Catapult Network as a Critical National Asset', <https://md.catapult.org.uk/news/house-of-lords-recognises-catapult-network-as-a-critical-national-asset/>, accessed 28 March 2025.
94. Interview with participant P7, online, 4 July 2024; interview with participant P8, online, 4 July 2024; interview with participant P2, online, 17 June 2024.
95. Innovate UK Catapult Network, 'Who We Are', <https://catapult.org.uk/>, accessed 28 March 2025.
96. Interview with participant P7, online, 4 July 2024.
97. *Ibid.*
98. *Ibid.*
99. Interview with participant P41, online, 21 February 2025.
100. *Ibid.*
101. KfW Entrepreneurship Monitor, 'KfW Research: KfW Entrepreneurship Monitor: Number of Start-ups in Germany has Increased Slightly to 568,000', 17 June 2024, <https://www.kfw.de/About-KfW/Newsroom/Latest-News/Pressemitteilungen-Details_810880.html>, accessed 15 September 2025.
102. Darko Radic, 'Eye-Opening UK Startup Statistics for 2025', Moneyzine, 14 February 2024, <https://moneyzine.com/uk/resources/startup-statistics-uk/>, accessed 15 September 2025.
103. Naveen Kumar, 'Startup Statistics (2025) – Numbers by Country & Success Rate', Demandsage, 2 June 2025, <https://www.demandsage.com/startup-statistics/>, accessed 15 September 2025.
104. KfW Entrepreneurship Monitor, 'KfW Research'.

Estonia

As a global leader on software as a service (SaaS) and on digital public services, participants saw Estonia as a model of best practice – particularly due to an innovation-friendly regulatory landscape. Indeed, Estonia is home to Europe's highest number of unicorns per capita.[105] Its business-friendly tax regime and low administrative hurdles – for example, in ease of doing business – are considered beneficial for attracting innovation.[106]

A notable Estonian practice is to remove regulation that inhibits innovation, not simply enact innovation-friendly regulation. This is the task of Accelerate Estonia, a government agency with the motto of 'making illegal things legal'.[107] It provides companies with a transparent mechanism to lobby for the removal of regulation or administrative hurdles which stop them from innovating. This unusual government agency, combined with an availability of interoperable data provided through a high degree of data capture from digital services, contributes to Estonia's success as an innovation testing bed.[108]

The UK as a Tech Convener and Diplomat

Participants repeatedly stressed that the UK's track record as a technology convener on the international stage is a key asset.[109] The AI Safety Summit has become a striking example of successful UK tech diplomacy,[110] despite the summit series' now uncertain future.[111] The UK's active role in S&T diplomacy allows the UK to represent its interests abroad and leverage its diplomatic strength and experience. Convening on technology subjects often requires skilful diplomacy, especially when inviting both allies and adversaries to the table. It can also be a resource-intensive pursuit. For example, many civil servants across Whitehall were reallocated to conference preparations on short notice in preparation of the UK's AI Safety Summit. The external perception of the UK's role in the international race for technology is linked to its efforts in tech diplomacy. It is therefore key that these efforts continue to be adequately resourced and to evolve in light of geopolitical and technological developments.

105. Hannah Brown et al., 'The Big Question: Estonia has the Most Tech Unicorns Per Capita in Europe – What's Their Secret?', 23 September 2024, <https://www.euronews.com/business/2024/09/23/the-big-question-estonia-has-the-most-tech-unicorns-per-capita-in-europe-whats-their-secre>, accessed 28 March 2025.
106. Interview with participant P43, online, 3 March 2025.
107. Accelerate Estonia, 'Making Illegal Things Legal', <https://accelerate.ee/>, accessed 28 March 2025.
108. Interview with participant P43, online, 3 March 2025.
109. Interview with participant P18, London, 12 November 2024.
110. *Ibid.*; interview with participant P51, online, 6 March 2025.
111. Siméon Campos and Chloe Touzet, 'We Need to Avert an AI Safety Winter', *RUSI Commentary,* 7 March 2025, <https://www.rusi.org/explore-our-research/publications/commentary/we-need-avert-ai-safety-winter>, accessed 28 March 2025.

In addition, the UK's international engagement in technology includes work with Chinese counterparts, something that sets the UK apart from many other Western allies.[112] While some allies lack the resources to staff this work adequately, others lack the risk appetite for this kind of engagement. The US, for instance, is unlikely to seek this type of public-facing engagement. Although such work needs to be balanced against national security considerations, and the risk of offending other allies such as Taiwan or the US, it allows the UK to gain unique insight from China. It therefore constitutes an asset that the UK can bring to the negotiation table with partners such as the US or the EU, which otherwise outperform the UK in terms of size and market share. The work of the Foreign, Commonwealth & Development Office (FCDO) on AI in China, and engagement with China via the AI Security Institute (AISI), have been received especially positively.[113] It was considered crucial that the UK maintains its unique position despite potential US pressure to disengage.[114]

Advancing UK ST&I Through the Science and Innovation Network

The first workshop organised in the context of this project identified the SIN as an underused tool in the UK's pursuit of strategic advantage from disruptive technologies. The network is made up of approximately 130 SIN officers who are embedded in 65 UK embassies across the globe, [115] promoting the UK ST&I ecosystem and mapping the host country's equivalent ST&I ecosystem.[116] SIN has arguably always comprised technology,[117] a commitment which was reconfirmed with the transformation of SIN into the Science and Technology Network (STN) in February 2025.[118]

However, SIN officers receive their mandate and tasks from their funding organisations – the Department of Science, Innovation and Technology (DSIT), and the FCDO – and only rarely, if at all, interact with the national security community.[119] This is partially due to the sizeable discrepancies in posting allocations, as some embassies

112. Interview with participant P34, online, 11 February 2025.
113. *Ibid.*
114. *Ibid.*
115. Interview with participant P21, online, 14 January 2025; UK Government, 'UK Science and Technology Network', <https://www.gov.uk/world/organisations/uk-science-and-innovation-network>, accessed 28 March 2025.
116. Interview with participant P18, London, 12 November 2025.
117. Interview with participant P21, London, 14 January 2025.
118. UK Government, 'UK Science and Technology Network'; Ian Wiggins, 'From SINners to SaiNTs – Shifts in UK Science and Tech Diplomacy', *RUSI Commentary,* 26 March 2025, <https://www.rusi.org/explore-our-research/publications/commentary/sinners-saints-shifts-uk-science-and-tech-diplomacy>, accessed 28 March 2025.
119. Interview with participant P37, online, 19 February 2025; interview with participant P41, 21 February 2025.

host several SIN officers, while others are responsible for a whole region. The majority of SIN officers are country-based hires,[120] and therefore do not hold security clearance. Replacing some officers with holders of security clearance may enhance their ability to engage with national security matters or increase the willingness of the national security community to engage with them. Conversely, such a move also risks losing staff with local knowledge, if these staff members are not eligible for security clearance. More direct communication from the national security community would already be achievable without enhanced security clearances.

Making the most of the STN to achieve national security objectives also comes at the risk of securitising the domain of ST&I, which can close the door to further engagement.[121] Moreover, there is a lack of standardised reporting, combined with the perception that SIN does not sufficiently fulfil its 'inform[ative]' mission, nor does it sufficiently report back to UK stakeholders (including stakeholders in the national security community).[122] Enhancing STN officers' duty to collect relevant information to national security may, however, not always fall within the skillset of STN officers, particularly when they are nationals of the host country or are uncomfortable with being associated with national security matters. Obtaining information on technology investment may also fall within the expertise of local DBT staff.[123]

The STN can only be leveraged more effectively for national security considerations if there is a clear 'demand signal' from the national security community. A demand signal is needed to assess whether increasing the number of national security objectives requires formal or informal changes to ways of working, such as sponsoring security clearances, or informal communication about those technologies that should receive greater focus. Closer exchange between the national security community and the STN's hosting departments – the FCDO and DSIT – is necessary to assess which risks in securitising science and innovation may be worth taking to fulfil essential UK missions.

120. Interview with participant P21, London, 14 January 2025.
121. Interview with participant P37, online, 19 February 2025.
122. Interview with participant P21, London, 14 January 2025.
123. Interview with participant P41, online, 21 January 2025.

The UK's Leading Role in AI Safety and Technical Standard Setting

The interview data confirmed that the UK is internationally recognised as a thought leader on AI safety, evaluation and assurance.[124] Several initiatives in the public domain, including the AI Safety Summit and the strong track record of the AISI, conduct and fund work on AI safety and standards. In addition, the AI Standards Hub has also contributed to the UK's body of work on the topic.[125] One participant explicitly credited Rishi Sunak and the AI Safety Summit for putting the UK on the international AI agenda.[126]

Nevertheless, several participants stressed that the UK needs to enhance its efforts on technical standard setting, especially within international technology standard bodies,[127] where the UK 'had fallen behind in presence'.[128] The UK's efforts were seen as falling short especially compared with China's, a country which 'has done very well on … standards'.[129] The call for greater UK and Western involvement in technical standard setting has been raised publicly for a number of years – pointing both to the link between technical standards and national security considerations,[130] as well as to China's success in enhancing its presence in technical standard bodies, especially the International Telecommunications Union (ITU).[131] One participant considered technical standard setting as a critical tool to avoid the adversary outpacing the UK in securing strategic advantage from disruptive technologies.[132] However, participants offered little details as to what 'maximising our capability' [133] or securing strategic advantage in the standards space could look like.

