



Wilton Park



Report

## Enhancing security to support international collaboration in the Higher Education sector – exploring ‘Trusted Research’

Tuesday 12 November 2021 | WP1999V

In partnership with:



UK Research  
and Innovation



Universities  
UK



In association with:



Security, Privacy, Identity, Trust,  
Engagement, NetworkPlus



## Report

# Enhancing security to support international collaboration in the Higher Education sector – exploring ‘Trusted Research’ | WP1999V

Tuesday 12 November 2021 | WP1999V

In partnership with UKRI, UUK, UUKi and in association with SPRITE+.

## Background

Governments internationally are concerned that academic research and innovation could be exploited by state or state-linked actors which do not respect fundamental rights and freedoms or who are hostile to UK interests; the ‘trusted research’ initiative was developed to consider how to respond to rising concerns among UK universities about how best to protect their staff, research and infrastructure when collaborating with international partners, to ensure that universities can continue to collaborate whilst maintaining the protection of UK interests.

The UK is a top destination for foreign students, who not only contribute to the culture and diversity of institutions but provide a key source of funding for UK universities. The UK has a thriving research and innovation sector that attracts investment from across the world, with more than half of UK research being a product of international partnerships. Developing and maintaining these international collaborations is critical to the success of UK research and innovation, and there is a call for academia and partner countries to share knowledge and examine best practices to identify strategies and actions to protect higher education (‘HE’) institutions from hostile or unethical interference by state or state-linked actors.

Featuring representatives from the HE sector, as well as representatives from the Centre for the Protection of National Infrastructure (‘CPNI’), UK Research and Innovation (‘UKRI’), and the government’s recently formed Research Collaboration Advice Team (‘RCAT’), this dialogue aimed to identify strategies to enhance the security of the HE sector through sharing experiences and best practice to align security priorities, policies and messaging across the HE sector and government departments. It sought to raise awareness of the prevalent threat to the HE sector, strengthen the links between the government and the HE sector, identify opportunities to work collaboratively across the agenda, and support the development and dissemination of support, advice and guidance

This report should be read in conjunction with the scenario that was used to generate discussion at the event (see Annex I).

## Key points

- There are a number of risks impacting on HE institutions and their staff. The institutions themselves face interconnected reputational, legal, and financial risks related to trusted research, as well as potential damage to the culture of openness that enables research collaboration. But support is also required to reinforce the personal well-being of academics, students and personnel caught up in potential issues related to trusted research.
- Striking a proportionate and appropriate balance between promoting international collaboration and protecting national security and investments is key. The creation of

RCAT to coordinate interaction between the government and the HE sector will be crucial in calibrating the right level of response to risks and threats, while making the fragmented approach towards trusted research more coherent and easier for the HE sector to navigate.

- The HE sector has the opportunity to demonstrate a responsive, dynamic and proactive approach to mitigating risks around trusted research, ensuring all research collaborations and relationships are aligned around shared visions and values to support open, safe and secure international partnerships. A proactive, pre-emptive approach that allows for effective self-regulation would be preferred over the imposition of stringent government regulation or further, and possibly more restrictive, legislation around trusted research. There is an opportunity for the sector to work collectively to establish new mechanisms to manage risks as well as highlight and strengthen existing mechanisms.
- Only cultural change can foster a truly proactive approach. More should be done to ensure that the risks around trusted research are properly understood to address a lack of awareness across the research community. But what is also required is a whole system approach to ensure that institutions and organisations recognise the wide range of activities that should be covered by trusted research frameworks and principles, including teaching, students' data, facilities and personnel.
- The situation around trusted research should not be catastrophised – in many ways international partnerships are stronger and more productive than ever, as is the appetite from the sector to work together in response to this agenda. There is clear value in international research collaboration, and the benefits should be recognised and promoted at the same time as the areas of risk are highlighted.

