
CPNI
Centre for the Protection
of National Infrastructure
TRUSTED
RESEARCH
GUIDANCE FOR ACADEMICS
National Cyber
Security Centre
a part of GCHQ

The UK has a thriving research and innovation sector that attracts investment from across the world. More than half of UK research is a product of international partnerships. **Trusted Research** aims to secure the integrity of the system of international research collaboration, which is vital to the continued success of the UK's research and innovation sector.

# TABLE OF CONTENTS

# INTRODUCTION



## TRUSTED RESEARCH

Trusted Research aims to support the integrity of the system of international research collaboration, which is vital to the continued success of the UK's research and innovation sector. It is particularly relevant to researchers in STEM subjects, dual-use technologies, emerging technologies and commercially sensitive research areas. The advice has been produced in consultation with the research and university community and is designed to help the UK's world-leading research and innovation sector get the most out of international scientific collaboration whilst protecting intellectual property, sensitive research and personal information.

Trusted Research:

- Outlines the **potential risks** to UK research and innovation
- Helps researchers, UK universities and industry partners to have **confidence in international collaboration** and make **informed decisions** around those potential risks
- Explains how to **protect research** and **staff** from potential theft, misuse or exploitation

## THE UK AND BEYOND: RESEARCH & COLLABORATION AT A GLANCE

A fifth of the world's scientific papers are produced through international collaboration, and these partnerships play a vital role in scientific progress.[1]

The UK champions a rules-based system, which has served our interests as a global, outward-facing nation and continues to be of vital importance. This system has enabled global cooperation to protect shared fundamental values of respect for human dignity, human rights, freedom, democracy and equality. For academia this is demonstrated by the importance the UK places on the protection of academic freedom, something which is enshrined in law.[2]

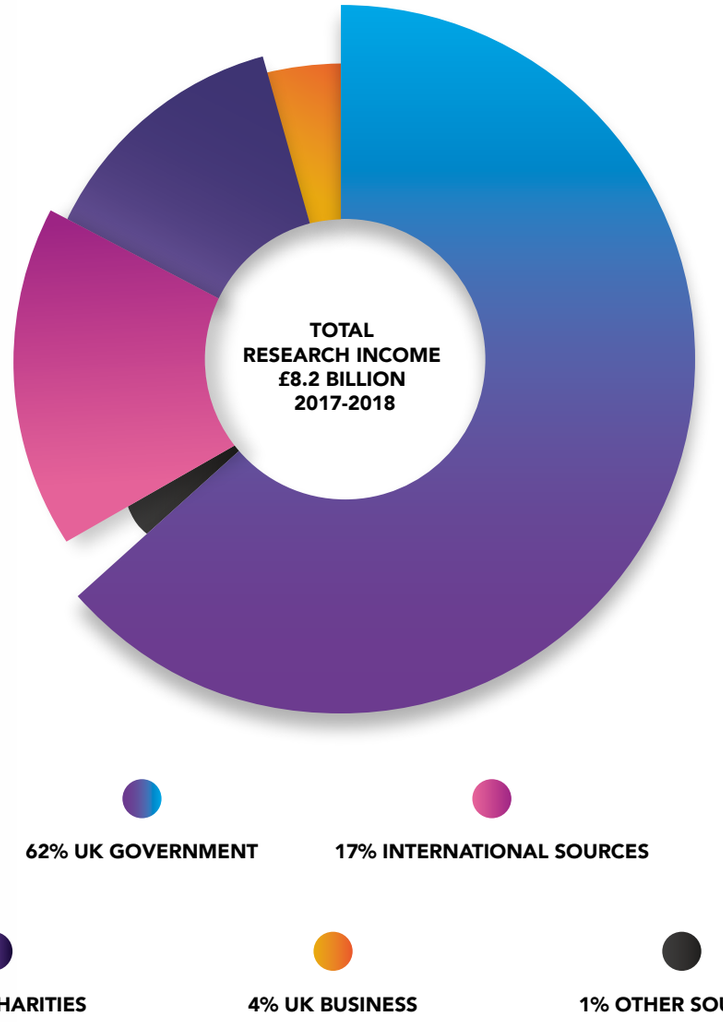
Universities in the UK work closely with partners from across the world - more than half of UK research is a product of international partnerships. These international relationships extend further than research funding and collaboration; 42% of postgraduates and 31% of staff in universities are from outside the UK.[3] Developing and maintaining these international relationships is key to the success of UK research and innovation. The Department for Business, Energy & Industrial Strategy (BEIS) published the UK International Research and Innovation Strategy,[4] which sets out a goal for the UK to be the partner of choice for international research and innovation for the long term.