This broader perception that the UK is positioned as an international leader in AI safety, evaluation and assurance was challenged by experts specifically working in the standards space. They painted a different picture than other participants, stating that

124. Interview with participant P24, online, 24 January 2025; interview with participant P34, online, 11 February 2025.
125. Interview with participant P51, online, 6 March 2025.
126. Interview with participant P34, online, 11 February 2025.
127. Interview with participant P27, online, 30 January 2025.
128. Interview with participant P24, online, 24 January 2025.
129. Interview with participant P3, online, 26 June 2024.
130. Dan Geer and Paul Rosenzweig, 'Importance of Standards to National Security', Lawfare, 6 February 2023, <https://www.lawfaremedia.org/article/importance-of-standards-to-national-security>, accessed 28 March 2025.
131. Brett Schaefer and Danielle Pletka, 'Countering China's Growing Influence at the International Telecommunication Union', *Heritage Foundation*, 7 March 2022, <https://www.heritage.org/global-politics/report/countering-chinas-growing-influence-the-international-telecommunication>, accessed 28 September 2025; Riccardo Nanni, 'China, Internet Governance, and the Liberal International Order', in Riccardo Nanni, *Rising China and Internet Governance* (Singapore: Palgrave Macmillan, 2024).
132. Interview with participant P31, online, 7 February 2025.
133. Interview with participant P29, online, 3 February 2025.

the UK is already 'punching above its weight'. It has strong participation in standards study groups, significant thought leadership in the space – especially given its limited technology-producing capacity – and is supported by the work of the National Cyber Security Centre (NCSC).[134] Another expert noted that 'the UK has been doing well, trying to drive engagement in AI standards', for example through the AI Standards Hub, or through workshops at the Alan Turing Institute, which tests draft standards.[135] The same expert added that the national security implications of Chinese influence in standard setting are 'hyped and overplayed' and primarily focused on 5G and internet governance questions. China does have the capacity to push people who favour its interests into the ITU. However, the processes in more relevant standard-setting bodies, such as the International Organization for Standardization (ISO), were considered 'harder to manipulate',[136] and these venues were more relevant to technologies such as AI. While there are certain measures which China has taken to enable other actors to participate, such as providing grants for standard proposals, Europe remains aligned and maintains critical voting power.

It is therefore critical that the UK maintains its strong position and leverages it in the future. This will show leadership among European and other allies, encouraging them to actively participate and resource relevant engagements. It is important to note that UK presence is strong overall but takes place in a very male-dominated field. In addition, it is primarily large, private sector companies which can afford to resource their engagement with these bodies. Greater diversity could be achieved by including more academics or civil society members as well as advocating for more women participants.

Finally, the AISI is a critical player in this space, benefitting from considerably more funding than other actors. It is important that the AISI is integrated in the UK's established standards ecosystem to ensure a strategic, coordinated approach that effectively leverages the AISI's funding.[137]

134. Interview with participant P46, online, 4 March 2025.
135. Interview with participant P34, online, 11 February 2025.
136. *Ibid.*
137. *Ibid.*

III. The UK as an Academic Powerhouse

The UK's Historic Strength in Academic Research

The UK's academic sector is a core national asset, recognised internationally for its exceptional academic institutions and contributions to global research. This foundational excellence is recognised in quantitative global measures, such as the 2024 Times Higher Education World University Rankings, in which UK universities occupy three of the top 10 spots. The University of Oxford notably holds the number one ranking.[138] High numbers of research outputs also contribute to the UK's strength in this domain. While representing only 0.9% of the global population, the UK produced over 16% of the world's top 10% most cited publications.[139] The academic community is also immensely collaborative, producing many co-authored publications in countries such as the US, China and Germany.[140] Participants confirmed that these quantitative findings applied to the ST&I ecosystem, agreeing that academia represents a core strength of the UK's approach to ST&I.[141] Participants cited 'world-class universities',[142] 'a substantial science and research base',[143] the fact that the UK 'competes effectively

138. Times Higher Education, 'World University Rankings 2024', <https://www.timeshighereducation.com/world-university-rankings/2024/world-ranking>, accessed 28 March 2025.
139. Universities UK, 'International Facts and Figures 2023', 3 March 2025, <https://www.universitiesuk.ac.uk/universities-uk-international/insights-and-publications/uuki-publications/international-facts-and-figures-2023>, accessed 28 March 2025.
140. Rachael Pells, 'Global Co-Authors on More than Half of French and UK Research', Times Higher Education, <https://www.timeshighereducation.com/news/global-co-authors-more-half-french-and-uk-research>, accessed 28 March 2025.
141. Interview with participant P4, online, 1 July 2024; interview with participant P5, online, 3 July 2024; interview with participant P7, online, 7 April 2024; interview with participant P8, online, 7 April 2024; interview with participant P10, online, 7 December 2024; interview with participant P18, London, 12 November 2024; interview with participant P21, London, 14 January 2025; interview with participant P22, online, 23 January 2025; interview with participant P23, online, 23 January 2025.
142. Interview with participant P22, online, 23 January 2025.
143. Interview with participant P7, online, 7 April 2024.

globally',[144] conducts 'large collaboration on international papers',[145] and has a positive academic culture.

Current Academic Strength under Pressure from Funding and Skills Gaps

The UK's current academic strength should not be taken for granted. Recent funding difficulties in the higher education sector threaten to undermine the historic success of the UK's academic reputation. Spending per student across the higher education sector has decreased by 18% in real terms since 2012.[146] Domestic students have been facing their own financial difficulties due to a real-term reduction in their maintenance loans and a parental earning threshold freeze.[147] British universities are also crucially dependent on international student tuition fees, which represented 23% of income for UK universities in 2023,[148] marking a rise from only 5% in the 1990s. This dependence was flagged by interviewees as a large risk to the success of ST&I in British academia.[149] Interviewees stressed that maintaining this academic strength will be essential to long-term growth and prosperity in a future geared towards ST&I, and highlighted this as a key area of development.

It is widely assessed that there is a shortage of STEM talent within the UK.[150] However, a more nuanced description of the difficulties facing STEM fields is that there is a 'mismatch' of skills between the UK's STEM talent and the available roles in industry.[151] This mismatch manifests itself in a high amount of top-level S&T talent graduating from UK universities at the postgraduate level, and a lack of top-level jobs in the UK requiring such expertise. Vacancies for technician roles in STEM and other roles with fewer qualification requirements remain unfilled. Moreover, the gender disparity of

144. *Ibid.*
145. Interview with participant P8, online, 7 April 2024.
146. Joe Lewis and Paul Bolton, 'Higher Education Funding: Trends and Challenges', House of Commons Library Briefing Paper, 16 July 2024, <https://commonslibrary.parliament.uk/higher-education-funding-trends-and-challenges/>, accessed 28 March 2025.
147. Elaine Drayton et al., *Annual Report on Education Spending in England: 2023* (London: Institute for Fiscal Studies, 2023).
148. Lewis and Bolton, 'Higher Education Funding'.
149. Interview with participant P4, online, 1 July 2024; Interview with participant P10, online, 7 December 2024.
150. Centre for British Progress, 'AI Industrial Strategy: A Plan for "Intelligence Too Cheap to Meter"', 15 October 2024, <https://britishprogress.org/reports/ai-industrial-strategy-a-plan-for-intelligence-too>, accessed 28 March 2025.
151. National Audit Office, *Delivering STEM (Science, Technology, Engineering and Mathematics) Skills for the Economy* (London, 2018), p. 7.

talent within these roles is still considerably high.[152] Interviewees deemed the ability to provide 'home grown' talent to be fundamental[153] for the development of sovereign capabilities in ST&I. A more strategic approach from the UK government is needed to ensure that talent at all levels is being fostered for roles across STEM – beyond the recruitment of PhD researchers and early career researchers. This would maximise the talent pool already present in the UK. From an academic perspective, international talent is also important, and talented candidates should arguably be incentivised to work and live in the UK. To draw talent into the higher education environment, some interviewees suggested affordable childcare and affordable housing.[154]

More generally, there is a broader need to encourage diversity within STEM subjects to attract a larger and more varied talent pool. One participant noted generally positive movements in equality, diversity and inclusion (EDI) within STEM subjects and the UK innovation ecosystem.[155] However, such EDI initiatives were mainly attributed to the UK government and the public sector's work in innovation, and do not reflect progress across other sectors in the ecosystem. One participant also expressed frustration with the speed of change of EDI in the academic sector and mentioned a lack of diverse representation in STEM subjects, an issue that should be addressed to maximise the domestic talent available to the UK.[156] A successful strategy would encourage diversity of thought for solving complex problems, such as gaining strategic advantage from disruptive technologies. Interviewees stressed the need to 'get rid of homogenous teams. Hire diverse people',[157] and added that 'if people are excluded, you are statistically missing out on talent'.[158] Improvement in this area should be prioritised across both public and academic sectors. Such prioritisation of EDI should include a focus on socio-economic diversity,[159] as well as racial and gender diversity.[160] Most participants were reluctant to comment strongly one way or another on EDI performance, but it is worth noting that despite the beneficial work attributed to the public sector noted above, one public sector interviewee went as far as to say 'it is terrible. Everyone is a white man'.[161]

152. Centre for British Progress, 'AI Industrial Strategy'; University of Oxford, 'Annual Admissions Statistical Report 2023', May 2023, p. 20, <https://www.ox.ac.uk/sites/files/oxford/AnnualAdmissionsStatisticalReport2023b.pdf>, accessed 28 March 2025.
153. Interview with participant P19, online, 6 December 2024; interview with participant P2, online, 17 June 2024.
154. Interview with participant P8, online, 7 April 2024.
155. *Ibid.*
156. Interview with participant P11, online, 15 July 2024.
157. Interview with participant P32, online, 4 February 2025.
158. Interview with participant P8, online, 7 April 2024.
159. John Van Reenen, 'Lost Einsteins: Who Becomes an Inventor in America?', *Centre for Economic Performance*, Spring 2018, <https://cep.lse.ac.uk/pubs/download/cp522.pdf>, accessed 12 June 2025.
160. Christina Palmer, 'Risk Perception: Another Look at the "White Male" Effect', *Health, Risk & Society* (Vol. 5, No. 1, 2003), pp. 71–83.
161. Interview with participant P32, online, 4 February 2025.

