What's next for national security and research?

Alexis Brown

hepi
Higher Education Policy Institute

HEPI Report 147

About the author

Dr Alexis Brown is Director of Policy and Advocacy at HEPI. Prior to joining HEPI, she was a Policy Manager at the Russell Group, where she managed a portfolio of policy issues related to higher education, skills and funding. She holds a PhD in English Literature from the University of Oxford, where she was a Rhodes scholar.

Methodology

This report draws on interviews with 36 stakeholders directly engaged on this topic, working across 12 universities, five mission groups in the UK and Australia, as well as in the Department for Business, Energy & Industrial Strategy (BEIS), the Centre for Protection of National Infrastructure (CPNI) and UK Research and Innovation (UKRI). While those who were happy to be on the record are named, many asked to be anonymous due to the sensitive nature of this topic. In Chapter 3, the webpages analysed come from a wide range of universities to reflect the diversity of the UK higher education sector, taking into account geographical differences and institutional size.

Acknowledgements

I am extremely grateful to all of the interviewees for their time, as well as to Professor Peter Mathieson and Professor Sir Anthony Finkelstein for their comments on earlier drafts of this report.

February 2022

Contents

Executive summary

The year 2022 is poised to be a crucial time for UK national security and university research. The National Security and Investment Act (NSIA) came into effect on 4 January, with proposed Foreign Interference Registration legislation, currently under scrutiny by the Home Office, potentially coming down the line. Universities UK (UUK) will revise its guidelines, *Managing risks in Internationalisation: Security related issues,* and new UK Research and Innovation-funded training on export controls will launch. Both universities and the Government increasingly realise that though academic freedom and national security need not necessarily be in tension – indeed, robust security measures can enable academic exploration – the dynamic still requires careful negotiation. Despite excellent progress and several initiatives emerging from both the sector and the Government, significant challenges remain in terms of coordination, communication and resources.

The NSIA gives the Government new powers, based in the Department for Business, Energy & Industrial Strategy (BEIS), to intervene in the acquisition of UK entities and assets by both foreign and domestic investors. The NSIA crystallises the many challenges and opportunities in what the Centre for Protection of National Infrastructure (CPNI) has termed 'Trusted Research', which broadly seeks to protect UK research from security-related risks.

While universities have a thriving international research base, and are keen to minimise any potential threats, they lack a clear sense of what the Government means by 'national security' and

have limited access to actionable intelligence on the threats they face. The Government, on the other hand, has a wealth of intelligence but cannot publicly share it and do not necessarily have either the resources or skills required to monitor and regulate cutting-edge research, even if that were desirable. Yet striking this balance is crucial to accomplishing the interlinked goals of robust security and strategic advantage through science and technology, as outlined in the Government's 2021 *Integrated Review of Security, Defence, Development and Foreign Policy*.

As the NSIA comes into effect, the time is right to reflect on the many recent developments that have taken place at the intersection of national security and university research, while also looking forward to what lies down the track and what gaps remain.

The introduction to this paper maps recent developments in the national security and research space, while the first chapter looks specifically at how the NSIA may affect universities, and what gaps remain when it comes to clarity, resources and informal collaborations that lie beyond its scope. The second chapter explores how to improve intelligence and advice links between the sector and the Government, particularly through the new Research Collaboration Advice Team (RCAT). The third chapter examines how universities can raise researchers' awareness of security issues online, including through their institutional websites and export control training to be launched in 2022.

Several recommendations emerge from this report:

- Government and the sector should collaborate to create a comprehensive, interactive map that shows not only

the government departments, sector bodies and other organisations that have responsibility within the research security space, but also the relationships between them. If regularly updated, this would help both university and Government stakeholders navigate what has become a complex landscape and avoid duplication of efforts.

- BEIS should introduce a list of targeted exemptions from the scheme, such as for trusted domestic investors and closely allied states, as countries such as the USA do for similar legislation. The Research Collaboration Advice Team (RCAT) and the Investment Security Unit should be properly resourced to ensure they can flexibly respond to an as-yet untested demand.
- A comprehensive review of research security skills should be undertaken to determine what kind of skills and knowledge will be needed in the coming years, and how that can be achieved. To ameliorate current deficits across both academia and government, the boundaries between academia and security bodies should be made much more porous through secondments, fellowships and working with Chief Scientific Advisers.
- Universities should host readily accessible resources and contact details related to research security on their public webpages, both to inform their own researchers as well as potential researchers and partners. They may also wish to consider developing principles for managing international risks to underpin the wide scope of these engagements, as their institutional risk profile warrants.

Foreword

Professor Sir Anthony Finkelstein CBE FREng
Former Chief Scientific Adviser on National Security
President of City, University of London

Universities have long been conscious of their part in defence and national security. Many researchers contribute directly to the development of sensitive technologies that provide security to the UK and its allies. They also provide expertise necessary for the retention of sovereign national capabilities. Whilst this part of the mission of UK universities has not been much spoken about, it is a familiar part of the scene. Most academics understand that this work must be protected and that there is a legitimate interest in government in ensuring that relevant knowledge is not acquired by, or proliferated to, states who do not share our democratic values.

This relatively straightforward picture has, however, grown increasingly complex. First, the range of disciplines that engage with defence and national security concerns has significantly expanded. Second, research has globalised, with more states possessing a sophisticated scientific and technological capability. Third, UK universities have a much larger and more complex set of international engagements, driven by both research and financial imperatives, and are perhaps less inclined to think of themselves as national institutions. Fourth, the always tenuous boundary between the UK's economic prosperity and its national security has become vaguer and less easy to draw. Finally, we are facing a sharpened geopolitical environment in which some states are willing to deploy espionage and subversion in pursuit of their interests.

For all these reasons it is necessary that government legislate for, and engage with, the higher education sector and the associated innovation ecosystem. This important HEPI report reviews the scene. It sets out the large changes that are in motion, identifies the positive steps being taken by BEIS (signally the creation of RCAT) and others, and makes some valuable recommendations about how universities can respond. It also contains some salutary messages for government. Research is a complex and highly dynamic business, it is undertaken at scale by universities through a great variety of different routes, and it is an important UK soft and hard power asset, so interventions must be very carefully measured. Seemingly small regulatory requirements readily spawn large bureaucratic responses. Partnership with the sector and a willingness to listen are strongly in the UK's national security interests.

All consideration of national security matters should proceed from an understanding of two key tenets. One: 'threats' and 'opportunities' are intertwined. Two: 'adversaries' are aware, smart and adaptive. The consequences should be clear. The UK has the opportunity to build a unique partnership between its universities and the national security community and to construct a trusted, secure, high integrity research capability that will yield a competitive advantage for the UK. Our adversaries will seek ways round our protections, they will exploit our naivety and weaponise our weaknesses. We should not give them the space to do this.

I commend this report and thank HEPI for their initiative.

Introduction: Mapping recent developments in national security and university research

UK research has never been more internationalised.[1] Overseas investment in UK Research and Development (R&D) is significant and continues to grow and, in 2018, overseas investment accounted for 14% of all R&D funding in the UK.[2] In 2019, this investment reached its highest-ever point, growing by 4.6% to £5.6 billion and surpassing its previous peak of £5.5 billion in 2014.[3] Office for National Statistics (ONS) data show that £1.47 billion of this overseas funding went directly to higher education, amounting to 16% of all R&D funding for the sector.[4] The UK also remains one of the least restrictive countries in the G20 for attracting Foreign Direct Investment (see Figure 1).[5]

Table 1: Flows of research and development funding in the UK, 2019

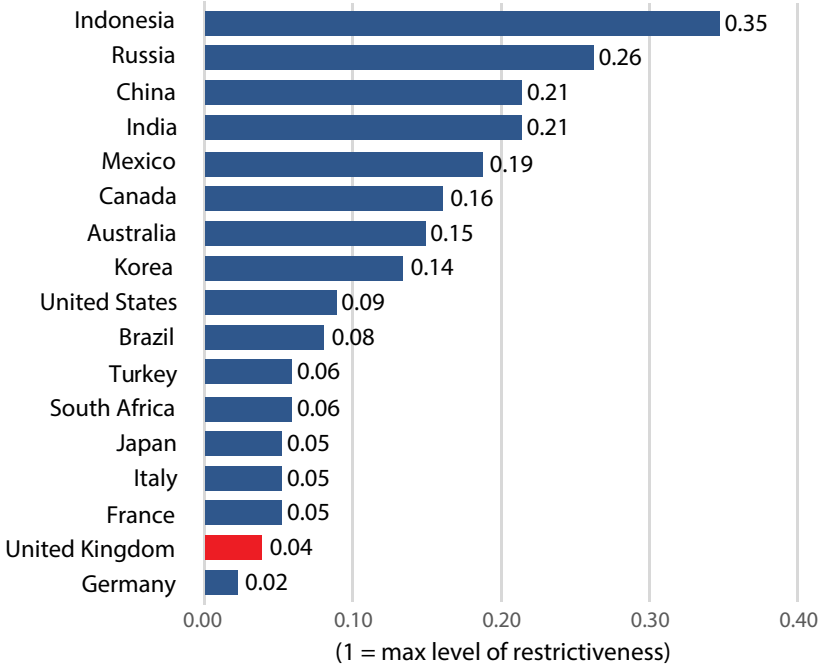
Sector receiving the funds:	Government & UKRI	Higher Education	Business Enterprise	Private Non-Profit	Total (£m)
Government	1,503	**421**	1,202	102	3,228
UKRI	819	**2,707**	634	198	4,358
Higher Education Research Funding Councils	-	**2,859**	-	-	2,859
Higher Education	21	**-**	28	17	65
Business Enterprise	81	**362**	20,192	25	20,660
Private Non-Profit	81	**1,247**	75	364	1,766
Overseas	157	**1,472**	3,818	137	5,583

Source: Office for National Statistics[6]

Parallel to this growing investment from overseas has been the growing number of internationally collaborative research projects. In 2019/20, 59.3% of UK publications were the result of international collaboration, compared to 39.8% in 2010/11.[7] Focussing specifically on Chinese / UK higher education relations, a 2021 report from The Policy Institute at King's College London shows that Chinese-collaborated research alone rose from 1% of UK publications in 2000 to 11% in 2019.[8] The relationship is financial as well as academic; the cross-subsidy between teaching and research from international students has been well-established, making the UK research base substantially dependent on international student income.[9]

But with growth in internationalisation comes associated risk. According to Anthony Finkelstein, former Chief Scientific Adviser for National Security, 'state power – both hard and soft power – is increasingly defined as a state's ability to leverage and advance science and technology'. A prime example of this geopolitical shift can be found in the COVID-19 vaccine, both in the UK's rapid development of a vaccine, significantly within universities, and the interference it encountered. In 2020, the UK's National Cyber Security Centre (NCSC) confirmed that it believed Russian intelligence services had targeted organisations involved in UK vaccine development, 'likely with the intention of stealing information and intellectual property relating to the development and testing of COVID-19 vaccines'.[10] As science and technology have become more central to state power, so too have universities moved from the periphery to the centre – both in terms of their national importance and the need to ensure the security of their research.