[1] Universities UK, Higher Education Research in Facts and Figures, 2017
[2] The Education Reform Act 1988
[3] Universities UK, Higher Education Research in Facts and Figures, 2017
[4] https://www.gov.uk/government/publications/uk-international-research-and-innovation-strategy



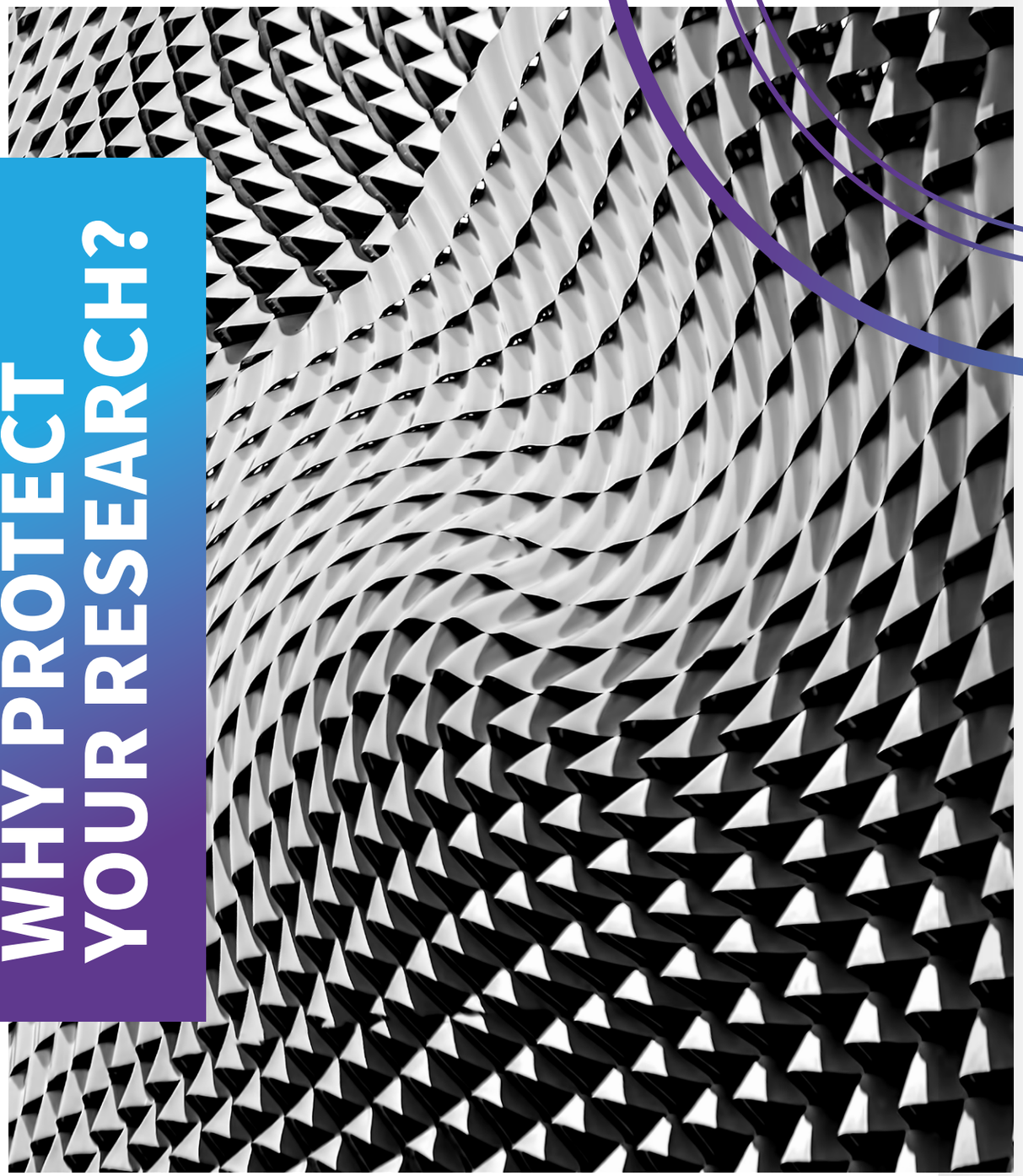
## MORE THAN £1 BILLION OF RESEARCH INCOME COMES FROM OVERSEAS

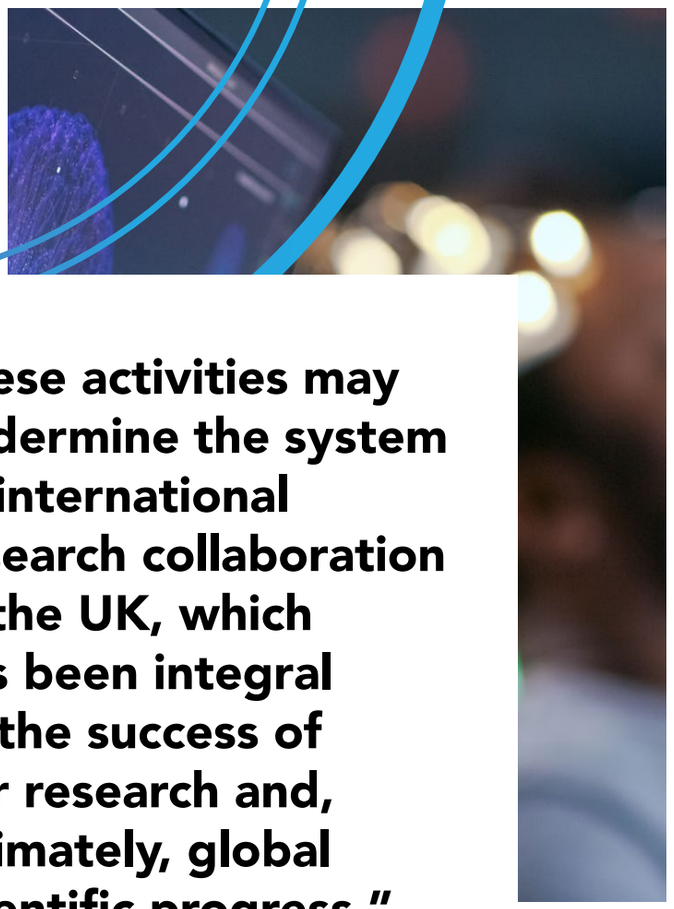
In 2017-18, UK universities received £8.2 billion in research income, £1.39 billion of which came from international sources.[5]