## Summary of discussions

### Risks and threats in international collaboration

1. **Adversaries' methodologies of stealing, spying on, or subverting research are evolving**, so government and the HE sector should collaborate to remain agile and adaptable in their responses to changing threats in order to minimise the potentially negative implications for academic freedom. These threats do not necessarily come from those countries most readily identified as likely actors and whose activities are being carefully handled through diplomatic channels (China, Russia, North Korea, Iran) but can also be from a wide range of countries and actors with varied motives.
2. Discussing sensitive information uncovered through specific government powers with HE institutions **risks disclosing confidential methods and sources**. The CPNI and RCAT would find it easier to discuss specific risks and threats if there was an improved repository of open-source information that could corroborate their intelligence. The risk of not sharing this information, and details of specific cases, is that decisions would then be made from an ill-informed position. There is therefore a need for multiple fora and mechanisms to help drive this ambition, with clarity around expectations and requirements and with more key people in the academic community, especially in science and technology given appropriate security clearances so they can be privy to classified information about different threats.
3. **HE institutions often lack country and actor specific knowledge** to help manage and mitigate risks around international collaboration. HE institutions should engage with in-house academics and research specialists and use their deep knowledge to help make more informed decisions and improve pre-collaboration on due diligence; these experts could help provide the kind of open-source intelligence that is perceived as lacking. Government responsibility in support of this should be to share information transparently, appropriately and in a timely fashion to inform decision-taking and risk management whilst overall encouragement needs to be given for greater engagement

between HE institutions and the security community.

4. There is a perception amongst HE institutions that being seen to report trusted research concerns to government could impact negatively on their reputation, and in turn their international partnerships and funding sources. **To mitigate this, there is a need for HE institutions and government to demonstrate a collective responsibility** across the sector to help colleagues to focus on how prepared or otherwise they are by taking steps to explain clearly why maintaining a degree of collaboration with a certain country is important and should be continued. As well as exchanging knowledge this could also focus on developing shared policy approaches, such as around the ethics of AI.
5. Media exaggeration and inaccurate supposition can be unhelpful, and the overall position would be improved if inaccuracies and suppositions could be rebutted, without undermining the security position.
6. There are implications from this not only for the institutions but importantly also for the people who are targeted as a result. In some cases, **media reporting and other pressures on staff and students can affect their well-being**, with the often broad and vague fallout leading to many being inadvertently implicated and unfairly treated with suspicion.
7. **The focus of risk mitigation should not only be on classic academic research, but also across the research and innovation pipeline.** . Government and the HE sector should adopt a broad perspective of potential threats – acknowledging, for example, that it may be easier for hostile parties to steal UK intellectual property from one of the start-ups, spin offs, and consultancies that form in and around HE institutions rather than from the institutions themselves.
8. Similarly, **the trusted research agenda should not be limited to emerging and dual use technology**; statements about dual use are hard to validate, as they are constantly evolving. It might be impossible therefore to control research in areas like AI when technology can be so easily repurposed. There is a great deal of complexity, that defies an easy fix, around the trusted research issue, and the government and HE sector should work through this together to identify solutions acceptable to both and continue to reflect the dynamic and evolving nature of trusted research.

#### **A fragmented approach**

9. **The landscape around trusted research compliance and risk mitigation is complex, fragmented, and hard to navigate**, both in terms of the government's communication around requirements and the interconnectedness of those requirements with HE institutions. There are good examples where HE institutions have embedded systems for assessing risk but collective improvements would help ensure consistency across the sector. HE institutions have the opportunity to ensure their own systems are sufficiently integrated so that there is a single 'point of truth' about the people and organisations they have relations with, that can be clearly communicated to external stakeholders, including government. HE institutions need 360-degree reviews to identify the overall situation and level of understanding around Trusted Research, including how government interventions relate and work together.
10. **Participants welcomed the formation of RCAT**, announced by the Department for Business, Energy & Industrial Strategy in May 2021 and due to be launched in 2022. Designed to be the first point of contact for HE institutions with trusted research-related concerns, RCAT advisors will work closely with HE institutions to identify potential risks institutions might face and possible mitigation they could adopt. RCAT will create greater understanding between the HE sector and the government, and connect HE

institutions to other government partners, such as the Export Control Joint Unit, the Investment Security Unit (in BEIS) or CPNI, should the need arise.

11. Participants from the HE sector **called for RCAT to provide up to date and timely advice** on what threats they may be exposed to, as well as clear communication of government policy. Overall, RCAT should help develop and enable a sector-wide response to the issue of trusted research that is not limited to individual institutions.