Figure 1: OECD Foreign Direct Investment restrictiveness index – G20 countries (2020)[11]



Stealth attacks in the UK have been coupled with increased public scrutiny of the risks attached to researchers' collaborative behaviour. In November 2019, a Foreign Affairs Committee report into the UK's foreign policy regarding autocracies found mounting evidence of foreign influence in UK universities, including 'alarming evidence' about the extent of Chinese influence on UK campuses.[12] In September 2021, *The Times* also accused the University of Cambridge of being 'infiltrated' by Huawei, alleging ties between the tech giant and the Cambridge Centre for Chinese Management (CCCM).[13] The

recent January 2022 MI5 memo relating to foreign influence in Parliament may also increase calls for further scrutiny.[14]

The USA has taken a particularly determined approach to countering foreign interference in university research – not without controversy.[15] A 2019 Senate subcommittee inquiry report, *Threats to the U.S. Research Enterprise: China's Talent Recruitment Plans*, detailed a wide range of incidents of intellectual property (IP) theft, including a postdoctoral researcher who stole 30,000 electronic files from a national lab and another who stole proprietary defence information related to US military jet engines.[16] Most recently in December 2021, Harvard University professor Charles Lieber was convicted of hiding his ties to a Chinese-run recruitment programme, including making false statements to authorities and filing tax returns that failed to mention payments of $50,000 a month and up to $158,000 in living expenses from the Wuhan University of Technology.[17]

Australia has also been especially vulnerable to foreign interference, in part because of how it is positioned geopolitically.[18] One former Government adviser described Chinese interference in the country as 'brazen' and 'aggressive', in response to a report from intelligence services on foreign interference in Australian political parties over the previous decade.[19] This vulnerability has made the Australian Government particularly sensitive to the risks to its research base, not least after the Australian National University (ANU) reported a major data breach of 19 years of students' personal data in 2018.[20] This heightened sensitivity has resulted in Australian universities being subject to ten pieces of proposed and actual legislation and regulations related to national

security, which universities have criticised for creating piecemeal, duplicative regulation.[21]

In this global context, the UK Government has also become increasingly aware of and responsive to the security risks attending international collaboration and research, in particular where there are economic consequences. As the Rt Hon Alok Sharma MP, former Secretary of State for BEIS, described in relation to the NSIA:

> *The UK is very much open for business, but being open for business does not mean that we are open to exploitation. An open approach to international investment must also include appropriate safeguards to protect our national security. Those are not conflicting approaches; prosperity and security go hand in hand. Otherwise, we leave the United Kingdom open to the risk of being targeted and compromised by potential hostile actors who are looking to disrupt our economic and wider security.*[22]

The NSIA takes its place among a series of instruments through which the UK Government seeks greater influence over foreign involvement in UK research. There are broadly three ways in which the Government, along with non-departmental public bodies such as UKRI, can seek to influence or control this involvement:

1. **Controlling who can perform research:** For example, the use of Academic Technology Approval Scheme (ATAS) certificates – once only required of international students studying particularly sensitive subjects – as of May 2021 was expanded to include researchers, citing threats from 'Hostile State Actors'.[23] International researchers

and students must apply for these certificates before commencing their research or study, unless they are from an exempt country.[24]

2. **Producing guidance on how sensitive research should be performed, stored and disseminated**: Several bodies have produced guidance and principles related to 'Trusted Research' and how it should be performed. For example, the Centre for the Protection of National Infrastructure (CPNI) launched their Trusted Research campaign in 2019, which included academia-specific guidance on research collaborations and a social media campaign.[25]

3. **Restricting how research and research outputs are funded and acquired:** This has historically been controlled through export regimes, which were expanded in January 2021 to include all exports of controlled dual-use items and technologies to the European Union, and will be expanded further in 2022.[26] Export control guidance was recently revised in March 2021 to include higher education-specific guidance.[27] UKRI has also recently revised its funding terms and conditions to incorporate trusted research principles.[28] The NSIA will create mechanisms for further government intervention in investment in this space.

Responsibility for these different mechanisms is housed across a range of different government departments and bodies (detailed in Table 2).

Table 2: Government departments, agencies and non-departmental public bodies with functions affecting national security and research

		Function (or proposed function) related to HE research and security
Government departments	Department for Business, Energy and Industrial Strategy (BEIS)	• Investment Security Unit • Research Collaboration Advice Team (RCAT)
	Home Office	• Foreign Influence Registration Scheme (proposed, consultation closed July 2021)
	Foreign Commonwealth and Development Office (FCDO)	• Academic Technology Approval Scheme (ATAS)
	Cabinet Office	• Office for Science and Technology Strategy (OSTS)
	Department for International Trade (DIT)	• Export Control Joint Unit (ECJU)
Government agencies	Centre for Protection of National Infrastructure (CPNI), parent agency is MI5	• CPNI Trusted Research campaign, including sector guidance and toolkits
	National Cyber Security Centre (NCSC), part of GCHQ	• Supports cyber security education and provides a range of support to HEIs, such as sector risk assessments[29]
	Intellectual Property Office (executive agency for BEIS)	• Lambert Toolkit (currently being updated in light of Brexit)[30]
Non-departmental public body	UK Research and Innovation (UKRI)	• Funded new training into export controls for researchers • Integrated Trusted Research principles into latest funding requirements in 2021 • Supported ARMA project exploring an online national service for due diligence in UK funded research projects and partnerships[31]

The Centre for the Protection of National Infrastructure (CPNI), the Government's technical authority for protective security, launched its Trusted Research campaign in 2019 to raise awareness across both academia and industry of the risks of international collaboration. It offers guidance on how to protect research and staff from potential theft, misuse or exploitation. The campaign – which consists of guidance notes, checklists and social media messaging – is aimed particularly at those working in STEM subjects, dual-use technologies, emerging technologies and commercially sensitive research areas.[32] More broadly, CPNI works collaboratively with universities to address national security threats to research via direct engagement and focus groups.

The UK higher education sector has also proactively responded to these issues, recognising both the security risk to their research and the potential burden of additional legislation should they fail to tackle these issues head on. Complementing the CPNI campaign, in 2020 Universities UK developed its own guidance for institutions, *Managing risks in Internationalisation: Security related issues,* on the considerations and measures universities should take to guard against hostile interference, which is currently being revised.[33] The UUK Security Group further draws on relevant stakeholders across government departments and bodies to negotiate a range of relevant issues and determine where more guidance may be needed. The Russell Group helped develop higher education-specific guidance on the NSIA, in addition to regularly engaging directly with the Export Controls Joint Unit (ECJU). Moreover, in 2022 the sector-led Higher Education Export Control Association will launch to address a range of export control issues.

While national interest and national security are not synonymous, they are increasingly intertwined, as the recent *Integrated Review* showed. Published in March 2021, the *Integrated Review* explicitly linked its ambition of building 'a durable competitive edge' in science and technology to 'better protect[ing] our intellectual property and sensitive research'.[34] In other words, 'To be open', the report says, 'we must also be secure'. [35] This HEPI report focusses specifically on the international research investment and collaboration element of security issues, given the recent political attention in this area, as well as the legislative and sector initiatives set to take place in 2022. But there are many other elements at the intersection of universities and national security – cybersecurity, teaching, and freedom of speech, to name a few – that will also warrant more attention in the coming years.

1. The National Security and Investment Act (NSIA) (2021)

The NSIA will introduce a new hybrid regime of mandatory and voluntary notifications for certain acquisitions the Government believes could pose a threat to the UK's national security. Acquisitions can be of entities (for instance, a company, partnership, unincorporated association or trust) or assets (such as land or intellectual property). To qualify within this scheme, an acquisition must meet several conditions, such as the acquired asset or entity being from, in, or having a connection to the UK. The level of control being acquired must also meet a certain threshold – for instance, passing the thresholds of more than 25%, more than 50% or 75% or more of shares or voting rights; gaining the ability to block or pass resolutions; or gaining 'material influence' over the entity, according to guidance from the Competition and Markets Authority (CMA).[36]

The mandatory regime involves 17 defined 'sensitive areas' of the UK economy, from advanced robotics and artificial intelligence to energy and transport.[37] Acquisitions of entities – though crucially, not assets – in these areas must be approved by BEIS before the transaction can go forward. Acquisitions that do not fall under the requirements listed for the mandatory regime may still be reported under the voluntary element of the regime using a slightly different form. The guidance advises that:

> *You can submit a voluntary notification if you are a party to a completed or planned qualifying acquisition that is not covered by mandatory notification and want to find out if the government is going to call it in*.[38]

Once the notification form is submitted, the Investment Security Unit (based in BEIS) will aim to inform the submitter whether the form has been accepted 'as soon as is reasonably practicable'.[39] From then, the Investment Security Unit has 30 days to either clear the submission or 'call in' the acquisition for a further 30 working-day assessment period, which can be extended for an additional 45 working days under some circumstances.

The Government has stated that it anticipates only 1,000 to 1,830 acquisitions to qualify for notification annually, with only 70 to 95 predicted to be called-in for national security assessment.[40] While there are no penalties for not making voluntary notifications, acquisitions that fall under the mandatory regime that are not reported will be void, and subject to civil and criminal penalties, the latter of which can be up to 5% of the organisation's global turnover or £10 million – whichever is greater.[41]

In many ways, the NSIA legislation will bring the UK closer in line with other global developments in national security and investment. Several countries have investment security regimes not dissimilar to the NSIA, including: the USA (Foreign Investment Risk Review Modernization Act, or FIRRMA, 2018); Canada (Investment Canada Act 1985); Germany (German Foreign Trade Act and German Foreign Trade Regulation, extended 2009); and Australia (Australia's Foreign Relations (State and Territory Arrangements) Act 2020). However, the new UK legislation will have a considerably wider scope than its global counterparts in that it includes domestic as well as foreign investors.