[5] Universities UK, Higher Education in Facts and Figures, 2018

# WHY PROTECT YOUR RESEARCH?





**"These activities may undermine the system of international research collaboration in the UK, which has been integral to the success of our research and, ultimately, global scientific progress."**

Whether you hold sensitive medical data for genetic research or commercially sensitive information on behalf of a research sponsor or business, protecting your research is important to you, your institution and your partners.

Joint research is vulnerable to misuse by organisations and institutions who operate in nations whose democratic and ethical values are different from our own. It allows them to work with experts in a field of cutting-edge research and innovation, and obtain the resulting output of that work, all without having to steal it (e.g. through cyber espionage). It provides those with hostile intent overt access to expertise, IT networks and research. These activities may undermine the system of international research collaboration in the UK, which has been integral to the success of our research and, ultimately, global scientific progress.

## “All research can be at risk, but areas around applied research are particularly vulnerable”

**All** research can be at risk, but areas around applied research are particularly vulnerable, especially where there is a specific problem that you are seeking to solve, or where you are trying to develop a commercial application. In these cases, the consequence of research outcomes being exploited could be far greater and could result in the loss of intellectual property and misuse of your research.


For individual researchers, interference with (or loss of) research is likely to limit your ability to publish first or take credit for the resulting intellectual property. This could negatively affect your reputation and ability to demonstrate the impact of your research.

# WHO ARE YOU AT RISK FROM?

**"A hostile state is one whose democratic and ethical values are different from our own and whose strategic intent is hostile to the UK."**

A hostile state may:

- seek opportunities to increase its own economic advantage, in particular to develop a research and innovation base to increase military and technological advantage over other countries
- prioritise the stability of its regime and focus on preventing internal dissent or political opposition
- seek to deploy its technological and military advantages against its own people in order to maintain the stability of the regime

### MEMORANDUM OF UNDERSTANDING

A university signs a memorandum of understanding (MoU) to collaborate on research into facial recognition technology with an overseas university. As part of the proposal, the overseas university commits to provide significant funding and to sponsor two research fellows. The university conducts in-depth due diligence, including financial assurance and checking compliance with export control legislation. A year into the research, a newspaper publishes an exposé highlighting well-publicised details of the overseas university's work with the military and police of their country to support surveillance and repression of dissent to the political leadership.





## HOW MIGHT YOU BE TARGETED?

Hostile state actors are targeting UK universities to steal personal data, research data and intellectual property[4] and this could be used to help their own military, commercial and authoritarian interests.

International collaboration offers hostile state actors the opportunity to benefit from research without the need to undertake traditional espionage or cyber compromise. Collaboration can provide those with hostile intent access to people, IT networks, and participation in research which may be sensitive or have sensitive applications.

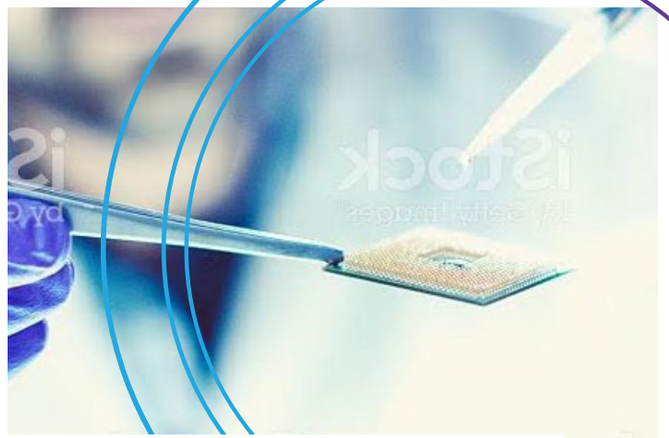
Individual researchers may be targeted by a hostile state actor, but equally you may also be targeted by an academic institution to undertake research which is of strategic benefit to that country.

Traditional academic engagement provides an easy route for a hostile foreign intelligence service to gain access to you, for example at a conference or research placement.

You might also be targeted through a cyber attack, such as a phishing email, which might try to trick you into revealing sensitive information or contain links to a malicious website or infected attachment.

[4]NCSC Cyber Threat to Universities Assessment 2019

# WHAT ARE THE RISKS TO YOUR RESEARCH?



**"If your research is obtained by a hostile state actor, whether through legitimate means or not, you and your research could be affected in a number of other ways"**

Academic competition and plagiarism will be familiar concerns to many working in the field of research and innovation. If your research is obtained by a hostile state actor, whether through legitimate means or not, you and your research could be affected in a number of other ways:

# Identify the risks

## TRUST

Conducting research in a way that maintains the trust of the public and private industry is vital to the continued success of the sector. Researchers need to demonstrate that you can meet the expectations of that trust in order to access sensitive data and funding. If the data on which your research depends is stolen, inappropriately protected or misused, this may mean that your institution is not trusted with such data in the future.