Tackling National Security Concerns in Scientific Collaboration

Academics and the national security community tend to have diverging assessments of international collaboration. Interviewees disagreed on approaches to international collaboration and the admittance of international students from 'high-risk' states. Members of the national security community also perceived a lack of understanding from the academic community on the risk of IP theft. To numerous academics, international collaborations with Chinese, Russian and other international scientists and technologists resulted in valuable partnerships.[162] To some, the benefits of such partnerships outweigh the national security arguments in favour of limiting these. One participant from academia even noted that 'anything that is being stolen from [a] UK lab will be printed in a year's time anyway',[163] and that the concern about espionage was overblown.

However, to the national security community, these relationships and collaborations are indeed considered high risk, especially for UK IP and 'pure research' – the latter is research that has not yet been applied in a particular context. The national security community warned about potential espionage and theft of valuable UK assets.[164] Nonetheless, several participants from both inside and outside the national security community agreed that there needed to be a stronger focus on the security of early research or pure research, particularly in the case of innovative science or technology with dual-use capabilities. Moreover, participants agreed that the potential misuse of such technologies should be better understood by academics.[165] Some directly emphasised that universities 'are harder than ever to secure',[166] and that 'you need to incentivise security at the beginning of the cycle'.[167]

Despite a rising awareness of the criticality of securing research in the academic community, it remains a challenge to implement these considerations, given the stark cultural differences between the national security community and the academic sector.[168] Participants underlined how there is little incentive for academia to consider national security concerns more broadly in their pure research. Measures enforced by the national security community – such as the National Security and Investment Act

162. Interview with participant P8, online, 7 April 2024.
163. *Ibid.*
164. Interview with participant P2, online, 17 June 2024.
165. Interview with participant P3, online, 26 June 2024; interview with participant P4, online, 1 July 2024; interview with participant P32, online, 4 February 2025.
166. Interview with participant P32, online, 4 February 2025.
167. Interview with participant P3, online, 26 June 2024.
168. Neil Ashdown and Natasha Buckley, 'Securing Innovation in an Epoch of Geopolitical Competition', *RUSI Commentary*, 4 September 2024, <https://rusi.org/explore-our-research/publications/commentary/securing-innovation-epoch-geopolitical-competition>, accessed 28 March 2025.

(NSIA) and export control responsibilities – are operationally difficult to deliver and restrict the academic culture of collaboration for international research outputs.[169] The NSIA, for example, imposes significant administrative and operational challenges on universities. Universities need adequate support to comply with their responsibilities under the NSIA, otherwise the legislation risks imposing a chilling effect on research and innovation.[170] There is a risk that the national security community assumes that academics take into account security considerations and prioritise these over a number of other competing factors that determine research partnerships. However, this assumption is not warranted in light of the limited level of national security considerations currently communicated to academics (who do not hold the same information as members of the national security community) to prioritise these considerations over others.. That is, it may not be obvious to an academic that the technology in question is a dual-use technology of relevance to national security.[171] Moreover, the national security community may be aware of such relevance, but may not inform those in the academic sector of such use cases. Such situations might arise due to a lack of established channels of communication, or because of classification concerns. Conversely, there may be a similar lack of communication from the academic side. The national security community might be unaware of pure research occurring at the forefront of ST&I through international collaborations, and of the potential dual-use technologies already being developed in countries deemed high-risk from a national security perspective.

The UK is not alone in struggling with these considerations; experts on the Dutch innovation ecosystem discussed similar issues between the academic and national security community in the Netherlands.[172] A significant amount of work has been undertaken in the Netherlands to reframe the secure research narrative, thereby highlighting the commercial, industrial and competitive opportunities available to the academic sector.[173] Germany[174] and Estonia[175] have also been grappling with the impact of securing research in the field of emerging technologies. German policymakers reportedly see value in the UK's ability to communicate with its academic sector through teams such as Research Collaboration Advice Team (RCAT),[176] which is run out of DSIT. It should be noted, however, that the UK participants interviewed for the

169. Interview with participant P9, online, 7 April 2024.
170. Interview with participant P9, online, 4 July 2025.
171. Interview with participant P47, online, 4 March 2025.
172. Interview with participant P37, online, 19 February 2025; interview with participant P38, online, 19 February 2025.
173. *Ibid*.
174. Interview with participant P41, online, 21 February 2025.
175. Interview with participant P43, online, 3 March 2025.
176. Department for Science, Innovation and Technology, 'Research Collaboration Advice Team (RCAT)', <https://www.gov.uk/government/organisations/research-collaboration-advice-team>, accessed 28 March 2025.

research for this paper spoke about the relatively small size of the RCAT and how difficult it is to contact it, even though it was a valuable resource.[177]

It was clear from interviews of UK participants that there is a tension between some national security priorities and the academic culture of collaboration. Much of this tension is based on a lack of mutual understanding of each party's motivations – both in terms of academics requiring more knowledge of national security considerations, but also the national security community's limited understanding of how academic and scientific collaboration fosters innovation. An opportunity therefore remains to improve the communication between the national security and academic communities, and to learn from international practices.

Translating Academic Success into Industrial Strength

The UK struggles to pull early research through to fully developed commercialisation, despite having a generally thriving start-up ecosystem. This was one key finding that was stressed by numerous participants, and which must be addressed from an academic perspective.[178] The lack of success in this area was generally deemed a weakness in the ST&I ecosystem.

One possible explanation for this shortcoming is the academic community's lack of commercial awareness and its lack of access to funding. The Industrial Strategy Challenge Fund was an example of a successful funding pot to encourage the commercialisation of innovative research,[179] but it was rarely mentioned by interviewed academics. Interviewees instead noted that UKRI funding, including Innovate UK funding, focuses more on impact than commercialisation.[180] Academics more often discussed a lack of funding opportunities for scaling up early innovation, a lack of access to international research funding from within the UK,[181] and the enticing opportunities to sell products or early stage businesses to international investors and subsequently leave the UK.[182] These issues are covered further in Chapter IV.

177. Interview with participant P21, London, 14 January 2025.
178. Interview with participant P8, online, 7 April 2024; interview with participant P9, online, 7 April 2024; interview with participant P24, online, 24 January 2025; interview with participant P26, online, 30 January 2025.
179. UK Research and Innovation, 'Industrial Strategy Challenge Fund: Process Evaluation Report', 15 September 2023, <https://www.ukri.org/publications/industrial-strategy-challenge-fund-process-evaluation-report/>, accessed 28 March 2025.
180. Interview with participant P30, online, 7 February 2025.
181. Interview with participant P4, online, 1 July 2024.
182. Interview with participant P24, online, 24 January 2025.

Such discussions on funding respond to another concern expressed by some participants: the retention of research talent within academia,[183] due to the prolific ST&I VC funding available from other states (particularly from the US). It is important to ensure that the UK is an attractive place to work and live for researchers and academics. An opportunity exists to encourage commercialisation of early research within academia and to foster a funding environment which supports academics to spinout early, encourages innovative research and creates economically viable businesses within the UK.

The UK is not alone in its concerns over funding and retention of talent; an expert on the German innovation ecosystem expressed the same concerns, particularly for AI technologies. The expert explained that while early talent is readily available, talented researchers often move to the US to seek VC funding when it comes to spinning out the research into commercial viability.[184] Experts on the Dutch ecosystem noted that academic institutions in the Netherlands, like those in the UK, struggle with funding cuts, but highlighted that the Netherlands can taking advantage of European funding.[185]

To conclude this analysis of academic considerations, it should be noted that when conducting desk-based research in this space, there was a distinct lack of academic literature reflecting critically on the strengths and weaknesses of academia's role in ST&I in the UK and the subsequent implications for the UK's position in the global race for technology. The existing literature especially fails to evaluate the successful transition from research to innovation. This gap in the literature must be filled.

183. Interview with participant P23, online, 23 January 2025; interview with participant P9, online, 7 April 2024.
184. Interview with participant P41, online, 21 February 2025.
185. Interview with participant P37, online, 19 February 2025; interview with participant P38, online, 19 February 2025.

IV. Leveraging Public–Private Partnerships for Strategic Advantage

PPPs are a critical mechanism for fostering innovation in ST&I and a key aspect for gaining strategic advantage from disruptive technologies. Several studies highlight the potential of PPPs to drive technological advancements by facilitating risk sharing, enhancing resource mobilisation and using public procurement as a strategic tool.[186] There is, however, an ongoing debate on their effectiveness in promoting ST&I innovation. Some scholars argue that PPPs create an environment conducive to technological breakthroughs by combining public funding with private sector expertise,[187] whereas others suggest that contractual rigidities and market failures can limit their transformative impact.[188]

Based on data collected throughout the research, this chapter explores the relationships between the UK government and the private sector in the UK ST&I ecosystem. This section argues that PPPs need to be better leveraged for national security advantage through disruptive technologies, for example by enhancing funds for government to send a signal to the private sector when investing in key technologies. Communication can also be improved, through an increased use of problem books or by ensuring that relevant private sector partners have adequate security clearances.

186. Jakob Edler and Luke Georghiou, 'Public Procurement and Innovation – Resurrecting the Demand Side', *Research Policy* (Vol. 36, No. 7, 2007), pp. 949–63; Nunzia Carbonara and Roberta Pellegrino, 'The Role of Public Private Partnerships in Fostering Innovation', *Construction Management and Economics* (Vol. 38, No. 2, 2020), pp. 140–56.
187. Jens K Roehrich, Michael A Lewis and Gerard George, 'Are Public–Private Partnerships a Healthy Option? A Systematic Literature Review', *Social Science & Medicine* (Vol. 113, July 2014), pp. 110–19.
188. Annalisa Caloffi et al., 'Public–Private Partnerships and Beyond: Potential for Innovation and Sustainable Development', *Environment and Planning C: Politics and Space* (Vol. 35, No. 5, 2017), pp. 739–45.