How the NSIA will affect universities: to submit or not submit?

Universities are broadly supportive of the new legislation and support the Government's aim of increasing national security around investment. Questions remain, however, as to how elements of the legislation will be implemented in practice. While many agree that the mandatory notification requirements are fairly straightforward, there is much less clarity around the voluntary element of the regime. The guidance directs those trying to decide whether to submit a voluntary notification to Section 3, which gives a series of five scenarios in which a voluntary notification may be called in. In many of these example scenarios, whether a notification will be called in depends on what the Government knows about the proposed investor and believes to be a risk to national security. Yet any definition of national security is deliberately absent:

> *The government intentionally does not set out the exhaustive circumstances in which national security is, or may be, considered at risk. This is longstanding policy to ensure that national security powers are sufficiently flexible to protect the nation*.[42]

This is understandable from a Government perspective – threats may evolve, and flexibility aids reactivity. However, universities are unlikely to know whether (and in what capacity) specific investors are known to the UK Government and without any working definition of national security, it may be difficult for them to determine whether they should submit a notification in this instance. One Regulatory

Compliance Manager described the issue as a:

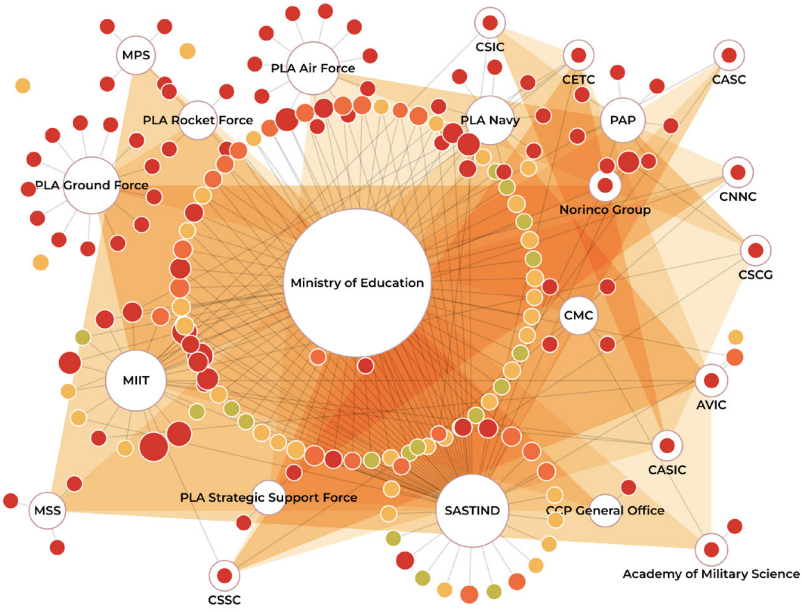
> *lack of guidance, lack of understanding or lack of intelligence sharing … it's really hard for us to know how a project could be impacting on national security without having the intelligence that they have. So that gap there is making it hard, I think, for us to assess what could be of concern or not.*

The UK is not alone in its reluctance to define national security within its investment regime. As Ashley Lenihan, Fellow at the London School of Economics' Centre for International Studies, has noted, similar legislation in 18 other countries also refer to national security without offering a definition within the law.[43] While other countries do not define national security as a concept, however, they do often offer guidance as to what might constitute a security-risk. The Committee on Foreign Investment in the United States (CFIUS) regulations, for example, offer 12 examples of factors to be taken into consideration when deciding whether to block a transaction, including potential effects on critical infrastructure and the long-term projection of US requirements for sources of energy.[44] In this way, implicit parameters can be drawn around areas of concern.

Universities will have dealt with similar issues through other due diligence measures, though their methods are limited to what they can find in the public domain. Some universities use resources from abroad, such as the Australian Strategic Policy Institute (ASPI) China Defence University Tracker. This categorises and rates potential Chinese partners by sector and risk, in addition to providing an interactive visualisation

of the relationships between various bodies (see Figure 2).[45] The institutions listed by the Tracker are not officially endorsed as threats by the UK Government, and of course, it covers only one country. The CPNI guidance directs researchers to rankings such as the Human Freedom Index, though this only contains information at the country level, rather than about specific potential partners.[46] While these resources can help raise 'red flags', what precisely to do once those red flags have been raised is not always clear.

Figure 2 - Australian Strategic Policy Institute (ASPI) China Defence University Tracker[47]



One potentially problematic scenario frequently cited in interviews is that of PhD studentships that result in the generation of intellectual property (IP). Simeon Yates,

Associate Pro-Vice-Chancellor of Research Environment and Postgraduate Research at the University of Liverpool, pointed in particular to the joint PhDs supervised through universities in Asia and Africa. His own university's partnership with Xi'an Jiaotong-Liverpool University (XJTLU), for example, has over 340 PhD students and he estimated another comparable UK university partnership had over 300 PhD students in China. Many international PhD students in the UK are also self-funded or funded by their home country. These students may have contracts with their funders that include clauses on who owns IP rights, which their own university does not necessarily have sight of.

Yates also raises the issue of what to do with grey areas related to, but outside of, the 17 sensitive areas listed in the guidance. For example, should a university with a biosciences project studying insect behaviour report a spin-out company because its computer scientist has done modelling with possible relevance for military swarm devices?

The guidance's lack of clarity in this respect risks creating a bias towards excessive prudence when it comes to submitting voluntary notifications. It also can make it more difficult for research administrators to justify their concerns to academic researchers who want concrete reasons why they cannot advance with a specific collaboration. Chris Buckland, Research Commercial Director at Cranfield University, describes the difficulty he encounters when working with researchers:

> *That's a question I'm repeatedly asked: what are the restricted countries? It's very difficult for an individual to relate to something that you say you can't tell them about.*

He recommends a quarterly threat briefing disseminated to the executive levels of universities – which could help raise awareness of specific threats in a controlled way – though this would require more university personnel with security clearance.

In the absence of more specific guidance or intelligence, some institutions have begun developing formalised internal processes to navigate voluntary notifications – particularly if they have significant exposure to the new regime through spin outs. Peter Hedges, Head of the University Research Office at the University of Cambridge, described the decision-making tree their team had established to streamline the voluntary notification process at the University of Cambridge, which in 2021 helped launch 29 start-up firms worth more than £750 million.[48] This internal process does not have government sign-off, though it has been sense-checked and shared with peers at other research-intensive universities.

Administrative burden and capacity issues

The lack of clarity around voluntary notifications may naturally lead to an issue of capacity. One issue cited by many people working in universities was the potential administrative burden the scheme could create, both for universities and the BEIS team receiving notifications. As Michael Leiter, former Director of the United States National Counterterrorism Center, noted in testimony to the House of Commons, the UK will see an 'explosive increase in matters' under this new regime, as it goes from reviewing very few cases to over a thousand. This number will far outstrip its US equivalent, which under the Committee on Foreign Investment in the United States (CFIUS) now

reviews approximately 240 full cases and another 100 short-form cases. The sheer scope of the UK regime 'poses some real risk for management', according to Leiter.[49] He pointed to the resource difficulties this may cause:

> *When you talk about going from a few dozen to 1,000, you have to be very sure that you have both the resources and the expertise to process that. I would be concerned by that. Another case where your Bill [the NSIA] goes much farther than anything I have seen, and certainly much farther than anything in the United States, is in encompassing not just acquisition and investment in businesses but acquisition and investment in supplies, goods, trade secrets, databases, source code and algorithms, so it is tangible and intangible objects, rather than businesses. That scale is very difficult to predict.* [50]

LSE's Ashley Lenihan agreed the new scheme is 'arguably broader in scope on call-in powers than some other foreign direct investment regimes', including the US, which could create capacity issues:

> *My primary concern would be that the institutional capacity and resources behind the review regime are not made clear ... An inter-agency review team is needed. You need enough staff to actually handle and catch all the risks. You the need the proper resources to do so – the right access to the databases, the right security clearances, the right training.* [51]

She further believed that including domestic investors in the scheme – which few other countries do – is 'probably too broad a formulation for focusing on and identifying real

risk'.[52] Universities particularly have concerns around the voluntary notification scheme, which some suspect could generate far beyond the 1,830 potential notifications cited in the NSIA's impact assessment. Because of the lack of public data available about the number of intangible asset sales each year, it is especially difficult to predict how many voluntary notifications could be made.[53]

Universities may be incentivised to over-submit to the scheme for several reasons. This tendency in the first instance arises from the vagueness of the voluntary notification element of the scheme, which universities could interpret as very wide-reaching. Because of the newness of the scheme and the guidance that encourages a voluntary submission if you 'want to find out if the Government is going to call it in', universities are incentivised to submit a range of cases to get a sense of the boundaries of what will qualify as a national security concern. More generally, universities will also want to show their desire to be transparent and support the scheme by reporting voluntarily.

There is also the question of whether to submit voluntary notifications related to licensing intellectual property. The Rt Hon Alok Sharma MP drew attention specifically to licensing as a way in which '[t]hose who wish to do us harm … bypass our current regime' by 'licensing certain intellectual property rather than acquiring the company'.[54] Within the university context, non-exclusive royalty-free agreements (NERFs) are frequently used as a means of sharing IP in international collaboration agreements. Peter Hedges cites NERFs as an area of possible concern should they ultimately fall into what should be included in the voluntary notification category.

The University of Cambridge has currently decided to exclude these exchanges from what it will voluntarily report, because they involve licensing IP to partners, rather than actually transferring legal ownership. If NERFs should be included in voluntary notifications, however, it would 'open the floodgates', according to Hedges, and their institutional reporting burden would increase significantly.

Depending on how the sector responds to the voluntary elements of the regime, there may be significantly more submissions than the impact assessment anticipated. The lack of any *de minimus* threshold for investment or exemption for domestic investors will also make the scheme more difficult to manage.[55] If the BEIS team is inundated with more notifications than are anticipated, this could cause delays in approving transactions in the 17 sensitive areas. Though the BEIS team will have 30 working days to assess mandatory notifications, this process will only start after the notification has been accepted, which the guidance says will be done 'as soon as is reasonably practicable' – but gives no timeline.[56] More impatient investors may not be willing to wait for approval on mandatory notifications and competitors in countries with fewer bureaucratic impediments may prove more attractive.