## INTEGRITY

The integrity of your research methodology is as important as the integrity of the research data and outcomes. In addition to the ethical framework surrounding research, consideration should also be given to compliance with legislation and regulation such as General Data Protection Regulation (GDPR), export control and the Academic Technology Approval Scheme (ATAS). Each of these has its own conditions, and complying with one will not satisfy the conditions of the other two. Failure to comply with legislation may expose you to criminal charges or litigation.

## CUMULATIVE RISK

At an institutional and even a departmental level there is a significant risk of over-dependence on a single source of funding, whether that is from a single organisation or from a single nation. Such over-dependence creates the opportunity for funders to exercise inappropriate leverage across a range of areas, for example, pressurising an organisation where it seeks to protect freedom of speech or even academic freedom.



## FINANCIAL LOSS

You and your institution may find it difficult to attract future funding if it were to be discovered that your research had been stolen by a foreign state who may not impose the same sort of controls and protections around the privacy of that data, or might seek to misuse it for unethical purposes. You could face financial loss if a competitor were to access research data or information owned by your sponsor.

## REPUTATION

Your reputation and the reputation of your institution is critical to your future individual and institutional success. Your reputation could be damaged if it were to become apparent that your research had been exploited by the military of another country.

### REPUTATIONAL RISK

A university provided a course on cyber security, which included modules on how to hack into secure IT networks. A national newspaper published details of two North Korean students who were studying on the course and allegedly had links to political figures in the North Korean state, shortly after the hack of Sony by alleged North Korean cyber actors.

# HOW MUCH OF A TARGET ARE YOU?

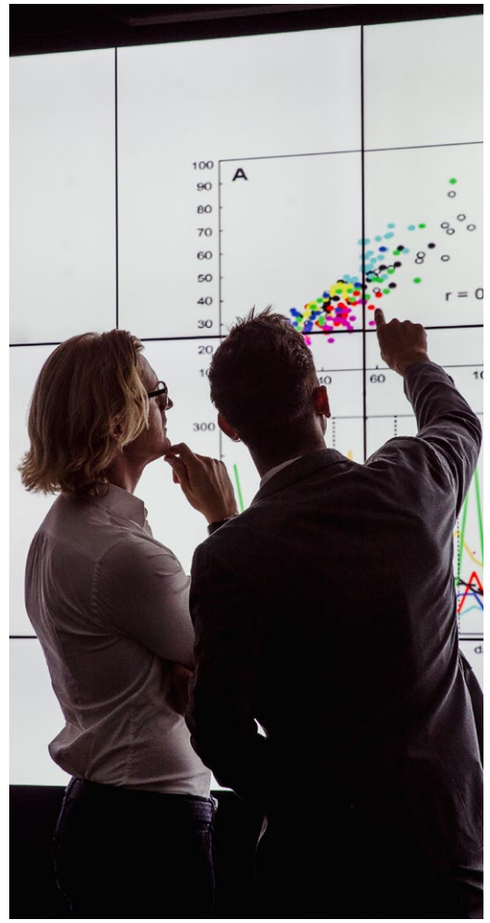
The first step is to have an awareness of the potential threat and this needs to be combined with an understanding of what you want to protect. This should involve identifying what you value the most - the **'crown jewels'** of your work.

## "Being clear on what areas of research are sensitive is critical"

Most research will not have any sensitive application and will not cause concern, but being clear on what areas of research are sensitive is critical.

You need to consider whether your research is commercially sensitive, has potential for patent, is related to sensitive defence or national security technology and/or could have future dual-use or unethical applications.

In most cases, as an expert in your field, you are ideally placed to judge the potential interest and broader application of your research. Some research will be subject to export control and the Department of International Trade's Export Control Joint Unit (ECJU) will be able to advise – For instructions on how to contact the ECJU, please see the *Further Information* section.



# Things to consider:

ARE THERE ANY POTENTIAL ETHICAL OR MORAL CONCERNS FOR THE APPLICATION OF YOUR RESEARCH?

COULD YOUR RESEARCH BE USED TO SUPPORT ACTIVITIES IN OTHER COUNTRIES WITH ETHICAL STANDARDS DIFFERENT FROM OUR OWN, SUCH AS INTERNAL SURVEILLANCE AND REPRESSION?

COULD YOUR RESEARCH BE OF BENEFIT TO A HOSTILE STATE MILITARY OR BE SUPPLIED TO OTHER HOSTILE STATE ACTORS?

ARE THERE ANY DUAL-USE (BOTH MILITARY AND NON-MILITARY) APPLICATIONS TO YOUR RESEARCH?

IS ANY OF THE RESEARCH LIKELY TO BE SUBJECT TO UK OR OTHER COUNTRIES' EXPORT LICENCE CONTROLS?

DO YOU NEED TO PROTECT SENSITIVE DATA OR PERSONALLY IDENTIFIABLE INFORMATION? THIS MAY INCLUDE GENETIC OR MEDICAL INFORMATION, POPULATION DATASETS, DETAILS OF INDIVIDUALS OR COMMERCIAL TEST DATA

IS YOUR RESEARCH LIKELY TO HAVE A FUTURE COMMERCIAL OR PATENTABLE OUTCOME WHICH YOU OR YOUR ORGANISATION WOULD WANT TO BENEFIT FROM?