The Ecosystem and the Broader Context

A fundamental tension exists between the terminology of 'strategic advantage' and the focus of the Labour leadership on 'economic growth' for private industry actors. When developing a technology to achieve a strategic advantage in security, there is a perception that such technology needs to be 'controlled', notably through export controls. Such measures restrict to whom a product can be sold, and are therefore in tension with the objective of economic growth. This tension was frequently underlined at the December 2024 roundtable event that was organised for this project. Numerous private industry participants[189] suggested that there was an appetite to build and innovate in line with national security missions. However, they highlighted how restrictions placed on board members or directors of small companies who are British citizens – as well as issues with security clearances – often stand in the way of a company choosing to develop a product as a sovereign capability and remain funded in the UK. A company may instead explore international funding options.[190] Participants from other sectors also identified this difficulty of contributing to national security priorities, due to the rigour and bureaucracy of clearance processes.[191] In addition, the national security community lacks clarity in communicating which technologies it considers strategically important.[192] There is consensus within industry that top-down messaging is crucial: on which technological capabilities should be considered a national capability and which can be commoditised and outsourced. The NSIA only achieves this in a limited manner.

Similarly, participants noted that several private companies currently take a mission-based approach within the UK, and a number of their directors have a security clearance to enable greater cooperation with the national security community. Yet, mission-based technologies require trusted capital to scale. It was clear from participants at the roundtable that there was a lack of trusted international investment in the UK, and a lack of understanding of how to achieve this trusted funding.[193] There was also discussion on the current volatility of geopolitical relationships, and participants noted that it would be beneficial for the national security community to clearly signal which international markets would be considered trusted sources of investment.[194]

189. Participants at a private sector roundtable, London, 12 December 2024.
190. Participants at a private sector roundtable, London, 12 December 2024.
191. Interview with participant P48, online, 5 March 2025; interview with participant P49, online, 5 March 2025.
192. Participants at a private sector roundtable London, 12 December 2024.
193. Participants at a private sector roundtable, London, 12 December 2024.
194. Participants at a private sector roundtable, London, 12 December 2024.

The tension between securing strategic advantage and achieving economic growth, combined with the lack of clarity from the national security community, also exists against a backdrop of British dependency on Big Tech companies.[195] Interviewees noted that entire technological sectors can be dominated by single large players.[196] This dependence naturally applies to all states. The US has recently demonstrated a conflation of technology priorities with national security priorities: for example, when the US Department of Commerce banned the Chinese AI app DeepSeek from government devices,[197] and with representatives of Big Tech companies joining and shaping national security conversations.[198] In the UK, the entrepreneur and serving chair of ARIA, Matt Clifford, formulated recommendations for the UK AI Action Plan,[199] showing that Big Tech was increasingly included in policy conversations. Another noteworthy example of political engagement with disruptive technologies was the recent memorandum of understanding signed between the UK government and Anthropic[200] – an AI safety and research company best known for developing the Claude AI models – confirming a rising dependence on Big Tech more broadly. It is important for the UK government to ensure effective oversight of these developing dependencies and to make use of the appropriate levers.

The UK Government as an Early Customer and the Private Sector's Relationship with the National Security Community

Interviewees for this paper highlighted the value of having the UK government (including the MoD and the intelligence community) as a customer of first resort, to strengthen the partnership between industry and the government.[201] UK government investment through national security and defence departments – in even modest funding pots – is an invaluable signal to markets on the prioritisation of technology

195. Interview with participant P2, online,17 June 2024; interview with participant P30, online, 7 February 2025.
196. Interview with participant P2, online,17 June 2024.
197. James Rundle, 'New York State Bans DeepSeek From Government Devices', *Wall Street Journal*, 10 February 2025, <https://www.wsj.com/articles/new-york-state-bans-deepseek-from-government-devices-de7a9df4>, accessed 28 March 2025.
198. Erin Banco, 'Elon Musk Visits US National Security Agency Amid Ongoing DOGE Cuts', *Reuters*, 13 March 2025, <https://www.reuters.com/world/us/elon-musk-visits-us-national-security-agency-amid-ongoing-doge-cuts-2025-03-13/>, accessed 28 March 2025.
199. Department for Science, Innovation and Technology (DSIT), *AI Opportunities Action Plan*, CP 1241 (London: The Stationery Office, 2025).
200. DSIT, 'Memorandum of Understanding Between the UK and Anthropic on AI Opportunities', 14 February 2025, <https://www.gov.uk/government/publications/memorandum-of-understanding-between-the-uk-and-anthropic-on-ai-opportunities>, accessed 28 March 2025.
201. Participants at a private sector roundtable, London, 12 December 2024; interview with participant P2, online, 17 June 2024; interview with participant P35, online, 13 February 2025.

and innovation. This subsequently allows for product testing and development. Such investment also offers credibility to technology companies that receive this. In turn, this can attract further capital from the private sector. DASA[202] and NSSIF were explicitly name-checked as two examples for successful funding mechanisms that subsequently attracted capital from the private sector.[203] These initiatives can have a significant impact on the development of technological capabilities for defence and national security, and yield benefits beyond the security community by attracting further funding or creating spillover effects for other areas of innovation.

DASA, for example, is a government organisation that is part of the MoD. It finds and funds innovative ideas to support national security and defence needs. A recent report on DASA's success shows that early government investments are a catalyst with far-reaching economic outcomes across the UK. Investments by DASA have contributed to levelling-up in different geographical areas and have supported small and medium-sized enterprises (SMEs) in generating a large improvement in gross value added.[204] The NSSIF – another success story of early government funding – is the UK government's VC arm for national security and defence technologies, and is guided by the intelligence community. Although the NSSIF was generally considered a potentially powerful mechanism, several participants agreed that its investments are spread too far across too many technologies. It was suggested that there are too many small funding opportunities and not enough 'large bets'.[205] Participants from larger companies did not always agree that the UK government could be considered as a pilot customer for new technologies coming out of established, large corporations;[206] this PPP is particularly beneficial for SMEs.

At present, a company wishing to make the most of its connections with the UK government and to learn about available funding is highly dependent on individual relationships and targeted networking.[207] In general, participants expressed positive feelings towards certain aspects of the relationship between government and the private sector, but stressed the need for a more accessible way to engage with the national security community. Members of the national security community also acknowledged that there is room for better interaction with all sectors – including with

202. Defence and Security Accelerator, 'About Us', Ministry of Defence, 2025, <https://www.gov.uk/government/organisations/defence-and-security-accelerator/about>, accessed 28 March 2025.
203. British Business Bank, 'National Security Strategic Investment Fund', <https://www.british-business-bank.co.uk/for-financial-advisors/equity-finance/national-security-strategic-investment-fund>, accessed 28 March 2025.
204. Beauhurst and Defence and Security Accelerator, 'Growth Impact Report 2025', 12 May 2025, <https://assets.publishing.service.gov.uk/media/6823094cf16c0654b1906159/12_05_25_-_DASA_Impact_Report_2025_Final.pdf>, accessed 12 June 2025.
205. Participants at a private sector roundtable, London, 12 December 2024.
206. Interview with participant P52, online, 13 March 2025; interview with participant P53, online, 13 March 2025; interview with participant P54, online, 13 March 2025; interview with participant P55, online, 13 March 2025; interview with participant P56, online, 13 March 2025.
207. Participants at a private sector roundtable, London, 12 December 2024; interview with participant P48, online 5 March 2025; interview with participant P49, online, 5 March 2025.

industry, academia and investment communities[208] – to maximise relationships and achieve strategic advantage. These individuals noted that the relationships with the private sector are generally underexploited and that a far more beneficial collaboration could be achieved.[209] There has historically been a tendency in the UK national security community to prioritise building technology 'in house', to keep it secure. However, due to technologies such as AI, collaboration with the private sector is even more important.

For public–private collaboration to work, interviewees noted that it is crucial to incentivise 'secure' thinking at the early innovation stage.[210] Currently, the biggest obstacle to taking security into account at an early stage is the lack of financial incentive to consider it over speed of development. There is therefore an opportunity to consider how to incentivise an early 'securing' of technologies, whether that is by making security an integral part of successful VC funding or by other means.

Funding Mechanisms for Maximising PPPs

One clear finding from the research conducted for this paper was understanding the challenges of bringing innovation through what is known as 'the valley of death': in other words, for innovation to reach technology readiness levels four to seven (the first 10 levels define the developmental readiness of a product). Indeed, interviewees were nearly unanimous in their agreement that industry has struggled for many years to bring technology and innovation through these technology readiness levels.[211] It is extremely difficult for start-ups to financially support the development of their product from technology readiness levels one to four (the stages of innovation and prototyping), to technology readiness levels eight to nine (operational delivery). Participants commonly used the 'valley of death' as a metaphor in this research. It should be noted that this finding was not based on a quantitative examination of various products' technical capabilities and their success (or lack thereof) within the market; it is rather a representation of the commonly used metaphor by participants in this research.

208. Interview with participant P2, online, 17 June 2024; interview with participant P3, online, 26 June 2024.
209. Interview with participant P2, online, 17 June 2024; interview with participant P35, online, 13 February 2025.
210. Interview with participant P3, online, 29 June 2024.
211. Participants at a private sector roundtable, London, 12 December 2024; interview with participant P8, online, 7 April 2024; interview with participant P26, location, 30 January 2025; interview with participant P28, online, 3 February 2025; interview with participant P48, online, 5 March 2025; interview with participant P49, online, 5 March 2025; interview with participant P52, online, 13 March 2025; interview with participant P53, online, 13 March 2025; interview with participant P54, online, 13 March 2025; Paul Ellwood, Ceri Williams and John Egan, 'Crossing the Valley of Death: Five Underlying Innovation Processes', *Technovation* (Vol. 109, 2022), pp. 102–62; Engineering the Future, 'Bridging the "Valley of Death": Improving the Commercialisation of Research', February 2012, <https://raeng.org.uk/media/gaele1fj/bridging_the_valley_of_death_improving_the_commercialisation_of_research-2012.pdf>, accessed 28 March 2025.