This is the central irony of the NSIA: it creates greater impediments to innovation and commercialisation precisely at the time when the Government has committed to reducing research bureaucracy.[57] Louise Dunlop, Head of Research Governance, Ethics and Integrity at Queen's University Belfast, says bureaucracy in relation to research has recently 'really escalated' rather than decreased and has become even more complicated for Northern Ireland in particular because of

Brexit and the Northern Ireland Protocol. While universities understand and support the Government's drive to protect national security, Dunlop says that more support from the Government as well as more lead time in introducing changes would help them navigate these shifts more effectively.

More seriously, an influx of notifications and queries could mean missing the notifications that the Government is genuinely after, according to Peter Mathieson, Vice-Chancellor of the University of Edinburgh, who has led on national security work for UUK and the Russell Group:

> *If you overwhelm the system with enquiries and investigations, which are really not justified by the level of risk, then you may well miss those areas that you should be targeting.*

While he says the NSIA may provide helpful due diligence assistance for smaller and less experienced institutions in particular, he wonders whether that could be more simply accomplished at the level of the sector – for example, through a buddying system pairing smaller and larger institutions together to share intelligence and experience when assessing potential partnerships.

Many of the issues presented here may be resolved as further guidance and feedback is developed iteratively over the coming years, and BEIS has said that it will publish market guidance notes within the first six months of the scheme's commencement drawing on an analysis of notifications submitted thus far. Nonetheless, the regime's development and initial implementation reveals the fundamental difficulties that both government and universities face in navigating

this space through legislative means. It also raises important questions about IP issues – such as ownership over the IP generated by PhDs – that many universities will now have to explore further.

What gaps remain

Universities broadly agree that, as much as the NSIA regime might add some additional administrative burden, it was not their greatest concern in this area. Stephen Conway, Executive Director of Research Services at the University of Oxford, drew special attention to more informal kinds of collaboration that might not trigger normal due-diligence measures. For example, he says:

> *The vast majority of circumstances that could give rise to consideration under the NSIA, such as creation of new entities or granting of rights to intellectual property under a research contract, will necessarily involve expert professional services teams at institutional level. This lowers the risk of things inadvertently slipping through the net and makes compliance with the NSIA more manageable. In contrast, relatively informal arrangements such as the transfer of information by researchers could fall within the scope of export control requirements and here compliance is much more reliant on awareness amongst research groups and departments that they need to seek advice and support.*

Louise Dunlop points to potential examples of academics travelling overseas to teach but bringing their sensitive research with them on their laptop, which could breach existing export control legislation. 'The challenge is getting

academics to understand that this material could be subject to export control', she says, 'when that's not how they necessarily think'. These scenarios rely much more on the awareness of academic and research staff, and their ability to know whether they need professional services support.

While Conway and Dunlop show the difficulties of ensuring researcher compliance with existing UK legislation, Peter Hedges also worries, for example, about UK researchers accidentally falling afoul of US export controls in the course of their collaborations, which could result in them being extradited to face charges in the US. He also points to other concerning scenarios in which the current UK legislation has no bearing:

> *If a Chinese collaborator comes to the UK to meet one of our researchers who then stays for a few days and acquires some knowledge or understanding that they simply keep in their head to use when they get home, this risks circumventing any export control and NS&I Act procedures.*

Because this kind of intellectual property exchange is intangible – contained in someone's head, rather than physically on a laptop – these kinds of collaborations would not only escape the NSIA and UK export control regimes, but also potentially the ATAS certificate process, as short stays on a Standard Visitor visa (for example, to attend a conference or give a seminar) do not require foreign visitors to undergo the same scrutiny.[58]

These examples underscore the difficulties of legislating research security issues, where even the most robust due

diligence mechanisms cannot draw all potentially problematic behaviour into scope. This is a natural consequence of how university research functions; professional services provide crucial due diligence and compliance functions but have only so much reach into the daily working lives of researchers, many of whom may have limited awareness of what centralised services exist outside of their own department or lab, let alone the wider geopolitical context of their research.

Legislation is only one tool among many, however, and efforts are increasing to both share some intelligence with universities in a controlled way and raise awareness in academic communities about the potential risks of international collaboration. It is precisely because of these grey areas that both UUK and the Centre for the Protection of National Infrastructure have produced guidance and campaigns around Trusted Research and managing risks. The Research Collaboration and Advice Team (RCAT) launching this year will seek to fill this gap further.

2. Creating stronger intelligence and advising links between the Government and the sector

The previous chapter outlined the difficulties that universities may encounter in navigating the new legislative requirements and assessing risk without a definition of national security. To help further open lines of communication between the Government and the sector, in May 2021 the Government announced the formation of the Research Collaboration Advice Team (RCAT), a new team to be based in BEIS dedicated to protecting researchers' work from hostile activity.[59]

David Mossley, who leads the new team in BEIS, described RCAT as having three core objectives:

1. **Providing guidance and advice to universities**. While universities will have policies and processes in place for many higher risk activities, Mossley said that RCAT will add value in those cases where, for example, a partner has approached a university with associated funding and the university is unsure of how they should assess the collaboration's risk. RCAT will provide advice and guidance in that space to universities – not to 'shut down' any collaboration but to help put in place safeguards and the right due diligence measures to ensure that universities are appropriately assessing the risk themselves. RCAT anticipates that they will be contacted with a range of questions that do not fall into any of the currently prescribed categories and will offer informal chats that allow senior leaders to have 'a trusted conversation without it necessarily triggering any alarm bells'. Ultimately, he said, the risk will still belong to the sector and RCAT has no intention of taking away that risk.

They will only provide advice – though sometimes that will be 'quite strong advice', depending on how they view the risk.

Mossley, however, was keen to emphasise that RCAT – rather than acting as a one-stop shop for everything security-related for universities – will function more as a first port of call for these issues, which can then act to signpost researchers on to other resources, such as the CPNI Trusted Research framework, which will form the basis for much of their work.

2. **Creating communities of practice.** While this advice service will form a significant element of RCAT's work, the second role of RCAT will be to help universities grow 'communities of practice' around security, effective collaboration and building better awareness of risk into research and research training. 'I think this is quite important as, unless universities themselves own these processes, it doesn't really embed or track through', Mossley said. With support from senior leaders, he believes building communities of practice will help disseminate appropriate training and guidance to research communities, which 'has to be central to the longer-term success of good security practice and risk assessment around collaboration'.

3. **Conveying sector issues back to the Government.** The third component of RCAT's work will be helping the Government understand the nature of the risks the sector faces. In this sense, RCAT will work as an intermediary between the Government and universities on this issue, communicating back to government any issues as they arise in the sector.

In the spring / summer of 2022, the RCAT service will 'open for business' as they complete recruitment and initial conversations with stakeholders in the sector.

One concern for the team is capacity, and Mossley was keen to manage expectations at this stage. The team as it stands at the beginning of 2022 is still a small one, learning on the job, though it will grow as the year goes on. Currently they are working to build a team that has a) a sense of the wider security context; b) familiarity with the research areas they are concerned with; and c) the ability to make the right assessments around risk in sensitive conversations. They will also draw on technical expertise from policy teams across government.

RCAT has many champions in the higher education sector. Rhys Morgan, Head of Policy, Integrity and Governance at the University of Cambridge, says RCAT, or a similar means of getting advice, was something for which they had been advocating for years:

> *The ability to get quick informal advice on national security issues ranging from NSIA, to export control, to just general Trusted Research type things such as, "These collaborators are interested in working with us, and is there anything that we need to know?" – those sorts of issues would just be so valuable. It will defuse a lot of worries within the sector that we don't know what's going on [in terms of national security threats], and just give us that knowledge that we need to make informed decisions about our research and our collaborations.*

Similarly, Stephen Conway, Executive Director of Research Services at the University of Oxford, is strongly supportive of the role RCAT can play in representing sector issues within government and hopes RCAT can be influential in ensuring that requirements and guidance are informed by and relevant to higher education and research scenarios.

Australian higher education professionals working in this space are also keen to see what can be learned from RCAT, with an eye towards potentially developing something similar. Paul Harris, Executive Director at Innovative Research Universities (IRU), noted that the Australian Government and universities had reached a new phase in their collaboration, in which universities wanted to maintain institutional autonomy in their due diligence processes but were unable to access the kinds of intelligence that the Government had when making decisions. He believes that 'we need some new kind of partnership model between government and universities to better share information', and some kind of advice service such as RCAT could give them the intelligence they need to facilitate more robust due diligence while avoiding more onerous research bureaucracy. 'Universities here have tightened up their internal processes and are focused on maintaining institutional autonomy in managing risk', he says, 'but will need some additional support from government, which has access to intelligence and information that universities don't'.

But implementing RCAT will not be without challenges. Mossley noted that a key challenge for RCAT was that they do not know what the demand for their services will be like. Much like the volume of voluntary notifications that will be submitted to the Investment Security Unit is unknown,

demand for RCAT is still untested. Though RCAT plan to have regionally based teams supporting universities in each part of the country, how that resource should necessarily be allocated to meet the needs of a very diverse sector is not yet clear.

From universities' perspectives, it is also not yet clear what the balance will be between RCAT giving advice on the one hand and referring researchers to other government units on the other. Universities interviewed were very positive about the advice-giving function of RCAT, but believed its referral function might have more limited value for universities with experience and designated teams working in this space (though this would be less true for universities who, for example, rarely use processes such as export control). It is also currently unclear to them how RCAT's advice-giving function will interact with other government bodies currently offering universities support in this area. Some university staff worried whether delays would emerge similar to those that have occurred with the Academic Technology Approval Scheme (ATAS) certificates; speed will be crucial in maximising RCAT's utility.

Ensuring the team has the skills needed to triage a wide range of research security issues may also be a challenge. They will need to have knowledge across a wide range of legislation related to export control, immigration and investment, in addition to having a map of stakeholders in these fields across multiple government departments. They will also need at least some familiarity with sensitive research areas and how universities function, especially around technology transfer and spin out processes. These skills will be enormously valuable in advising researchers, but it is not just RCAT who wants

them; several interviewees noted how in-demand this skill set now was across both universities and the civil service, with demand far outstripping supply. The NSIA coming into effect will increase this demand further, as recent job advertisements demonstrate.[60]

RCAT is only one way to approach this complicated issue, however, and there are also additional models being explored around how universities might become better informed about their potential partners. For example, former Chief Scientific Adviser for National Security, Anthony Finkelstein, is exploring a collaboration with King's College London and the University of Edinburgh on a community-funded research centre that does open-source attribution and analysis on threats facing university research. Operating in a way not dissimilar to Bellingcat, this centre would use 'highly specialised, investigative open-source methods' to 'get within a few percent' of potential threats, after which 'government can do the rest'. This approach, he believes, would openly communicate to universities a very close approximation of the relevant threats without requiring any exposure of classified material, as ultimately, he says, 'universities will have to do the heavy lifting on this'.