## WHAT TO DO IF YOU ARE CONCERNED

Every university will have different oversight arrangements for research activities. Many aspects of research and academic activity are devolved to a local level, for example, to a Head of Faculty or to an individual principal investigator (PI). There is a delicate balance for universities in protecting academic freedoms whilst trying to improve visibility of issues such as cumulative risk of investment (where the institution becomes overly dependent on single sources of funding).

Where you identify concerns around a potential collaboration, ethics committees or university governance boards may be the appropriate bodies to consider the balance of risks for the organisation.

# HOW TO PROTECT YOUR RESEARCH



## 01 Collaborating with research partners

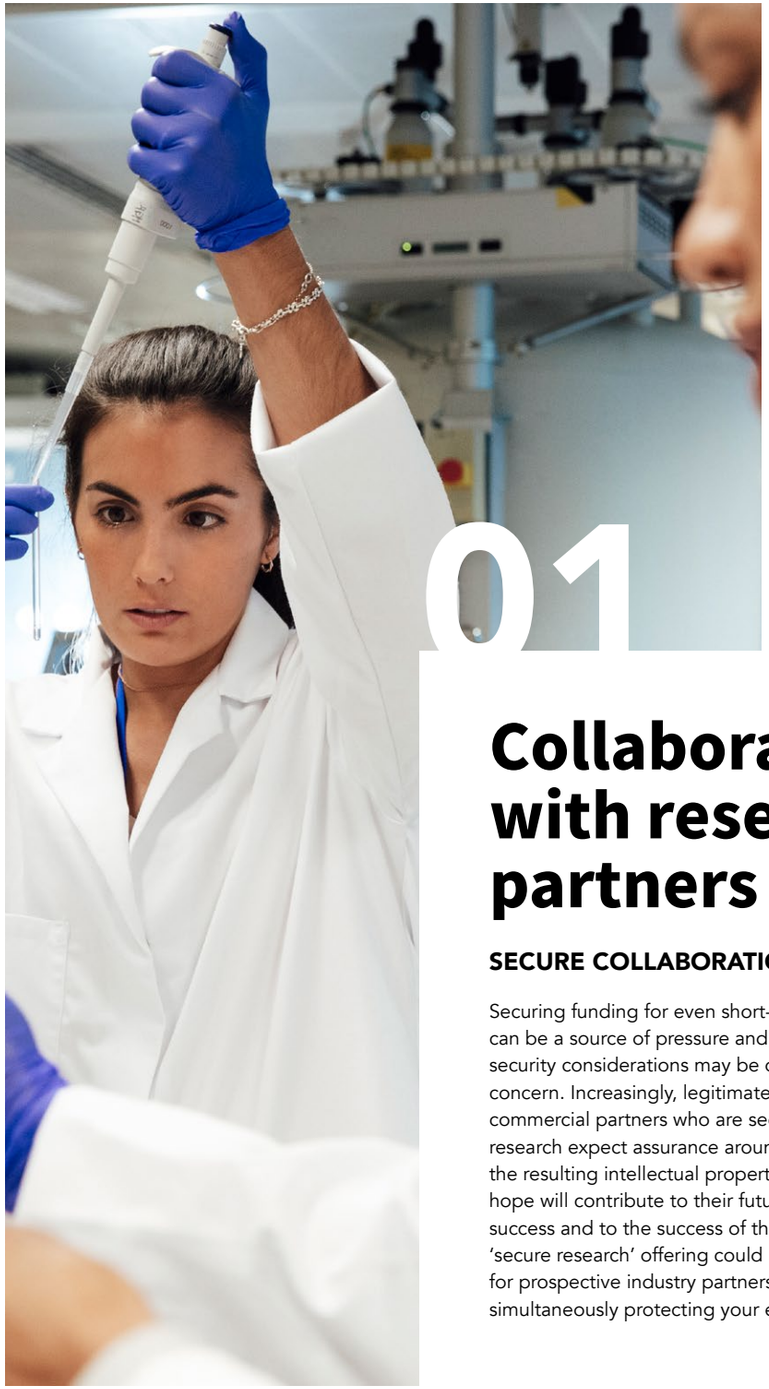
– Protecting intellectual property, making informed decisions about international collaboration and managing cyber risks

## 02 Using legal frameworks

– Understanding contractual expectations, export controls and GDPR

## 03 Helping researchers to stay safe

– Protecting your personal and research data, working with overseas researchers and attending conferences abroad



01

# Collaborating with research partners

## SECURE COLLABORATION

Securing funding for even short-term research can be a source of pressure and, understandably, security considerations may be of secondary concern. Increasingly, legitimate industry or commercial partners who are seeking to fund research expect assurance around the protection of the resulting intellectual property (IP), which they hope will contribute to their future commercial success and to the success of the wider economy. A 'secure research' offering could result in assurance for prospective industry partners or sponsors whilst simultaneously protecting your existing relationships.



# 3 key things to consider

## MANAGE CONFLICTS

If you are collaborating with multiple partners, it is crucial to avoid **conflicts of interest.** It may be possible to explore a related but different focus for collaboration with a new research partner in order to avoid a conflict of interest with your existing partner.

## DEMONSTRATE TRANSPARENCY

As part of managing long-term research relationships, it is important to be **transparent** about new research commitments. This may mean speaking to your existing sponsors, with potential implications for your ability to enter into non-disclosure agreements. **Visibility** of research across a laboratory, department or university is also critical. Laboratory or departmental meetings are a key opportunity to provide such visibility, and your regular meetings with research partners could include discussion about security.