While the valley of death conceptualisation is useful, it may not be nuanced enough to fully convey a deeper understanding of the issues at hand.

The Small Business Innovation Research (SBIR) and Small Business Technology Transfer[212] programmes – run under the US Seed Fund – are success stories for addressing the funding challenges described above. Their framework generated enthusiasm thanks to very clear investment pathways, measuring milestones for taking a product to full technical commercialisation. They were also praised for their clarity on equity and IP ownership, and the amount of relative control that the company retains throughout the process. At the roundtable, participants held up this framework as a gold standard.[213] The existing literature on PPPs supports these findings: statistical and case study analysis of the programme found that it successfully promotes innovation and commercialisation and yields significant net social benefits.[214]

Patient investment in certain technologies in the UK appeared to address the valley of death issue, particularly with long-term, reliable public sector funding for quantum technologies and semi-conductors. This (arguably) led to success in those industries. Many participants agreed that the success of the quantum funding structures resulted from patient investment that stretched across electoral cycles.[215] Space technologies – namely the space clean-up projects,[216] which particularly lacked a customer base or appetite – were, however, cited by participants as examples of technologies where government funding was not strategically placed. Participants also noted that public funding for space technologies was generally available in small pots, which is only useful for making incremental progress. To remedy this, larger, more strategic funding pots are needed.[217] The example of undesirable space clean-up projects points to a larger question of demand. Delivering leading university research is significantly less expensive than delivering commercialised products in areas such as space. Without the pre-existing demand for the products within a market, there is a high likelihood of failure to commercialise an innovation. As mentioned earlier, strategic funding and direction given by the government is a crucial signal for demand, and the national security community should consider its responsibility for shaping market demand when communicating its strategic priorities.

212. US Small Business Administration, 'About SBIR and STTR', <https://www.sbir.gov/about>, accessed 28 March 2025.
213. Participants at a private sector roundtable, London, 12 December 2024.
214. David B Audretsch, Albert N Link and John T Scott, 'Public/Private Technology Partnerships: Evaluating SBIR-Supported Research', in Albert N Link and John T Scott (eds), *The Social Value of New Technology* (Cheltenham: Edward Elgar Publishing, 2019), pp. 264–78.
215. Participants at a private sector roundtable, London, 12 December 2024; interview with participant P2, online, 17 June 2024; interview with participant P5, online, 3 July 2024; interview with participant P31, online, 7 February 2025; interview with participant P48, online, 5 March 2025; interview with participant P49, online, 5 March 2025.
216. Participants at a private sector roundtable, London, 12 December 2024.
217. Interview with participant P53, online, 13 March 2025; interview with participant P54, online, 13 March 2025.

Generally, participants at the roundtable preferred problem-based funding calls, which offer the room to innovate and problem-solve in the UK. A favourite example given by industry participants was the NATO Innovation Fund (NIF).[218] Participants deemed the NIF to lack agility due to the bureaucracy that comes with multilateral engagement and believed that speed and agility were more readily available from UK funding pots. However, partnership with the NIF was deemed valuable, and good relationships with the initiative have been preserved.[219] The UK problem-based approach instead allows the national security community to communicate its strategic priorities and technological focus while still maintaining the required secrecy for classified information. Certain problem books are made available by the NCSC, but this method of communication should be increased across departments and institutions.

Making the Most of the UK's Spinout and Start-Up Environment

Numerous research participants across all sectors agreed that the UK has a 'phenomenal start-up environment',[220] and that early R&D in innovative start-ups is a core strength of the UK,[221] creating a positive reputation for the UK in Europe.

Experts in European innovation ecosystems said that, in Germany, the UK's risk appetite and VC culture for innovation is seen as strong, and that a particularly positive relationship between Germany and the UK exists through Innovate UK's joint funding process.[222] It was also anecdotally noted that there is a tendency for Danish start-ups to seek to move to the UK for early R&D,[223] and that in the Netherlands, the UK is seen as second only to the US in terms of its successful entrepreneurial approaches in research, start-ups and spinouts.[224] The Netherlands also values the UK's prioritisation of investment in ST&I for the future.

For all the European praise for the UK's approach to innovation and R&D, UK participants discussed a lack of experimental innovation opportunities in the UK, which are subject to stringent regulation and legislation. One participant noted that the

218. NATO Innovation Fund, 'About the NATO Innovation Fund', <https://www.nif.fund/>, accessed 28 March 2025
219. Interview with participant P35, online, 13 February 2025.
220. Interview with participant P23, online, 23 January 2025; this view was also supported by interview with participant P30, online, 7 February 2025. `
221. Participants at a private sector roundtable, London, 12 December 2024; interview with participant P2, online, 17 June 2024; interview with participant P23, online, 23 January 2025; interview with participant P26, online, 30 January 2025.
222. Interview with participant P41, online, 21 February 2025.
223. Interview with participant P40, online, 20 February 2025.
224. Interview with participant P37, online, 19 February 2025; interview with participant P38, online, 19 February 2025.

UK is 'good for doing business, not for innovation'.[225] Estonia was again held up as a strong example of how to ensure that legislation does not stifle the capacity for innovation.[226] Estonia has been dubbed the 'unicorn factory',[227] and with a population smaller than London's, it has created one unicorn for approximately every 130,000 residents. This phenomenal progress was partly attributed to Estonia's ability to undo restrictive legislation.[228] The UK has taken certain steps towards addressing regulatory restrictions to innovation through the Regulatory Innovation Office (RIO),[229] which is chaired by David Willetts through DSIT. This office was created in October 2024, so it is too early to assess the success of this initiative.

Another clear weakness of the UK's ST&I ecosystem is the regular loss of early innovators to international competitors and allies, to the detriment of commercialisation of innovation. There was also near-unanimous agreement among research participants that foreign investment in the UK is needed to keep companies within the UK. Notable examples include the commercial success stories of ARM[230] and Google's DeepMind,[231] which started as UK companies before each was sold to investors abroad. The UK therefore invests significant funding in early innovative research, only to lose these assets to other markets at the commercialisation stage.[232] An expert in Estonia's innovation ecosystem, as well as roundtable participants,[233] cited Estonia's leadership in talent retention. Estonia has indeed cultivated an employer-friendly environment through employment law that enables easy staff turnover, low tax requirements for private industry and (incidentally) through low living costs.[234]

In the future, the UK ST&I ecosystem requires a cultural change to create a higher tolerance for failure within the innovation process. Most research participants agreed

225. Interview with participant P25, online, 30 January 2025.
226. Interview with participant P43, online, 3 March 2025; participants at a private sector roundtable, London, 12 December 2024.
227. Agur Jõgi, 'Entrepreneurial Lessons from the Estonian Unicorn Factory', *Forbes*, 6 May 2024, <https://www.forbes.com/councils/forbestechcouncil/2024/05/06/entrepreneurial-lessons-from-the-estonian-unicorn-factory/>, accessed 28 March 2025.
228. Interview with participant P43, online, 3 March 2025.
229. Department for Science, Innovation and Technology, 'Game-Changing Tech to Reach the Public Faster as Dedicated New Unit Launched to Curb Red Tape', press release, 8 October 2024, <https://www.gov.uk/government/news/game-changing-tech-to-reach-the-public-faster-as-dedicated-new-unit-launched-to-curb-red-tape>, accessed 28 March 2025.
230. Leo Kelion, 'ARM: UK-Based Chip Designer Sold to US Firm Nvidia', *BBC News*, 14 September 2020.
231. Samuel Gibbs, 'Google Buys UK Artificial Intelligence Startup DeepMind for £400m', *The Guardian*, 27 January 2014.
232. Interview with participant P9, online, 7 April 2024; interview with participant P24, online, 24 January 2025; interview with participant P26, online, 30 January 2025; interview with participant P30, online, 7 February 2025; interview with participant P49, online, 5 March 2025.
233. Participants at a private sector roundtable, London, 12 December 2024; interview with participant P43, online, 3 March 2025.
234. Interview with participant P43, online, 3 March 2025.

that the UK government, the UK VC community and other funders have an extremely low appetite for risk, and that must change.[235]

IP, Equity and Patents

Unlike commercial contracts, agreements with the UK government often include strict provisions on IP ownership, licensing rights, confidentiality and export controls. Businesses must carefully assess how their existing IP will be protected, what rights the government will acquire over newly developed technologies and how security classifications or national interest clauses might limit future commercialisation. Many research participants agreed that the government should not have the rights to both equity and IP: only one or the other was considered appropriate.[236]

Research participants highlighted a current challenge: to innovate in strategic technologies, it might not be desirable to patent an idea or capability. Yet, UK VC funds and public sector funding often require at least a patent application. The existing literature currently supports the idea that patents lead to more successful funding: having a patent or a trademark leads to more positive outcomes when applying for VC funding, especially if an innovator has both.[237] However, roundtable participants instead held up the US approach as an ideal. Participants cited Elon Musk's view on patents for Space X. Musk does not believe in patents 'because the Chinese would just use them as recipe books'.[238]

This conversation on the advantages and risks of patents highlights the tension in industry between seeking investment and developing strategically useful technologies for national security priorities, which can add obstacles to receiving such financial investment. Research participants from businesses of all sizes unanimously agreed that the current UK government funding opportunities are punitive for smaller companies.[239] Liabilities and tax responsibilities linked to this funding make the

235. Participants at a private sector roundtable, London, 12 December 2024; interview with participant P26, online, 30 January 2025; interview with participant P52, online, 13 March 2025; interview with participant P54, online, 13 March 2025; interview with participant P55, online, 13 March 2025; interview with participant P56, online, 13 March 2025.
236. Participants at a private sector roundtable, London, 12 December 2024; interview with participant P26, online, 30 January 2025; interview with participant P52, online, 13 March 2025; interview with participant P54, online, 13 March 2025; interview with participant P55, online, 13 March 2025; interview with participant P56, online, 13 March 2025.
237. Haibo Zhou et al., 'Patents, Trademarks, and Their Complementarity in Venture Capital Funding', *Technovation* (Vol. 47, 2016), pp. 14–22.
238. Participants at a private sector roundtable, London, 12 December 2024. See also Kim Bhasin, 'Elon Musk: "If We Published Patents, It Would be Farcical"', *Business Insider*, 9 November 2012, <https://www.businessinsider.com/elon-musk-patents-2012-11>, accessed 15 September 2025. Michael Heller and James Salzman, 'Elon Musk Doesn't Care About Patents. Should You?', *Harvard Business Review*, 4 March 2021, <https://hbr.org/2021/03/elon-musk-doesnt-care-about-patents-should-you>, accessed 28 March 2025.
239. Participants at a private sector roundtable, London, 12 December 2024.

funding less appealing than it should be, and do not provide a secure level of base funding. To improve in this area, the national security community should clearly communicate which technologies are of strategic interest, in an open and accessible way. Furthermore, the UK government should offer clarity on the allocation of equity and IP, while allowing companies to maintain an element of control over both.