3. Raising researchers' awareness

As Chapter 1 shows, even the best-informed due diligence frameworks cannot always cover the full gamut of potentially risky researcher behaviour. There are, however, several simple cost-effective measures that universities can take to inform their staff and researchers about the risks in international partnerships. This chapter examines how universities can develop an online presence devoted to Trusted Research principles and offers examples of best practice.

Raising and maintaining staff awareness – and especially researcher awareness – of the risks associated with international partnerships is a crucial element of effective mitigation. The UUK *Managing Risk* guidelines identify an issue in 'institutional cultures where staff may be unaware of the risks or not sufficiently empowered to act on the risks that they have identified within the risk-management processes'.[61] A workshop of 37 researchers held by SPRITE+ in March 2021 showed that there was significant confusion among participants as to what 'Trusted Research' as a concept entailed. They also tended to be over-confident in their knowledge on the topic and had limited awareness of the available guidance.[62]

The ways in which universities house (or do not house) Trusted Research material on their websites is a crude measure of the extent to which this agenda has permeated institutional culture and practice. Such websites are, however, likely to be a researcher's first port of call when interacting with the institution, especially as the pandemic has increased the amount of online engagement. An individual researcher

approached by a potentially suspect partner, for example, may begin by googling what institutional support and guidance is available and is unlikely to be independently aware of CPNI's work on Trusted Research.

Few universities house Trusted Research materials on their publicly available webpages. An initial internet search of 100 UK universities revealed only ten had easily accessible online materials related to Trusted Research, while 42 of 100 of these institutions had public webpages devoted to developing and showcasing international research partnerships. There are historical reasons for this; the Research Excellence Framework (REF) and impact agenda more broadly has embedded external engagement quite successfully in institutional missions and processes, while Trusted Research is a far more recent concept. This will also be due in part to the differing risk profiles across the sector; a large, research-intensive institution, for instance, will not have the same risk as a small teaching-focussed institution with few international partnerships. This is reflected in the fact that eight of the ten institutions with Trusted Research materials publicly online are Russell Group members. More materials may also be housed behind institutional web portals or within non-public due diligence processes.

However, publicly hosting some form of these materials on institutional webpages is an easy way to reinforce a university's commitment to these principles for its researchers. It also asserts that commitment to potential researchers and international partners as well, thereby complementing existing due diligence policies.

Accessibility

The SPRITE+ workshop on Trusted Research recommended providing accessible resources to help ameliorate researchers' awareness of this issue.[63] The majority of universities who do reference Trusted Research on their websites do so on their research governance and integrity pages, though two universities explored Trusted Research via blogs. Ideally, some combination of the two would help both introduce and reinforce these messages. While blogs are helpful in drawing new content to researchers' attention, they can get lost in the archive of previous blog posts as time passes. A permanent base on either the research integrity or partnerships webpages (or both) helps ensure a lasting presence for this content.

A web presence can also helpfully recognise the overlapping elements of Trusted Research advice and reflect that across multiple resources. For example, the University of Cambridge references Trusted Research both on the parts of its website devoted to research governance and strategic partnerships, recognising the overlap between these areas.[64] Likewise, the University of Manchester features Trusted Research links on both its export controls page and its research and business engagement pages.[65]

Collaboration checklists

Most sites featuring Trusted Research principles have some form of checklist or questions for researchers to ask themselves as they embark on a research partnership. These are largely adapted from the nine core messages of the Government's Trusted Research Partnership toolkit, circulated in 2019 as a part of their campaign.[66] They are, however, not

adapted without difference; Cambridge, for example, softens the Government's question of 'Are your ideas worth stealing?' to 'Could your research make you a target?', presumably to dissociate research's overall value from its potential security risk.[67]

The University of Manchester distils its checklist into just three questions: 1) 'Who's funding your research?'; 2) 'How well do you know your research partners?'; and 3) 'How is your research being used?'.[68] The University of Bath helpfully asks questions about who will own the intellectual property generated from the project and the University of Strathclyde, rather than articulating its own set of questions for researchers, links directly to the CPNI's Trusted Research Checklist.[69]

In addition to an 'International Collaboration Checklist', the University of Oxford has created a 'Strategic Partnership Scorecard', an evaluation process through which researchers report potential partnerships that meet a certain threshold, such as requiring a material contribution from the university, typically of over £500,000. The International Engagements Office and advisory panel then provides a recommendation on whether the partnership should proceed based on the scorecard.[70] Similarly, the University of Nottingham has a 'project notification form' that researchers should fill out if they are involved in an international collaboration.[71]

Case study: University of Cambridge Principles for Managing International Risk

The University of Cambridge is unique in having developed a set of five principles underpinning their approach to international collaboration. They are:

1. *Protect our people in their international engagement.*
2. *Defend academic freedom.*
3. *Promote and support an academic culture of vigilance and awareness of these risks, and ensure that people are equipped to know how to minimise or mitigate them.*
4. *Protect the open flow of ideas, data and other forms of intellectual property – including a duty to protect it against wrongful exploitation or interference.*
5. *Safeguard the University's funding autonomy – including a duty to ensure the diversity and transparency of our funding sources.*[72]

These principles have the effect of not only articulating the institution's obligations to protect research, but also its expectations on staff to partake in a 'risk-literate academic culture'.[73] While not paraphrasing the UUK *Managing Risk* guidelines exactly, it too envisions increased safeguarding as a necessary measure to facilitate successful international research and collaboration.

The pages that follow tie together a wide range of risk-related concerns, including due diligence on philanthropic gifts and research relationships, cybersecurity, personal safety when

travelling and export controls. Links are provided to not only relevant external guidance (such as from CPNI) but also relevant university policies, contacts and training videos – including a video introduction from Vice-Chancellor Stephen Toope.

Links to resources and contact details

All ten sites link to the CPNI's Trusted Research guidance, save the University of Nottingham, which links to its own Trusted Research toolkit and University Trusted Research Team.[74] The University of Cambridge's strategic partnerships' page links directly to their due diligence team and while the University of Manchester's page does not link directly to a contact email, a related page on due diligence contains a link to the research operation team's email.[75] Making contact details of relevant staff available will be crucial, as workshops have shown that researchers find it difficult to know who to seek guidance from on these issues.[76]

Interestingly, only three of the ten sites linked to the UUK *Managing Risk* guidance and only two linked to the UKRI Trusted Research and Innovation Principles. This is likely in part because the *Managing Risk* guidelines are aimed specifically at providing university governing bodies and the executive heads of universities with tools and support, rather than individual researchers (though they may be useful to researchers wishing to understand the wider context). This may also be due in part to the relative newness of these documents – while the CPNI campaign began in 2019, the UUK guidance was published in October 2020 and UKRI principles in August 2021.

Training

While most sites link to relevant guidance and research teams, few link to training that researchers can undertake on Trusted Research issues – in part because, while there is significant guidance in this area, such training specifically for university audiences is currently unavailable on a nationwide basis (though individual universities, such as the University of Manchester and the University of Sheffield, among others, offer export control training for their own staff).

Recognising the need for more training in this area, in October 2021 UKRI awarded £200,000 in funding to a partnership between Cranfield and Edinburgh Universities to create an open-source virtual learning tool on export control issues for the higher education sector.[77] Chris Buckland, who has been leading development of the new Research England-funded export control training, hopes to have the beta test of the training ready by April 2022. The aim of the training is to integrate awareness of export controls across all stages of research activity, including the associated professional service functions.

In the early stages of their careers, Buckland says, researchers are not currently given a foundation as to 'why this is important, and why it's relevant to you as a student or academic who is going to have access to information about emerging technology that's sensitive from an export controls perspective'. The training will help them digest and understand the risks that can be associated with their activities, integrating risk awareness as a normal aspect of their work, rather than something to be fearful of or confused by. Ideally, awareness

of security risks will become 'just second nature', he says, and something they are conscious of both when they are speaking in person and interacting online. Workshops for the training have thus far involved 125 individuals at 45 institutions. Collectivised training such as this will conserve university resources and keep individual institutions from having to reinvent the wheel – but it will need to be adapted to fit institutional contexts and risk profiles as well.

The success of resources such as the Trusted Research guidance will depend on how well universities are able to embed them within their own institutional cultures. Researchers are unlikely to seek out external resources on their own initiative, and government bodies do not have the resources to reach all relevant individual researchers directly without the help of institutional reinforcement. Likewise, these external resources can help universities demonstrate to researchers that their concerns around security are not institutional, but national in nature, and the relationship between these external resources and university practice must be mutually reinforcing to be effective.

Conclusions and recommendations

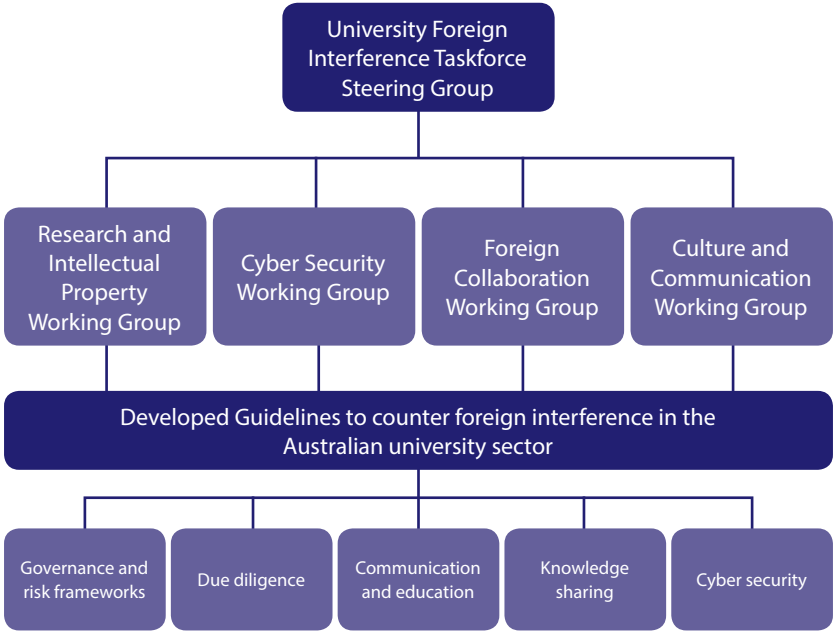
Mapping and coordination

The sector needs a comprehensive map that shows the relationships between government departments, sector bodies and other organisations that have responsibility within the Trusted Research space. Much has happened in this area over the last two years, creating what one interviewee called 'a crowded territory', and there is not yet a single resource that draws these developments together in a coherent form. As Chris Buckland at Cranfield University put it, 'the biggest issue immediately is the consolidation and coordination of various local and national efforts in a coherent, understandable tool that can be visualised, communicated and understood across the sector'. This, he believes, will be crucial to coordinating efforts and avoiding duplication and confusion in the coming years. An interactive map – not unlike the kind used by the Australian Strategic Policy Institute (ASPI) Tracker, which shows not only relevant information about organisations, but also their relationship with one another (see Figure 2) – could help convey the complex landscape in an easily digestible way.