## PROTECT COMPETITORS

Without compromising academic freedoms or curtailing the benefit of collaboration, some degree of separation between areas of research may be necessary. In some cases, you may wish to consider segregating IT **network access, information** and potentially **people** to prevent one partner having visibility of the work which another partner is sponsoring. Developing a good research security culture and having agreed guidelines between fellow researchers is a positive way of approaching this issue.

# Cyber security for research collaboration

When entering a new foreign collaboration, including a funding arrangement, you will need to understand the cyber security risks presented and the additional mitigation activities required.

Your IT department will be able to support you with implementation of the following measures:

## ACCESS CONTROL

It is important that you control access to sensitive data, whether that is personal data or research data. You should only allow users and partners with a valid requirement to have access to sensitive data, research and other parts of your networks. You should also ensure that you understand the security of any collaborative platforms, especially those used by third parties.

## UNAUTHORISED ACCESS MONITORING AND PREVENTION

Even when critical or highly sensitive data is separated and privileged access is limited, there may be instances of unauthorised access attempts. These could be from system users (insider threat) or from partners or other sources (external threat). You must ensure there are effective cyber security arrangements in place to monitor and defend against unusual or malicious network activities.

## SUPPLY CHAIN OR PARTNER ORGANISATION SECURITY

Many issues around supply chain security are due to the poor security practices of partner organisations or managed service providers. Working with overseas partners may present a higher level of risk. You should develop an understanding of the cyber risks associated with partner organisations, managed service providers and potentially vulnerable components at an early stage.

You may also wish to confirm whether your institution is recognised as cyber security industry standard, in line with the NCSC's Cyber Essentials, as that will demonstrate to your partners that your institution is working to secure your IT against a whole range of the most common cyber attacks.

## A SECURITY-MINDED AGENDA FOR RESEARCH PARTNERS

A university with long-established research partnerships saw that critical to the success of those relationships was having regular interactions, usually on a quarterly basis, and they ensured that security was a standing item for discussion. When it came to publishing, they had an agreement with their sponsors that they would consult on the content of papers and have a set process for arbitrating conflicts.

As the sponsors were engaged in a long-term funding relationship, there was an opportunity to consult early on new areas of research. These early discussions provided an opportunity to give confidence to the long-established research partner.

The open and transparent relationship included talking about who was working on a project, changes to personnel, and any visiting research fellows working on closely related topics. This ongoing dialogue extended to IT/network security and data protection and was an opportunity to discuss how the sponsor's data and information was protected and held.

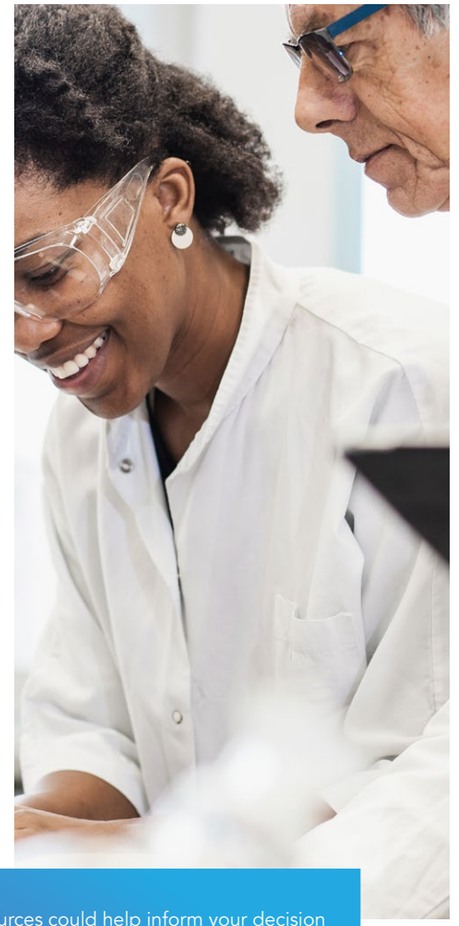


## WHAT DO YOU KNOW ABOUT YOUR POTENTIAL RESEARCH PARTNER?

Universities already invest significant effort in conducting due diligence around the financial sustainability or fraud risk associated with a research partner or funder. You should also consider whether a research or funding partner poses ethical or national security concerns. This consideration should go beyond questions of compliance (such as the export control regime) and consider reputational risks. An internet search can provide a lot of information about a partner, their relationship with a state or state military, and the nature of any previous research they have undertaken.

Things to consider include:

- Is there any publicly available information about an organisation, institution or entity which might give you cause for concern?
- In view of that information, what might be the broader application or unintended consequences of working with them in the area of research that you intend to undertake?
- What information is available about the level of freedom and the state of law of the country where your research partner is based?



The following resources could help inform your decision about the suitability of research with specific partners:

- US export entity control list
- UN sanctions list
- Country corruption index
- Trade restrictions on export
- Human Freedom Index
- World Justice Project Rule of Law Index

For a checklist on how to evaluate research proposals, visit the CPNI website.

# In summary

1

### DUE DILIGENCE

Conduct due diligence when considering a new research and/or funding collaboration. This should include ethical, legal and national security considerations as well as financial. You will then have all the information needed to make an informed and balanced decision about whether you want to work with them.