### Raising awareness

12. **Awareness of the issues around the trusted research agenda should be raised** among academics to provide assurances that it is not a way to spy on colleagues, which academics sometimes fear. There should be more openness about any conflicts of interest or dependencies that researchers and/or institutions might have. **A set of test cases** demonstrating the potential complexity and subtlety of trusted research challenges, including positive examples of international collaborations that are conducted safely and effectively, could be very helpful for HE institutions to sensitise staff to the nature of different risks and threats. The key is to evidence to colleagues that this is work being done for and with them, not to them.
13. Cultural change is already underway in relation to trusted research, but there is an opportunity to strengthen and raise visibility of good practice more broadly across the HE sector, to embed this cultural change routinely in the same way as the equality, diversity and inclusion agenda has become integrated into HE institutions' daily work. There are wider aspects for consideration – IP, for example – and so institutions need to be alive to the risks across these other spaces rather than seeing this as an issue that only impacts PIs. This will be challenging in several respects, not least because Principal Investigators pride themselves on their entrepreneurial skills and academic freedom, and therefore may prioritise securing funding over national prosperity and security.
14. The UK could **learn lessons from other approaches to trusted research**. The USA's National Science Foundation ('NSF'), for instance, has a list of 'catechisms', such as 'can the terms of engagement be clearly stated in writing?', and 'can you trace where all the funding comes from?'. The USA also have Information Sharing and Analysis Centers ('ISACs') focussed on cybersecurity and are considering establishing ISACs for research security too; in this event there could be an opportunity for coordination with the RCAT. There are obligations on HE institutions in the USA that receive grants over a certain threshold, and the USA requires public reporting of foreign donations to the Department of Education. The NSF is also going to fund research security training modules in the USA that will be made openly available to all.
15. **Other approaches to trusted research include the OECD's**, whose member states now see information leakage as a serious threat to national and economic security; the organisation is holding international workshops and collating data on members' experiences and approaches toward trusted research which the UK could learn from. **The G7 has put together a toolkit for training** on research security best practices which could help coordinate international thinking on trusted research challenges and opportunities. The G7's research compact tagline: 'open as possible, secure as necessary', received wide approval from participants.
16. The HE sector could also **learn lessons from certain industries**, such as the defence industry, which have the kind of clear guidance over prohibited activity that the HE sector would benefit from further developing.

### Regulation

17. **HE institutions should continue to improve and demonstrate self-regulation around trusted research to reduce the risk that government may impose broad**



**regulation and legislation, with a resultant further risk of this impacting negatively on academic freedom** To avoid this HE institutions should demonstrate that trusted research is part of their values and incorporate it into their culture. One approach could be to encourage staff participation in the governance of universities' international partnerships. Participants acknowledged that the **HE sector has a limited window to shape the regulatory response that it should not squander**.

18. The sense that the UK government and security committee wants a more stringent regulatory approach, especially talk of registers, is raising concern in the research community, which **questions the effectiveness of more government regulation and legislation with regards to trusted research**. Collaboration between government and the HE sector, as well as cultural change, will work more effectively than new a set of rules and regulations that may not effectively address the problem. Any regulation should not raise barriers to international collaboration but enable it to thrive in a safe and secure way.
19. **Creating and maintaining mutually supportive links between the HE sector, and government is essential**. There should be more opportunity for collaborative work between the HE sector and government, with opportunities for sharing information and best practice. RCAT, which will be at the heart of this process, could look into coordinating a joint statement from the HE sector and government on the values they share concerning trusted research.
20. Instead of a 'box-ticking' approach to compliance, some participants thought there should be **more emphasis on personal integrity and individual responsibility** for academics to bring the trusted research agenda into their work, avoiding the burdensome bureaucracy that regulation could bring. Opportunities should be identified to support engagement with academics and how to increase visibility of their role with regards to Trusted Research and Innovation.
21. HE institutions are already demonstrating a 'proactive' approach towards building systems and processes around trusted research aimed at mitigating risks and threats. Working together with the RCAT will further the opportunities to strengthen and build on this approach as well as provide consistency and efficiency. Examples from participants included the scrutinising of grants by an expert panel; laying out researchers' responsibilities around trusted research in the grant award letter; and making grantees tick a box to say they have read the trusted research materials. HE institutions could also institute more robust processes like review boards. Though a burden, without taking these steps there is a risk that more hard-line stakeholders may intervene, shutting down potentially beneficial research opportunities in the future.
22. **Data on the effects of countries' different mitigation strategies around trusted research is lacking**. The NSF will soon start research to fill this knowledge gap and the UK should monitor the results closely. The government and HE institutions should cooperate to identify what specific, tangible outputs can be achieved, without getting bogged down in the broader context.