By making clear which body is responsible for what, such a map could also help conserve the Research Collaboration Advice Team's (RCAT) resources in terms of signposting, particularly if it includes detailed, up-to-date explanations of each stakeholder's responsibilities and relevant contact details. It would also help make sense of the enormous plurality of effort that has taken place in the past few years. As Rhys Morgan, Head of Policy, Integrity and Governance at the University of Cambridge, put it, the Trusted Research space is like 'a snow

globe that has been shaken up, which we now need to make sure settles in the right way'. Understanding and articulating these efforts, as well as how they relate to one another, is the first step. For example, Universities UK could collaborate with RCAT to create a purpose-built website that gathers all of this information in one place.

Figure 3: Structure of the Australian University Foreign Interference Taskforce Steering Group (UFIT) and guidelines[78]



In terms of how leadership in this space is organised, much could be learned from Australia's University Foreign Interference Taskforce (UFIT) model, which convenes a taskforce of equal membership between senior government and higher education sector stakeholders. Rather than

government having just a seat at the table, or vice versa, a more formal structure could recognise the shared endeavour and responsibility for national security, in addition to aiding in coordination between government departments. Such a structure, implemented sensitively, would crucially not impinge upon sector autonomy but rather recognise the burden of responsibility for security as fundamentally shared and collaborative in nature.

Streamlining the NSIA's implementation

The NSIA is only one element in the complex environment of university research and national security. However, **there are several concrete ways in which its implementation could be streamlined to best serve its aims – particularly if the volume of voluntary notifications exceeds expectations.**

Drawing on the USA and Australian models, BEIS could introduce a list of targeted exemptions from the scheme including domestic investors and allied states. This would reduce bureaucracy while maintaining a robust security framework. The Investment Security Unit and Research Collaboration Advice Team (RCAT) should also be properly resourced to make sure staff are able to respond to a potentially large pool of enquiries and referrals quickly.

Skills and knowledge base

A comprehensive review of research security skills should be undertaken to determine what kind of skills and knowledge base will be needed in the coming years, and how it can be achieved. The recent inquiry in Australia, for example, showed how the skills needed in this area were

complex. When former ASPI researcher Alex Joske was asked what would be necessary to explore ties between Australian research and hostile state actors, he said that 'doing this sort of research is very time intensive and it relies on people with skills that aren't very common'. It not only requires language skills, but also knowledge of tech-transfer issues, political interference and 'the ability to actually do original, empirical research on these topics'.[79] Patrick Vallance, in his new role as National Technology Advisor at the Office for Science and Technology Strategy (OSTS), also noted the skills deficit in the civil service in this area in a talk to the Royal Society for Engineering in December 2021.[80]

The Government has already announced the formation of a College for National Security.[81] But the higher education sector as it stands is also extremely well placed to explore how it can support the skills pipeline and relationships necessary for this work in the future. **The boundaries between academia and security bodies should be made much more porous, with secondments, fellowships and networks of Chief Scientific Advisers.** Models such as the British Academy's recent Innovation Fellowships linked to the Integrated Review and the Foreign, Commonwealth & Development Office (FCDO) should be replicated across science and technology disciplines with BEIS.[82]

There are also simple, low-cost measures that individual universities can take to raise awareness of these issues. **Universities should host easily accessible resources and contact details related to research security on their public webpages, both to inform their own researchers as well as potential researchers and partners. They may also wish to**

consider developing principles for managing international risks, as the University of Cambridge has done, to underpin the wide scope of these engagements, as their institutional risk profile warrants.

Neither the higher education sector nor the Government suffers from a lack of willingness to address these issues, as the sheer number of initiatives that have been proposed over the last few years shows. The answer, however, is unlikely to lie in further legislation, at least as it has currently been proposed. For example, the Foreign Influence Registration Scheme proposed by the Home Office, modelled on the US Foreign Agents Registration Act (FARA) and the Australian Foreign Influence Transparency Scheme Act (FITS) 2018, would create 'a government-managed register of declared activities that are undertaken for, or on behalf of, a foreign state'.[83]

Many in the sector have been critical of this proposed scheme. The Royal Society, for instance, has said that the scheme could create a 'considerable bureaucratic burden' for institutions, in addition to having 'a chilling effect on the research community and act[ing] as a deterrent to international research collaboration'.[84] While supportive of the NSIA, by contrast Anthony Finkelstein believes this proposed new legislation is 'too broadly drawn and not based on a grounded understanding of how universities function.' Peter Mathieson believes that, with this proposed registration scheme and others, the 'devil will be in the detail'. Along with several mission groups, his own university responded to the Government consultation on the Foreign Influence Registration Scheme asking that the legislation not be made 'too onerous', or 'too broad in the sense that you'll end up overwhelming the

agencies with what they don't need to be worried about'. He pointed to helpful exemptions in the US equivalent of this legislation, which includes exemptions for those engaged in scholastic, academic or scientific pursuits.[85]

The Foreign Influence Registration Scheme is not the only potential new piece of legislation coming down the line. In January 2022, MP Jesse Norman proposed an amendment to the Higher Education (Freedom of Speech) Bill that would require universities to disclose any gifts, donations or other financial arrangements in excess of £50,000 to be kept on a public register. The amendment immediately faced criticism for its broad scope, which would require universities to gather and disclose 'everything from the personal financial circumstances of individual overseas students who are being supported by family members, to historic contractual data relating to major research partnerships, and everything in between'.[86] The amendment's definition of 'overseas counterparty' is so broadly drawn that it would even apply to UK dual citizens, and the threshold of £50,000 is far below its US equivalent of $250,000.[87] If this amendment is passed, it would also apply to financial arrangements already addressed through the NSIA, adding an additional layer of administrative complexity and duplication.

The Government's interim report on research bureaucracy, led by Adam Tickell, Vice-Chancellor at the University of Birmingham, identified the Trusted Research agenda as a specific example of where there is 'a need for bureaucracy', and few would argue that robust accountability mechanisms in this space are unnecessary.[88] But additional regulatory and legislative instruments do not in themselves necessarily make

research safer. Indeed, if their implementation overwhelms the administrative capacity of universities and government departments alike, identifying genuine threats becomes more, not less, difficult. Several leaders in Australian higher education argue this has already occurred in their context: 'We don't oppose any legislation,' Universities Australia CEO Catriona Jackson said in 2021, but rather 'just think that there is a genuine problem with duplication and overlap, which means it will be harder for universities to identify and root out foreign interference in collaboration with security agencies'.[89]

Any new legislation must be carefully designed if it is to avoid being counterproductive. What may be more effective and resource-efficient than additional legislation, however, is supporting universities to better tackle these issues themselves – especially given how much depends on raising the awareness of researchers who operate within their institutional walls. Many interviewees remarked on the significant and encouraging shift that had occurred between the sector and the Government in the last few years, with more open conversations far more common than they had been previously. Finding ways to expand, coordinate and support those conversations further, in addition to the recommendations outlined here, can continue to build trust and ensure progress moving forward.

Endnotes

1 Universities UK, *Future International Partnerships: putting the UK at the heart of global research and innovation collaboration*, October 2020. https://www.universitiesuk.ac.uk/sites/default/files/field/downloads/2021-07/Future-international-partnerships.pdf

2 Office for National Statistics, *Gross domestic expenditure on research and development, UK: 2018*, 2 April 2020. https://www.ons.gov.uk/economy/governmentpublicsectorandtaxes/researchanddevelopmentexpenditure/bulletins/ukgrossdomesticexpenditureonresearchanddevelopment/2018

3 Office for National Statistics, *Gross domestic expenditure on research and development, UK: 2019*, 4 August 2021. https://www.ons.gov.uk/economy/governmentpublicsectorandtaxes/researchanddevelopmentexpenditure/bulletins/ukgrossdomesticexpenditureonresearchanddevelopment/2019

4 Office for National Statistics, *Gross domestic expenditure on research and development, UK: 2019*, 4 August 2021. https://www.ons.gov.uk/economy/governmentpublicsectorandtaxes/researchanddevelopmentexpenditure/bulletins/ukgrossdomesticexpenditureonresearchanddevelopment/2019

5 The OECD does not rate G20 members Saudi Arabia or Argentina, therefore these are missing from Figure 1. See OECD, *Foreign Direct Investment Regulatory Restrictiveness Index*, 2021. https://goingdigital.oecd.org/en/indicator/74

6 Office for National Statistics, *Gross domestic expenditure on research and development, UK: 2019*, 4 August 2021. https://www.ons.gov.uk/economy/governmentpublicsectorandtaxes/researchanddevelopmentexpenditure/bulletins/ukgrossdomesticexpenditureonresearchanddevelopment/2019

7 Universities UK, *International Facts and Figures 2021*, 8 December 2021 https://www.universitiesuk.ac.uk/universities-uk-international/insights-and-publications/uuki-publications/international-facts-and-figures-2021

8 The Policy Institute at King's College London, *The China question: Managing risks and maximising benefits from partnership in higher education and research*, March 2021. https://www.kcl.ac.uk/policy-institute/assets/china-question.pdf

9 Nick Hillman, *From T to R revisited: Cross-subsidies from teaching to research after Augar and the 2.4% R&D target*, 9 March 2020. https://www.hepi.ac.uk/2020/03/09/from-t-to-r-revisited-cross-subsidies-from-teaching-to-research-after-augar-and-the-2-4-rd-target/

10 National Security Cyber Centre, *Advisory: APT29 targets COVID-19 vaccine development*, 16 July 2020. https://www.ncsc.gov.uk/files/Advisory-APT29-targets-COVID-19-vaccine-development-V1-1.pdf