2

### CONFLICTS OF INTEREST

Be aware of potential conflicts of interests between research and/or funding partners that you work with. Be open with your partners and discuss your security arrangements, and their security needs, regularly.

3

### SEGREGATION

Ensure that, where necessary to protect IP, research or personal data, there is appropriate segregation between research programmes, both physically and online. Only give access to research to those who have a valid requirement.






02

# Using legal frameworks

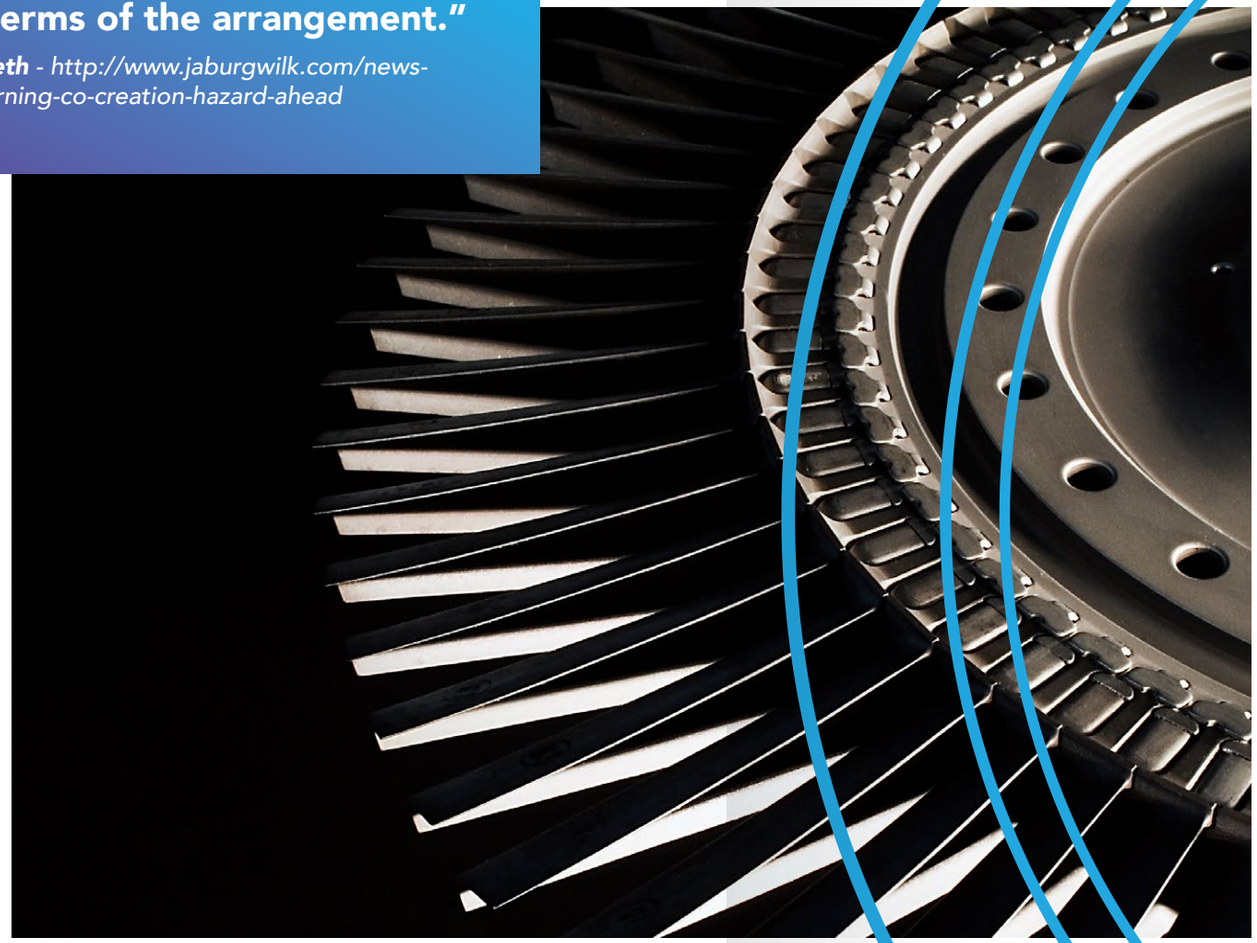
### COLLABORATION AND CONTRACTS

Your research will often be subject to contractual arrangements, providing greater certainty around the expectations of a research partner or sponsor. Equally, sponsors will have contractual expectations. It is critical that you have a clear understanding of the impact of these agreements on the research that you undertake.

The UK Intellectual Property Office (IPO) designed a toolkit to assist academic or research institutions and industrial partners who wish to carry out research projects together. To view the toolkit, please see the *Further Information* section.

**"Unfortunately, it is common for disputes to arise over co-created materials. That is not to say you shouldn't collaborate. It is, however, essential that the collaborators agree upon the terms of the arrangement."**

***Maria Crimi Speth*** *- http://www.jaburgwilk.com/news-publications/warning-co-creation-hazard-ahead*



## EXPORT CONTROLS

UK export controls are designed to restrict the export and communication of sensitive technology or strategic goods.