V. Policy Recommendations

This chapter sets out several policy recommendations designed to strengthen the UK government's approach to securing a strategic advantage from disruptive technologies. These recommendations are based on the data collected for this paper, and feed into three priority areas that the data suggests the UK government should focus on over the next three to five years.

Recommendations

- **The UK should maintain existing assets**. This research confirmed that the UK has core strengths that contribute to its current position in the global race for technology. These strengths include a world-leading academic sector and thought leadership in tech diplomacy and standard setting. These assets must not be taken for granted and must be protected in a competitive funding environment, for example through strategic, patient funding which allows academia to attract world-leading talent.[240]
- **Increased transparency and strategic input from the national security community are necessary**. Although general awareness of the overlap between technology and national security concerns is growing, the wider UK ST&I ecosystem requires greater strategic direction from the national security community – otherwise national security will remain one consideration among many. Despite ongoing efforts for interaction, this research found that the national security community still needs to enhance its interactions with other stakeholders in the tech ecosystem to communicate its priorities. This includes communication with UK government partners, academic researchers and the private sector, for example by publishing problem books and by delivering strategic investments. This input must contribute to narrowing down UK areas of focus while retaining strategic national security priorities.

240. Interview with participant P1, online, 19 April 2024.

- **Scaling up early success can bring wider economic, strategic and societal benefits.** The UK has a strong track record at early stages of the development cycle, for example with respect to early (academic) research, attracting talent at university level or launching start-ups. The challenge remains pulling through early research[241] and scaling up these start-ups while retaining talent and companies, so these companies can grow and secure strategic, economic and societal advantages for the UK. This requires a combination of many factors, including an innovation and business-friendly regulatory landscape, strong infrastructure, sufficient scale-up capital and an attractive quality of life for top talent. This research confirms that strategic government investment can send a strong market signal but recognises that working with international partners is key to securing more trusted capital.

The complexity of the priority areas and the need to balance competing economic, technical and national security considerations means there is no 'low hanging fruit' for policymakers. Many measures enacted over the past three to five years are in their early stages and conclusive assessments are often not yet possible. Many other countries experience similar challenges, such as the limitation of VC or the need to protect a strong academic sector, but do not necessarily provide clear best practices that can be easily replicated. The following sections provide policy recommendations to guide UK priorities in this complex field and identifies levers that constitute useful starting points for further research.

Cross-Sectoral and Governmental Approaches, Embedded in Tailored Strategies

Enhancing Cross-Governmental Coordination

The UK government currently runs several promising initiatives and workstreams to enhance the UK's track record on disruptive technologies, including in and for national security. A considerable number of these initiatives and workstreams have been launched in the past two to three years. This research shows that coordination across these workstreams and across departments remains unsystematic and requires greater streamlining and cross-pollination.[242] Cross-collaboration across government initiatives can always be improved, but there are challenges unique to the intersection of technology and national security. This is partially due to national security involvement – which many criticised as not joined-up with wider efforts[243] – and, more generally, because technology competences are divided across government and the

241. Interview with participant P1, online, 19 April 2024.
242. Interview with participant P28, online, 3 February 2025; interview with participant P35, online, 13 February 2025.
243. Interview with participant P33, online, 11 February 2025.

civil service.[244] Launching additional initiatives in this domain will not be beneficial if these are not properly integrated within existing projects that would benefit from greater funding or collaboration.

NSTIx was tasked with coordinating and facilitating cross-government engagements on national security, technology and innovation. Its closure in January 2025 came as a surprise to many, and at the time of writing, it is unclear which agency is taking over its tasks. It remains essential to facilitate greater coordination across government, especially for integrating national security considerations across departments.

- **NSTIx's functions need to be reviewed and reallocated**. These tasks need to be taken on by individuals and/or by offices that can lead cross-governmental and sectoral efforts through charismatic leadership and a suitable mandate.
- **'Champions' of cross-government efforts need to be empowered**. Champions can be empowered by broad and adequate mandates to meaningfully enable their work. For example, where a champion seeks to encourage collaboration across departments, they would require a mandate that allows them to impose budgetary consequences when certain government departments lack coordination. These champions are rare and must be specifically recruited and empowered where possible.
- **Informal coordination efforts need adequate recognition and support**. Support can come via formalising coordination efforts to make them less vulnerable to staff turnover, and by giving individuals allocated time in their schedule. This includes organising meetings across funders of technologies relevant to national security, such as DASA, the NSSIF and the DBT.
- **Government should ensure each technology cluster has a multistakeholder, independent advisory board and function**. Certain technology clusters in the UK already have an independent advisory board or function, namely the Bio Security Leadership Council (now the Engineering Biology Responsible Innovation Advisory Panel) and the National Quantum Computing Centre. This paper has confirmed the value of these clusters but has also identified technology clusters that are missing cross-sectoral functions, including the telecoms sector. Although the telecoms sector previously had an advisory board on vendor diversification, it was limited to this specific topic and subsequently closed under the new Labour government. A new advisory board should have broader competencies beyond vendor diversification.
- **Learning and upskilling with insights taken from different stakeholders in the ST&I ecosystem is vital**. This paper confirmed the overwhelming interest that UK civil servants and government departments have in enhancing UK ST&I for national security and broader society. However, the conversations in the context of this project – and not just with policymakers – often remained superficial, with participants having a limited understanding of the interplay and differences between areas of work such as science, early research, commercialisation and

244. Interview with participant P29, online, 3 February 2025.

innovation. This is not just a question of terminology; it illustrates the need for a more in-depth, evidence-based understanding for policymakers. When policymakers understand how their portfolio interlinks with other elements of the ST&I ecosystem, they will be able to optimise the policy levers at their disposal.

Updating Technology Strategies to Ensure Practical Focus and Input from the National Security Community

Current technology strategies in the UK received mixed reviews in the research for this paper. While the quantum strategy was generally seen as a good example of national security integration, others were lacking such input. Most strategies were seen as being too vague, and did not identify clear priority technologies, consider the intersections of technologies or tackle the challenge of scaling up technologies (rather than providing additional research funding). This research finds that the UK needs to concentrate its technology efforts and double down on existing strengths while exerting minimal effort in areas of weakness (in weak areas, it can partner with others).[245] The national security community must clearly set these strategies.

- **Updated national technology strategies need greater national security input**. This is crucial to identifying strategically important use cases for certain technologies, to indicate which technologies may have a first customer in government, and to outline where patient funding for technologies can offer strategic rewards in return.
- **Updated national technology strategies must include a greater focus on implementation, notably by identifying departments responsible for implementation and identifying which specific technologies or use cases take priority, and those that do not**. Previous strategies set out grand ambitions for UK technology clusters but lacked specificity to guide those in the tech ecosystem.[246] The Netherlands' approach was identified as exemplary in setting out strategies that explicitly identify areas that are not a priority and recognise the importance of technology intersections.[247]
- **Updated strategies and policies should make a sharper distinction between achieving a national advantage through R&D, commercialisation and/or adoption**. This would provide greater clarity for how strategic advantage can be achieved through science and technology.
- **Strategic funding cycles, and preparation for incoming funding, are crucial**. This research project identified the importance of strategic, long-term funding cycles that span beyond electoral cycles (10+ years). However, it is important to meaningfully prepare the receivers of this funding for implementation. [248]
- **A coherent strategy and an independent advisory for the telecoms sector is necessary**. There are several national strategies addressing different aspects of the

245. Interview with participant P29, online, 3 February 2025.
246. Interview with participant P31, online, 7 February 2025.
247. Interview with participant P35, online, 13 February 2025.
248. Interview with participant P31, online, 7 February 2025.

telecoms sector, such as diversification of vendors. However, participants felt the need for a coherent approach that strategically guides the whole sector. A cross-sectoral advisory board that includes the national security community could deliver meaningful input for this strategy.

An Innovation-Friendly Regulatory Ecosystem

Ensuring the UK is an innovation-friendly economy is a key requirement for ST&I success. As it stands, the UK is perceived as business-friendly but not innovation-friendly,[249] considering administrative and regulatory hurdles.

- **Evaluate and apply lessons from the Estonian government's 'Accelerate Estonia' project to the RIO**. Learning from Estonian counterparts is a great opportunity to exchange best practice.
- **Continue the creation of, and increase the use of, innovative testing environments**. Following Brexit, the UK benefits from more regulatory freedom and should use its position to attract foreign companies to test new products.[250] To do so, the UK must improve local testing facilities and testing areas and remove the remaining regulatory hurdles to the appropriate testing of technologies.[251] Carving out this niche requires understanding how other countries have become more attractive testing environments.