11 The OECD does not rate G20 members Saudi Arabia or Argentina, therefore these are missing from Figure 1. See OECD, *Foreign Direct Investment Regulatory Restrictiveness Index*, 2021. https://goingdigital.oecd.org/en/indicator/74

12 Foreign Affairs Committee 2nd Report, 'Autocracies influence in academia', *A cautious embrace: defending democracy in an age of autocracies*, November 2019. https://publications.parliament.uk/pa/cm201919/cmselect/cmfaff/109/10905.htm

13 Ben Ellery, 'Huawei "infiltrates" Cambridge University research centre', *The Times*, 13 September 2021. https://www.thetimes.co.uk/article/huawei-infiltrates-cambridge-university-research-centre-kn6m5lnhc

14 Gordon Corera and Jennifer Scott, 'MI5 warning over "Chinese agent" in Parliament', *BBC News*, 13 January 2022. https://www.bbc.co.uk/news/uk-politics-59984380

15 Vincent Ni, 'Abolish Trump-era "China Initiative", academics urge, amid racial profiling criticism', *The Guardian*, 15 September 2021. https://www.theguardian.com/us-news/2021/sep/15/abolish-trump-era-china-initiative-academics-urge-amid-racial-profiling-criticism

16 United States Senate, Committee on Homeland Security and Governmental Affairs, *Threats to the U.S. Research Enterprise: China's Talent Recruitment Plans*, November 2019. https://www.hsgac.senate.gov/imo/media/doc/2019-11-18%20PSI%20Staff%20Report%20-%20China's%20Talent%20Recruitment%20Plans%20Updated2.pdf

17 Associated Press, 'Harvard professor found guilty of hiding ties to Chinese-run recruitment program', *The Guardian*, 22 December 2021. https://www.theguardian.com/us-news/2021/dec/22/harvard-professor-found-guilty-of-hiding-ties-to-chinese-run-recruitment-program

18 Josh Garnaut, 'How China Interferes in Australia and How Democracies Can Push Back', *Foreign Affairs*, 9 March 2018. https://www.foreignaffairs.com/articles/china/2018-03-09/how-china-interferes-australia

19 Stephanie Borys, 'China's "brazen" and "aggressive" political interference outlined in top-secret report,' *ABC News*, 28 May 2018. https://www.abc.net.au/news/2018-05-29/chinas-been-interfering-in-australian-politics-for-past-decade/9810236

20 Michael McGowan, 'China behind massive Australian National University hack, intelligence officials say,' *The Guardian*, 6 June 2019. https://www.theguardian.com/australia-news/2019/jun/06/china-behind-massive-australian-national-university-hack-intelligence-officials-say

21 These include Autonomous Sanctions Act 2011; Commonwealth Integrity Commission Bill 2020; Defence Trade Controls Act 2012; Export Control Act 2020; Foreign Influence Transparency Scheme Act (the FITS Act) 2018; Foreign Relations (State and Territory Arrangements) Act 2020; Security Legislation Amendment (Critical Infrastructure) Bill 2020; Proposed Commonwealth Integrity Commission Bill; University Foreign Interference Taskforce (UFIT) Guidelines; TEQSA's Higher Education Integrity Unit. See the Innovative Research Universities submission to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) Inquiry into national security risks affecting the Australian higher education and research sector.

22 Hansard, *National Security and Investment Bill*, Volume 684: debated on Tuesday 17 November 2020. https://hansard.parliament.uk/commons/2020-11-17/debates/19A9B0C7-AFEC-4C25-8E47-5AD68BA4F127/NationalSecurityAndInvestmentBill

23 Letter from Foreign, Commonwealth and Development Office, 29 January 2021. https://www.imperial.ac.uk/media/imperial-college/administration-and-support-services/hr/public/policies/immigration-asylum-and-nationality-act-2006/ATAS-Expansion-to-Researchers-(PDf).pdf

24 Exempt countries include EU countries, the European Economic Area (EEA), Australia, Canada, Japan, New Zealand, Singapore, South Korea, Switzerland and the United States of America. See 'Academic Technology Approval Scheme (ATAS)' guidance, retrieved 31 December 2021. https://www.gov.uk/guidance/academic-technology-approval-scheme

25 DTE Network, *Trusted Research Partnership toolkit*, retrieved 19 December 2021. https://dte.network/trusted-research-toolkit-1

26 Steptoe & Johnson LLP, *UK announces measures to rework export control regime,* 13 December 2021. https://www.lexology.com/library/detail.aspx?g=20012578-4c3e-465e-a5b8-bcaf294ea21e

27 See 'Export controls applying to academic research' guidance, retrieved 31 December 2021. https://www.gov.uk/guidance/export-controls-applying-to-academic-research

28 See CPNI, 'Trusted Research' and 'Trusted Research Guidance for Academia', retrieved 31 December 2021. https://www.cpni.gov.uk/trusted-research ; https://www.cpni.gov.uk/system/files/Trusted%20Research%20Guidance%20for%20Academia.pdf

29 National Cyber Security Centre, retrieved retrived 2 February 2022. https://www.ncsc.gov.uk

30 University and business collaboration agreements: Lambert Toolkit, retrieved 21 December 2021. https://www.gov.uk/guidance/university-and-business-collaboration-agreements-lambert-toolkit

31 ARMA, Due Diligence in International Research – Options for Improved Efficiency, Equity and Quality, 5 March 2021. https://arma.ac.uk/wp-content/uploads/2021/04/Due-Diligence-Report-and-Appendicies.pdf

32 'Trusted Research Guidance for Academia', retrieved 31 December 2021. https://www.cpni.gov.uk/trusted-research-guidance-academia

33 Universities UK, *Managing risks in Internationalisation: Security related issues*, last updated on Wednesday 11 Aug 2021. https://www.universitiesuk.ac.uk/what-we-do/policy-and-research/publications/managing-risks-internationalisation

34 HM Government, *Global Britain in a competitive age: The Integrated Review of Security, Defence, Development and Foreign Policy*, March 2021, p. 36. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/975077/Global_Britain_in_a_Competitive_Age-_the_Integrated_Review_of_Security__Defence__Development_and_Foreign_Policy.pdf

35 HM Government, *Global Britain in a competitive age: The Integrated Review of Security, Defence, Development and Foreign Policy*, March 2021, p. 36. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/975077/Global_Britain_in_a_Competitive_Age-_the_Integrated_Review_of_Security__Defence__Development_and_Foreign_Policy.pdf

36 Mergers – the CMA's jurisdiction and procedure: CMA2, retrieved 21 December 2021. https://www.gov.uk/government/publications/mergers-guidance-on-the-cmas-jurisdiction-and-procedure

37 The full list of sensitive areas includes: Advanced Materials; Advanced Robotics; Artificial Intelligence; Civil Nuclear; Communications; Computing Hardware; Critical Suppliers to Government; Cryptographic Authentication; Data Infrastructure; Defence; Energy; Military and Dual-Use; Quantum Technologies; Satellite and Space Technologies; Suppliers to the Emergency Services; Synthetic Biology; Transport.

38 National Security and Investment Act: Check if you need to tell the government about an acquisition that could harm the UK's national security, 20 July 2021, retrieved 15 January 2021. https://www.gov.uk/guidance/national-security-and-investment-act-guidance-on-acquisitions

39 National Security and Investment Act: prepare for new rules about acquisitions, 20 July 2021, retrieved 15 January 2021. https://www.gov.uk/guidance/national-security-and-investment-act-guidance-on-acquisitions

40 Impact Assessment, National Security and Investment Act, 9 November 2020. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/934276/nsi-impact-assessment-beis.pdf

41 See draft regulation on monetary policies: https://www.legislation.gov.uk/ukdsi/2021/9780348226942/pdfs/ukdsi_9780348226942_en.pdf

42 National Security and Investment Act 2021: Statement for the purposes of section 3, 2 November 2021. https://www.gov.uk/government/publications/national-security-and-investment-statement-about-exercise-of-the-call-in-power/national-security-and-investment-act-2021-statement-for-the-purposes-of-section-3

43 Hansard, *National Security and Investment Bill (Second sitting)*, debated on 24 November 2020. https://hansard.parliament.uk/commons/2020-11-24/debates/baf4f10c-493a-49ec-9fca-8079eacb5a1e/NationalSecurityAndInvestmentBill(SecondSitting)

44 Congressional Research Service, *The Committee on Foreign Investment in the United States (CFIUS)*, 14 February 2020. https://sgp.fas.org/crs/natsec/RL33388.pdf

45 Australian Strategic Policy Institute (ASPI) China Defence University Tracker. https://unitracker.aspi.org.au/

46 CATO Institute, *Human Freedom Index*, 2021. https://www.cato.org/human-freedom-index/2021

47 Australian Strategic Policy Institute (ASPI), *China Defence University Tracker*. https://unitracker.aspi.org.au/

48 Dan Milmo, 'Cambridge is leading regional tech hub as UK draws record investment', *The Guardian*, 20 December 2021. https://www.theguardian.com/technology/2021/dec/20/cambridge-is-leading-regional-tech-hub-as-uk-draws-record-investment

49 Hansard, *National Security and Investment Bill (Second sitting)*, debated on 24 November 2020. https://hansard.parliament.uk/commons/2020-11-24/debates/baf4f10c-493a-49ec-9fca-8079eacb5a1e/NationalSecurityAndInvestmentBill(SecondSitting)

50 Hansard, *National Security and Investment Bill (Second sitting)*, debated on 24 November 2020. https://hansard.parliament.uk/commons/2020-11-24/debates/baf4f10c-493a-49ec-9fca-8079eacb5a1e/NationalSecurityAndInvestmentBill(SecondSitting)

51 Hansard, *National Security and Investment Bill (Second sitting)*, debated on 24 November 2020. https://hansard.parliament.uk/commons/2020-11-24/debates/baf4f10c-493a-49ec-9fca-8079eacb5a1e/NationalSecurityAndInvestmentBill(SecondSitting)

52 Hansard, *National Security and Investment Bill (Second sitting)*, debated on 24 November 2020. https://hansard.parliament.uk/commons/2020-11-24/debates/baf4f10c-493a-49ec-9fca-8079eacb5a1e/NationalSecurityAndInvestmentBill(SecondSitting)

53 The impact assessment of the NSIA describes the limitations of the publicly available data on asset sales and notes this creates a 'considerable limitation' of the analysis. See Impact Assessment, National Security and Investment Act, 9 November 2020. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/934276/nsi-impact-assessment-beis.pdf