### Academic freedom

23. **Participants emphasised that with academic freedom comes responsibility**. On the one hand, there is concern in some quarters about the possibility that government overreach in both the UK and elsewhere could damage research partnerships and collaborations. On the other hand, HE institutions should recognise their role and collective responsibility to national prosperity and security, especially when projects receive UK government funding.

24. Leaving HE institutions free to pursue **collaborative research opportunities in states with which the UK has challenging political relations can be both valuable and viable when appropriately managed.** One participant pointed to the UK's and Russia's research in arctic science; this world leading, peer reviewed research goes beyond political differences and has enabled conversations between the two governments on climate change, deforestation and broader science diplomacy and soft power initiatives that would otherwise not have been possible.
25. Many participants emphasised the importance of developing greater **trust between government, HE institutions, and academics, particularly in the face of increasing misinformation on the one hand and a lack of information on the other.** Some participants believed trust between academics and the heads of research organisations to be very low, while trust between academics and researchers is similarly undermined by competition over funding. Participants also noted the lack of trust between the government and the HE sector, with the latter extremely wary of the former's potential to impose additional, unpopular, and potentially ineffective, regulatory burdens.
26. Others argued that trust should not form the basis of cooperation between the government and HE institutions; rather, the HE sector should continue its measures to get below the surface of government statements by talking to stakeholders who work on trusted research to understand what the drivers behind the government's position really are, a role that RCAT would be well-placed to fulfil.

### **James Bolton-Jones**

Wilton Park | December 2021

Wilton Park reports are intended to be brief summaries of the main points and conclusions of an event. Reports reflect rapporteurs' accounts of the proceedings and do not necessarily reflect the views of the rapporteur. Wilton Park reports and any recommendations contained therein are for participants and are not a statement of policy for Wilton Park, the Foreign, Commonwealth and Development Office (FCDO) or Her Majesty's Government.

Should you wish to read other Wilton Park reports, or participate in upcoming Wilton Park events, please consult our website [www.wiltonpark.org.uk](http://www.wiltonpark.org.uk). To receive our monthly bulletin and latest updates, please subscribe to <https://www.wiltonpark.org.uk/newsletter/>.

### **Annex I**

#### **Scenario:**

A UK broadsheet newspaper has published a series of articles outlining collaborative partnerships between your university and institutions in China which are known to have links to China's military industrial complex and overseas talent programmes. Immediately prior to publication, the newspaper reached out to the university for comment, to which a brief response was provided.

Throughout a series of articles and interviews published over the course of the last week, the newspaper has disclosed details on a range of different types of these partnerships by your university. These include high levels of under- and post-graduate student intakes from China, collaborative research partnerships funded by UKRI that span a wide spectrum of disciplines and technologies, as well as a jointly funded center on a key emerging research area established last year.

It is also suggested that there has already been a potential loss of sensitive information and wrongdoing resulting from undue foreign interference on one of the collaborative research projects identified. The article provides the names, occupations and affiliations of a number of UK and non-UK based partners involved in these projects.

As well as highlighting the risks around the security of the intellectual property and sensitive information within these partnerships, the newspaper argues that your university is also

suppressing free speech and transparency by not being forthcoming about these links and their associated risks. In doing so, the articles conclude that your university has demonstrated an over-reliance on funding from China and needs urgent redress in order to help mitigate the current risk exposure.

Subsequent follow-up articles have also appeared in a number of other UK and international media outlets, as well as on social media channels. As well as the university, requests for comment were also made by to UKRI – as the funding agency for the research projects named, and the UK government, including a number of government supported facilities identified in the articles.