Leveraging Strong International Tech Diplomacy for National Security Purposes

Maintaining the UK's Strong Position in International Tech Diplomacy and Doubling Down on Thought Leadership in AI Safety

- **The UK must continue to be an international convenor on tech diplomacy**. The UK should also continue to engage with China as far as national security considerations allow.
- **The UK must double down on its leadership on AI safety issues**. The UK's AI safety community enjoys a strong reputation and significant funding that can be leveraged to maintain and expand the UK's leadership role in this area. However, the UK needs to maintain its independence and not be dissuaded by shifting US policy. Strengthening the UK's relations with other AI safety and security institutes internationally can further build up its standing.

249. Interview with participant P25, online, 30 January 2025.
250. Interview with participant P40, online, 20 February 2025.
251. Interview with participant P25, online, 30 January 2025.

Maintaining Presence in Technical Standard Bodies and Increasing Diversity

- **The UK needs to leverage its established position in technical standard-setting bodies**. This will encourage like-minded countries to engage at a similar level and to make effective use of their collectively strong voting power – especially considering the significant resources China spends on technical standard setting.
- **The UK needs to support women and new talent in standard setting**. Encouraging greater involvement of women and next-generation technology and standards experts ensures a robust talent pipeline to maintain this established position. The work in the ITU in particular – as well as other standard-setting bodies such as the IETF, the ISO and the IEC – lacks diversity. Measures such as a network for women and engagement with female academics and technical researchers would raise awareness and interest for standard-setting work beyond the current demographics.

Feeding National Security Needs into the Restructured STN

The STN sits under the FCDO and DSIT and receives little input from the national security community. Formal measures such as standardised reporting, or increasing the number of staff who hold security clearance, can facilitate engagement with the national security community. However, these measures are not essential for a closer relationship between the STN and the national security community.

- **The national security community should increase informal engagement with STN officers and should highlight countries of particular interest or technologies that are a priority for UK national security**. This could enhance the currently limited knowledge of international best practice among the national security community. A new approach to shaping this relationship would be well timed, as it coincides with the SIN's February 2025 restructuring to include technology in its remit. The global STN meeting planned for the end of 2025 or early 2026 is a crucial opportunity for strategic national security guidance.

However, this engagement should be weighed against the risk of 'securitising' an area of work which is often considered relatively neutral, and which is currently seen as a gateway to engagement. Depending on the national security community's motivation for engaging with STN officers – including motivations such as identifying joint investment opportunities in dual-use technologies – local DBT officers may be better placed to fulfil these roles (especially where they hold security clearances). The STN, however, must be leveraged to better identify long-term investment and strategic technology priorities of partners. To this end, the STN must improve its reporting channels to the wider communities in UK government.

Learning and Benefitting from the Global Experience

- **Departments currently mapping the UK's and other countries' strengths and weaknesses on technological progress need to identify what is blocking the circulation of findings, and how they can be centrally stored and accessed by a wider ST&I community**. National security considerations need to be balanced against the need to provide this information to other stakeholders in the ecosystem who are expected to contribute to a strategic approach to enhancing the UK's technology record.[252] Stakeholders with this data can review quantitative findings against qualitative assessments. Commercial data[253] and the VC community – which often operates in several countries – are underused sources to map these ecosystems.[254]
- **Conduct targeted additional research to strengthen comparative understanding and international best practice**. Further targeted research on specific themes identified in Chapter II, or for specific countries, would add to the national security-minded ST&I community's understanding of international best practice, an understanding which currently remains highly limited. Exchange with international counterparts must be encouraged, to also identify where existing partnerships have potential for greater tech dimensions.

Retaining UK Academic Strength

Securing Academic Research

- **Existing, largely informal, softer engagements seeking to enhance national security awareness among researchers need to continue**. They should expand beyond the core universities which are already a part of the security ecosystem.
- **A larger RCAT team, which supports universities in their compliance with the NSIA, is needed**. A larger RCAT team can offer easily accessible guidance to universities seeking to comply with national security measures.
- **Greater exchange with like-minded countries about best practices for balancing academic and national security needs is critical and should be expanded to other countries**. Dialogues, such as those held via the STN, should be held periodically to review the effectiveness of measures.

Strengthening the Link Between Academia and the Start-up Scene

Existing training offers to enhance entrepreneurial mindset and skills among students remain too often focused on PhD level students, for example via doctoral training centres.[255]

252. Interview with participant P4, online, 1 July 2024. This interview referred to a greater need of resources.
253. Interview with participant P42, online, 3 March 2025.
254. Interview with participant P39, London, 19 February 2025.
255. Interview with participant P57, online, 13 March 2025.

- **To meaningfully enhance entrepreneurial mindset across the wider ST&I ecosystem, more training needs to be available before PhD level – a stage at which numerous, practice-oriented students will have already left university – but also outside the university context, to encourage upskilling at a later stage**. Moreover, such training must include investors from the VC community and experienced founders, following the example of ARIA's Activation Partners.
- **To enhance EDI in the start-up scene, workshops should be offered to improve confidence among potential founders, improve their confidence when pitching for funding and empower them to take the next step**. This should include confidence-building training for women, and pitch workshops to facilitate interactions with the finance sector, which can be an exclusionary social context.[256]

The National Security Community Needs to Speak the Language of Academics to Generate Greater Involvement

To raise national security as a prime consideration, the national security community needs to engage with greater transparency while also speaking the language of academia.

- **The use of problem books, such as the books provided by the NCSC and the MoD, should be expanded**. Problem books should be issued by all institutions within the national security community, and wider distribution should be considered, for example through the Catapult Network.[257]
- **The national security community should explore to what extent the Research Excellence Framework (REF) cycle can be used to incentivise academic behaviour**. The REF cycle is the periodic, six-year assessment of the quality and impact of research in higher education institutions. This can be done by either adapting the REF cycle to include a national security relevant component (for example, within the current 'People and Culture'[258] requirement) or by better understanding how academics can qualify for impact assessment under an ongoing REF cycle.

Scaling Up the Start-Up Scene

Funding Models for Start-Ups Should Pre-Empt and Compensate for the Common Failure in the 'Valley of Death'

The valley of death remains a common problem not just in the UK, but for many smaller economies that, unlike the US and China, do not have access to vast capital. Previous efforts to counter this phenomenon have had some, albeit limited, success. These efforts include a funding mechanism to scale up companies at this readiness level. Their limited success in countering the valley of death leaves questions as to how

256. Interview with participant P39, London, 19 February 2025.
257. Interview with participant P50, London, 6, February 2025.
258. REF2029, 'People, Culture and Environment (PCE)', <https://2029.ref.ac.uk/people-culture-and-environment-pce/>, accessed 16 September 2025.

far government funding can ever compensate for scale (and possibly a lack of demand). Since starting this project, several initiatives have specifically focused on the scaling-up challenge – primarily from an economic perspective. The ongoing House of Lords Science and Technology Committee's inquiry 'Financing and Scaling UK Science and Technology: Innovation, Investment and Industry'[259] should be highlighted. However, the public-facing elements of oral and written evidence overwhelmingly do not consider national security considerations. The Tony Blair Institute also published several policy recommendations for scaling up UK start-ups and spinouts. Although it provides a detailed analysis and a large number of policy recommendations, the report merely mentions 'national security' once, in a reference to a different paper.[260]

The national security community must expand its role in signalling demand in the market and consider how it can collaborate with other economic initiatives to improve the prospects of UK start-ups through the valley of death.[261]

- **Milestone and problem-based funding should be offered to support technologies through each development stage**. Outlining contractual 'milestones' between a company and a public funder can offer a clear path to commercialisation. Providing problem-based funding or funding with more milestones creates more payment points for companies, thereby helping to mitigate the valley of death, and ensures that both parties are held to account. One example of this type of funding is the SBIR scheme in the US.
- **Expand government funding schemes that allow the UK government and the national security community to send a strong signal as a first customer, for example, via the NSSIF**.[262] Expanding the NSSIF and similar funding mechanisms is a good way for the government to send strategic signals and ensure national security and wider economic benefits from technologies.
- **Explore the possibility of reforming procurement requirements to also include SME requirements**.[263] Procurement favours government and large defence primes, leaving SMEs reliant on operator contracts or consortiums, with risks from uncertain supply, high taxes and punitive contract terms. For SMEs to benefit from government procurement contracts, there needs to be a greater level of certainty for

259. UK Parliament, 'Financing and Scaling UK Science and Technology: Innovation, Investment, Industry', July 2025, <https://committees.parliament.uk/work/9014/financing-and-scaling-uk-science-and-technology-innovation-investment-industry/publications/>, accessed 15 September 2025.
260. Tony Blair Institute for Global Change, 'From Startup to Scaleup: Turning UK Innovation Into Prosperity and Power', 9 June 2025, <https://institute.global/insights/tech-and-digitalisation/from-startup-to-scaleup-turning-uk-innovation-into-prosperity-and-power>, accessed 15 September 2025.
261. Elvira Uyarra and Kieron Flanagan, 'Understanding the Innovation Impacts of Public Procurement', *European Planning Studies* (Vol. 18, No. 1, 2010), pp. 123–43.
262. Since writing this paper, funding for the NSSIF has increased by £330 million. See Joseph Bambridge, 'Britain's Secretive Fund for Spies Comes Out of the Shadows', *Politico*, 16 July 2025, <https://www.politico.eu/article/britain-secretive-spy-fund-out-shadows-nssif-gchq-mi5-mi6/>, accessed 15 September 2025.
263. Interview with participant P25, online, 30 January 2025; interview with participant P28, online, 3 February 2025.

smaller businesses; enacting innovation-friendly procurement can create such conditions.[264]

- **UKIC must expand catapult programmes and problem-based contracts to leverage existing links to industry, rather than forming new contracts**. Catapults in the UK offer significant cross-sectoral reach with a good representation of industry (particularly SMEs) and academia. This avenue is underused when connecting national security priorities with other sectors.
- **Understanding the cost–benefit analysis for start-ups and early innovation funding should be explored in further research**. For example, Innovate UK offers vital start-up funding, but applications are burdensome and success rates can be as low as 3%.[265] The 'smart grant' process is currently being evaluated. This should lead to a decisive understanding of UKRI's role as either a developer of technologies, or a provider of small innovative company support.