54 Hansard, *National Security and Investment Bill. Volume 684*, debated on 17 November 2020. https://hansard.parliament.uk/commons/2020-11-17/debates/19A9B0C7-AFEC-4C25-8E47-5AD68BA4F127/NationalSecurityAndInvestmentBill

55 See Ashley Lenihan and Michael Leiter's evidence in Hansard, *National Security and Investment Bill (Second sitting),* debated on 24 November 2020. https://hansard.parliament.uk/commons/2020-11-24/debates/baf4f10c-493a-49ec-9fca-8079eacb5a1e/NationalSecurityAndInvestmentBill(SecondSitting)

56 National Security and Investment Act: Check if you need to tell the government about an acquisition that could harm the UK's national security, 20 July 2021, retrieved 24 December 2021. https://www.gov.uk/guidance/national-security-and-investment-act-guidance-on-acquisitions

57 Independent Report, *Review of research beaucracy*, 22 March 2021. https://www.gov.uk/government/publications/review-of-research-bureaucracy

58 The guidance on ATAS certificates states that 'If you're a researcher on a Standard visitor visa attending meetings, conferences, seminars or interviews, or giving speeches, and will not be undertaking research during your time in the UK, you do not need to apply for ATAS clearance.' See 'Find out if you need an ATAS certificate', 14 May 2021. https://www.gov.uk/guidance/find-out-if-you-require-an-atas-certificate#when-you-need-an-atas-certificate

59 Department for Business, Energy and Industrial Strategy, Dedicated government team to protect researchers' work from hostile activity', 25 May 2021. https://www.gov.uk/government/news/dedicated-government-team-to-protect-researchers-work-from-hostile-activity

60 For example, see a recent job advertisement from the University of Leeds for a Trusted Research Environment Manager posted 6 January 2022. https://jobs.leeds.ac.uk/Vacancy.aspx?ref=CSRIS1217

61 Universities UK, *Managing risks in Internationalisation: Security related issues*, last updated 11 Aug 2021, p. 15. https://www.universitiesuk.ac.uk/sites/default/files/uploads/Reports/managing-risks-in-internationalisation.pdf

62 SPRITE+, 'How do researchers understand "Trusted Research"? Findings of a SPRITE+ Workshop held March 2021', 2021, p. 5. https://spritehub.org/wp-content/uploads/2021/08/2021-SPRITE-TR-Workshop-summary-FINAL.pdf

63 SPRITE+, 'How do researchers understand "Trusted Research"? Findings of a SPRITE+ Workshop held March 2021', 2021, p. 7. https://spritehub.org/wp-content/uploads/2021/08/2021-SPRITE-TR-Workshop-summary-FINAL.pdf

64 University of Cambridge 'Trusted Research'; 'Responsible Collaboration' https://www.research-integrity.admin.cam.ac.uk/trusted-research; https://www.strategic-partnerships.admin.cam.ac.uk/managing-risks-international-engagement/responsible-collaboration

65 University of Manchester, 'Trusted Research'; 'Export Controls', retrieved 20 December 2021. https://www.staffnet.manchester.ac.uk/rbe/rs/preparing/trusted_research/; https://www.staffnet.manchester.ac.uk/export-controls-info/resources/-research/

66 DTE Network, Trusted Research Partnership toolkit, retrieved 19 December 2021. https://dte.network/trusted-research-toolkit-1

67 University of Cambridge, 'Trusted Research Checklist', retrieved 20 December 2021. https://www.research-integrity.admin.cam.ac.uk/trusted-research-checklist

68 University of Manchester, 'Trusted Research', retrieved 19 December 2021. https://www.staffnet.manchester.ac.uk/rbe/rs/preparing/trusted_research/

69 University of Bath, 'Trusted Research: Protecting you and your research', retrieved 23 December 2021. https://www.bath.ac.uk/guides/trusted-research-protecting-you-and-your-research/; University of Strathclyde, link to CPNI's 'Checklist: Evaluating research proposals', retrieved 20 December 2021. https://www.strath.ac.uk/media/1newwebsite/departmentsubject/researchintegrity/Trusted_Research_Checklist_for_Academia.pdf

70 University of Oxford, Strategic Partnerships Scorecard, retrieved 29 December 2021. https://globalresearch.admin.ox.ac.uk/strategic-partnership-scorecard

71 University of Nottingham, 'Trusted Research Toolkit: keeping our international partnerships safe', 25 May 2021. https://exchange.nottingham.ac.uk/blog/trusted-research-toolkit-keeping-our-international-partnerships-safe/

72 University of Cambridge, 'Managing Risks in International Engagement', retrieved 18 December 2021. https://www.strategic-partnerships.admin.cam.ac.uk/managing-risks-international-engagement

73 University of Cambridge, 'Managing Risks in International Engagement', retrieved 18 December 2021. https://www.strategic-partnerships.admin.cam.ac.uk/managing-risks-international-engagement/principles-managing-international-risks

74 University of Nottingham, 'Trusted Research Toolkit: keeping our international partnerships safe', 25 November 2021. https://exchange.nottingham.ac.uk/blog/trusted-research-toolkit-keeping-our-international-partnerships-safe/

75 University of Manchester, 'Due Diligence for Research Collaborators', retrieved 18 December 2021. https://www.staffnet.manchester.ac.uk/rbe/rs/preparing/research-collaborations/

76 SPRITE+, 'How do researchers understand "Trusted Research"? Findings of a SPRITE+ Workshop held March 2021', 2021, p. 7. https://spritehub.org/wp-content/uploads/2021/08/2021-SPRITE-TR-Workshop-summary-FINAL.pdf

77 Cranfield University, 'Cranfield University awarded £200,000 to lead on export control training in UK higher education', *FE News*, 14 October 2021. https://www.fenews.co.uk/skills/cranfield-university-awarded-200-000-to-lead-on-export-control-training-in-uk-higher-education/

78 Department of Home Affairs, *Submission to the inquiry into national security risks affecting the Australian higher education and research sector*, 18 December 2020. https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/NationalSecurityRisks/Submissions

79 Parliamentary Joint Committee on Intelligence and Security – 11 March 2021 – National security risks affecting the Australian higher education and research sector. https://www.aph.gov.au/Parliamentary_Business/Hansard/Hansard_Display?bid=committees/commjnt/4799720b-bfa4-43b4-baa7-57aed7755dbc/&sid=0000

80 Royal Academy of Engineering, A Q&A with Sir Patrick Vallance FRS FMedSci and guests, 13 December 2021. https://www.raeng.org.uk/events/events-programme/2021/december/delivering-uk-strategic-advantage-in-science-and-t

81 Ian Andrews, 'A College for National Security (and Resilience?)', National Preparedness Commission, 15 June 2021. https://nationalpreparedness-commission.uk/2021/06/a-college-for-national-security-and-resilience/

82 The British Academy, *Innovation Fellowships Scheme – Route B (Policy-led): Scheme guidance notes*, retrieved 17 December 2021. https://www.thebritishacademy.ac.uk/funding/innovation-fellowships-scheme-route-b-policy-led/innovation-fellowships-scheme-route-b-policy-led-scheme-guidance-notes/

83 Home Office, *Consultation document: legislation to counter state threats (accessible version)*, last updated 22 November 2021. https://www.gov.uk/government/consultations/legislation-to-counter-state-threats/consultation-document-legislation-to-counter-state-threats-accessible-version

84 The Royal Society, *Submission to the Home Office consultation on Legislation to Counter State Threats (Hostile State Activity)*, 22 July 2021. https://royalsociety.org/-/media/policy/Publications/2021/07-22-21-royal-society-submission-to-home-office-consultation-on-state-threats.pdf

85 Congressional Research Service, *Foreign Agents Registration Act (FARA): A Legal Overview*, 25 February 2020. https://sgp.fas.org/crs/misc/IF11439.pdf

86 John Morgan, 'English sector "won't be open on foreign donations unless forced"', *Times Higher Education*, 17 January 2022. https://www.timeshighereducation.com/news/english-sector-wont-be-open-foreign-donations-unless-forced

87 See Section 117 of the Higher Education Act of 1965 (HEA), 20 U.S.C. 1011f.

88 Independent Review of Research Bureaucracy – Interim Report, January 2022. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1046070/independent-review-of-research-bureaucracy-interim-report.pdf

89 Parliamentary Joint Committee on Intelligence and Security, hearing on National security risks affecting the Australian higher education and research sector, 19 March 2021. https://www.aph.gov.au/Parliamentary_Business/Hansard/Hansard_Display?bid=committees/commjnt/3ca6fe4f-b221-48f6-812e-ccfd3cd59d55/&sid=0005

Trustees

Professor Sally Mapstone (Chair)
Sir David Bell
Mary Curnock Cook CBE
Professor Dame Julia Goodfellow
Professor Dame Helen Wallace

Advisory Board

Alison Allden OBE
Professor Carl Lygo
Professor David Maguire
Professor Nick Pearce
Professor Iyiola Solanke
Professor Mary Stuart

President

Bahram Bekhradnia

Partners

Advance HE
BPP University
Coursera
Elsevier
GatenbySanderson
Handshake
iQ Student Accommodation
Kaplan
Lloyds Bank
Mills & Reeve LLP
Pearson
Research England
Taylor & Francis
Times Higher Education
Unite Students
UPP Group Limited

The increasingly global nature of UK research has come with associated risks for national security. Both the UK Government and the higher education sector have responded to these risks through a range of initiatives, including guidance for researchers from the Centre for the Protection of National Infrastructure (CPNI), new legislation such as the National Security and Investment Act (2021), and the formation of the Research Collaboration Advice Team (RCAT).

This report surveys the scene, reviewing the latest initiatives in this space and exploring what the impacts of new legislation may be. It argues that, despite significant progress and several joint initiatives emerging from both the sector and the Government to counter security threats, significant challenges remain in terms of coordination, communication and resources. While universities can do more to raise awareness of security issues with their researchers, any new legislative measures must also be carefully designed to avoid increasing administrative burdens in counterproductive ways. It concludes with recommendations for policymakers and universities on how to streamline and coordinate efforts in this space going forward.

HEPI was established in 2002 to influence the higher education debate with evidence.
We are UK-wide, independent and non-partisan.
February 2022 ISBN 978-1-908240-90-3
Higher Education Policy Institute
99 Banbury Road, Oxford OX2 6JX
www.hepi.ac.uk

Printed by BCQ, Buckingham
Typesetting: Steve Billington, www.jarmanassociates.co.uk