Joint and Trusted Capital Raising with International Allies

- **Understand what constitutes 'trusted' capital and how to attract it**. There is need for international investment in the UK to support the ST&I ecosystem and enhance talent retention. This investment, particularly in dual-use technologies of strategic advantage, needs to come from trusted sources. More research is needed to ascertain what constitutes trusted capital and where it can be found.
- **Options should be explored to increase availability of patient funding through research councils and government funding pots**. Investments from pension funds should also be considered,[266] and analysis should be conducted into best practices by allies.
- **The UK government should explore how international mechanisms such as the NIF can be used more effectively**. These mechanisms can increase agility and leverage the strength of joint funding, making the most of the UK's relative dexterity to compensate for bureaucratic disadvantages.

264. Interview with participant P33, online, 11 February 2025.
265. Alex Chalkley, 'Smart Grant Success Rate Drops Below 3%', Venturenomix, 13 November 2024, <https://venturenomix.com/smart-grant-success-rate-drops-below-3/>, accessed 28 March 2025; Jonny O'Rourke, 'Grant Funding Success Rates: Chances of Success in 2022', RedKnight Consultancy, 23 February 2022, <https://redknightconsultancy.co.uk/2022/02/23/grant-funding-success-rates/>, accessed 28 March 2025; TBAT Innovation, 'How Competitive is Grant Funding?', 2 September 2021,<https://tbat.co.uk/knowledge/how-competitive-is-grant-funding/>, accessed 28 March 2025; Millie Palmer, 'UK's SME Grant Scheme Paused for Evaluation', Myriad Associates, 30 January 2025, <https://www.myriadassociates.com/resources/news/uk-s-sme-grant-scheme-paused-for-evaluation/>, accessed 28 March 2025.
266. Interview with participant P26, online, 30 January 2025.

Increase Transparency on Areas of Underspending, and Clearly Communicate to Start-ups on Available Funding

- **Information about surplus funding should be easier to access**[267] **and more transparent**. It is recognised that information about surplus funding is often accessible through existing relationships with the national security community and private networking. There should be a portal through which SMEs and academia can access this information near the end of the financial year.
- **Simplified information should be available to start-ups, illustrating where there is government funding, for all development stages**. From founding to commercial development, illustrative examples of 'funding paths' should be written in a format and language that is appropriate to entrepreneurs, and not in government language. NSTIx created this type of output in the past, and it should be recreated for the audience of start-up founders and SMEs.

Making Early Stage Investments Pay Off

Commercialising and Protecting Ideas Coming from Government

Historically, sovereign tech capabilities developed from within the UK government have not always been commercialised, nor have they always benefitted their inventors.

- **Civil servants who develop IP that is patented and eventually licensed should be able to own a share of this IP.** This is a strong lever to incentivise and retain talent in the civil service. The US approach to NSA staff could serve as an example.[268]
- **Stagnant IP in government needs to be commercialised.** A lot of stagnant IP – IP which is currently not commercialised – exists in government, and its marketable value should be explored. Leveraging such IP can secure greater economic and societal benefits. The MoD already tries to leverage this IP and commercialise it via Ploughshare, primarily focusing on the Defence Science and Technology Laboratory and defence.[269] Similar mechanisms should expand to other areas of government and be coordinated by the DBT.[270] Attracting top talent IP lawyers is a key requirement for this.[271]

Equity in PPPs, an Improved Definition of IP and Keeping Start-Ups in the UK

- **Government should clarify its position on the allocation of equity and IP ownership for its private sector partners**. This can include a standardisation of contract types, a more predictable distribution of equity and IP, and ideally the full control of either equity or IP for private partners.

267. Interview with participant P25, online, 30 January 2025.
268. Interview with participant P23, online, 23 January 2025.
269. Ploughshare, <https://ploughshare.co.uk/>, accessed 28 March 2025.
270. Interview with participant P50, London, 6 February 2025.
271. Interview with participant P2, online, 17 June 2024.

- **The government should reduce patent-pending requirements for public sector funding pots**. This is particularly important for strategic technologies or desired domestic capabilities.
- **The UK government should evaluate Estonia's approach of attracting capital from abroad while maintaining headquarters and jobs in Estonia**. The UK should apply its lessons to the UK system to create economic benefit for society.

Fostering a Work-Friendly Environment in the UK

The UK has a good reputation for attracting university level talent from abroad, but this needs to also extend to postgraduate and industrial talent.

- **Ensuring available infrastructure for good work–life balance in the UK, including childcare, affordable housing and appropriate pay**. These measures must subsequently be marketed to international talent.
- **Conduct research into the factors that make UK talent move abroad**. This research should study a range of career stages, from PhD to successful commercial ventures.
- **Skilled Worker, Global Talent and postgraduate study visas should be extended to include immediate family members**. This will reduce administrative burden for incoming talent; currently, both visa processes require a separate application for every family member entering the UK, with individual visa requirements.

Conclusion and Further Considerations

The UK, like other countries, has intensified its recent efforts to develop leading, cutting-edge ST&I. Over the past three to five years, there has been an influx of government interventions, including from the UK national security community, to secure a strategic advantage from ST&I. This paper has highlighted several interventions in this area, focusing on the interaction between the national security community and the wider ST&I ecosystem.

Methodological challenges and the lack of clearly defined aims in the UK's technology policy make it difficult to assess what will make these efforts successful. While previous UK leadership set out grand ambitions for the UK to become a 'technology superpower', the current government appears to be more measured in terms of policy language in this domain, focusing instead on economic growth as a metric for success. This is generally welcome, but the ST&I ecosystem still requires greater clarity on how to balance economic growth and national security considerations. In particular, it requires clarity on what it means to secure a 'strategic advantage from disruptive technologies'.

When defining technology policy, the UK government and the national security community must clearly articulate which technology clusters and use cases constitute a priority, and which ones do not. A clear identification of priorities will help the wider ST&I ecosystem to better understand what 'securing strategic advantage' in technology means in practice. The national security community needs to contribute to this process, notably by providing input into national technology strategies, creating problem books and investing strategically in UK technology companies.

This paper has identified key assets, needs, risks and dependencies that determine the UK's international standing in this domain. Looking ahead, the UK needs to better understand its own strengths and shortcomings and identify partnership opportunities to develop tailored and implementable policies. It should also learn from other countries with similar market size and resources, since some states are currently

implementing parallel measures to achieve similar aims. Certain approaches might constitute inspiration for future UK policies.

Despite its recent push for technological advance, the UK continues to face many challenges. Larger economies – such as those of the US and China – are investing heavily in their own capabilities in an era of increased economic nationalism. This makes the UK's disadvantage in scale, resources and market share particularly stark. This research showed that the UK indeed struggles to scale up its strong start-up ecosystem and loses talent and promising companies to the international ecosystem. Further research should explore how the UK can navigate its relationship with the US in the area of disruptive technologies (both as a partner and competitor), and how the UK can attract trusted capital to ensure innovation benefits national security, the economy and society more broadly. For the UK to succeed in ST&I policy, it will have to grasp the international dimension of the technology ecosystem and strike the appropriate balance between cooperation and competition. Understanding how to better cooperate with international partners, including in Europe, Australia and Canada, will be a key lever to securing trusted capital for dual-use investments.

Finally, the UK must prioritise its efforts to gain a strategic advantage from disruptive technologies or risk stretching itself too thin. It is necessary for the national security community to provide clear strategic direction and investment for the wider ST&I ecosystem to increase the speed and scale at which technology can be developed for national security purposes. Not only does this require the national security community to articulate which technology clusters it wishes to reinforce domestically, but the national security community must also initiate a cultural change. Despite the national security community's efforts to change engagement protocols, there remain challenges to open communication and cooperation between the national security community, the private sector and academia. Without further cultural change and focused, strategic vision from the national security community, the UK will not be able to secure strategic advantage from disruptive technologies.

About the Authors

Pia Hüsch is a Research Fellow in cyber, technology and national security at RUSI. She leads RUSI's research on disruptive technologies, including on how national security and geopolitical considerations shape countries' science, tech and innovation policy.

Prior to joining RUSI, Pia conducted her doctoral research on offensive cyber operations in international law at the University of Glasgow. At RUSI, Pia researches tech policy issues (including AI policy), offensive cyber operations and cyber policy in the Indo-Pacific. Pia is a recognised expert in her field and has contributed to inquiries of the UK Foreign Affairs Committee and the UK Science and Technology Committee as well as a broad range of media outlets, including *The Economist* and *The Times*.

Natasha Buckley is a Lecturer in Cyber Security at Cranfield University and an Associate Fellow at RUSI. She is a recognised researcher in national security, emerging technologies and research security policy. Tash's work examines how technological disruption reshapes strategic, legal and institutional spaces, combining qualitative, creative and narrative-led methodologies to explore complex socio-technical systems and the evolving boundaries between technology, power and institutional identity. She has led high-level policy engagements, is a regular contributor to major think tanks and a frequent commentator on national security issues, including appearances on *BBC News*.

194 years of independent thinking on defence and security

The Royal United Services Institute (RUSI) is the world's oldest and the UK's leading defence and security think tank. Its mission is to inform, influence and enhance public debate on a safer and more stable world. RUSI is a research-led institute, producing independent, practical and innovative analysis to address today's complex challenges.

Since its foundation in 1831, RUSI has relied on its members to support its activities. Together with revenue from research, publications and conferences, RUSI has sustained its political independence for 194 years.

RUSI is registered as a charity in England and Wales

Charity number: 210639

VAT number: GB752275038