The controls apply equally to the academic community as to any other exporter, and from an academic perspective may touch on a range of areas of academic exchange which might enable technology transfer, either verbally or electronically. Failure to obtain a licence to export controlled goods (or transfer knowledge on related controlled technologies) may result in a criminal offence being committed.

The following routine academic activities could be covered by export control:

- Research on behalf of an international partner
- International collaboration
- Presentations at conferences
- Export of materials
- Teaching
- Academic exchange with a colleague at an overseas institution

Export control does not cover research which is already in the public domain or where the research is to be published into the public domain – For more advice on export control issues, please visit the CPNI website or refer to the resources listed in the *Further Information* section.

## WORKING WITH OVERSEAS INSTITUTIONS

A university worked in partnership with overseas institutions for a number of years on cutting-edge technology research. The university subsequently discovered that a significant proportion of existing research agreements should have been subject to export control licence applications. The university undertook an extensive review of those agreements and, working with the relevant government departments, went through a process of submitting export control licenses for those research programmes, some of which had to be paused during the process and some of which were stopped entirely.





## ARMS EMBARGOES

You should be aware that, at the time of publication, there are arms embargoes in operation against both China and Russia. You should also carefully consider whether any of your research is derived from the US, in which case you may also be subject to United States export control laws, specifically:

- ITAR (US International Traffic in Arms Regulations)
- EAR (Export Administration Regulations)

## COMPLIANCE IN FOREIGN JURISDICTIONS

If you are collaborating with an international partner there may be laws and regulations with which you will need to comply in your collaborator's country. Most countries will maintain some form of export control, they may have laws which restrict their institution's ability to share data or research outcomes, and the legal protections around IP may also differ in those jurisdictions. You should not assume that your research partner will take responsibility for such compliance, and you should be aware of any requirements that impact the collaboration.

## PUBLISH AND PROTECT

Freedom to publish will be of paramount importance to all academics, but it is possible to both publish and protect. In many cases, publishing first will be the means by which you protect your ideas but there may also be occasions when you want to protect aspects of your work if they have a sensitive application or if you are considering commercial opportunities.

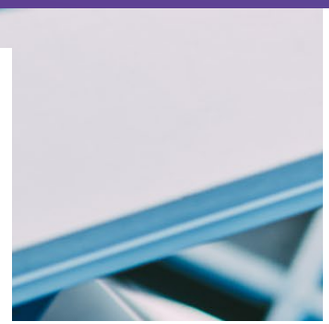
*Your Technology Transfer Office, legal department or other relevant supporting corporate services should be able to help with advice on export control issues and contractual undertakings.*

## PUBLISHING AND PROTECTING RESEARCH

At an early stage, before publishing or even speaking at a conference, consider if there is anything which is patentable within your research. Through the cycle of a research project, you should continually review progress and whether there is anything new which you have developed which might now be patentable. If working with sponsors, or partners where there is a co-creation agreement for IP, maintain a regular dialogue and discussion around what may be patentable and explore an early framework agreement or process for agreeing sensitive material that may be sanitised without damaging your overall ability to publish – For more information on patents and publishing research, please visit the CPNI website.

## GDPR: IMPLICATIONS FOR RESEARCH DATA

The Data Protection Act (DPA) 2018 sets out the framework for data protection law in the UK. It updates and replaces DPA 1998, and came into effect on 25 May 2018. It sits alongside the GDPR, and tailors how the GDPR applies in the UK - for example by providing exemptions. You must ensure that all data that you handle (including research data) is protected in compliance with GDPR. The Information Commissioner's Office (ICO) is the regulator for GDPR and there are circumstances in which you will have to report a data breach to the ICO. A detailed guide to your responsibilities under GDPR can be found on the ICO website.





# In summary

1

## EXPORT CONTROL

Ensure that you understand whether your research is subject to export control. Research activities are covered by export control legislation and there are tools that you can access to check whether your research needs to have an export control licence.

2

## LEGISLATION

When collaborating with a foreign research partner or funder, ensure that you have an awareness of the different legislative frameworks under which they may operate and how this might impact your agreements or partnership.

3

## GDPR

Be aware of your responsibilities to protect the data and information that you handle under GDPR legislation.

4

## TECHNOLOGY TRANSFER OFFICE

Speak to your Technology Transfer Office (TTO) or equivalent at the earliest stage of considering a new collaboration. They should be well-placed to advise you on legal conditions and compliance issues.

03

# Helping researchers to stay safe

## CYBER SECURITY

The nature of your collaborations, including how you use and share data and research online, will require a tailored approach to cyber security in line with your institution's security policies. However, there are some sensible tips that all individuals can follow, that will reduce the likelihood of loss or compromise of your research:

- Protect your email by using a strong and separate password
- Install the latest software and app updates
- Enable two-factor authentication on your email and collaboration platforms where possible
- Use a password manager to help you create and remember passwords
- Secure smartphones and tablets with a screen lock
- Always back up your most important data

Your IT department will be able to support you with any of the measures in this section.



## TAKE CARE WHEN USING USB DRIVES

USB drives or memory cards are a quick and easy way to transfer files between organisations and people. However, there are risks. If you're handed a USB drive at a conference, for example, before you insert it:

- Consider how trusted the source of the USB drive is
- Make sure autorun is disabled on your device via settings or system preferences
- Make sure your antivirus software runs an auto-scan before your device accesses the data on the USB drive

If you need to share information, consider alternative means (such as cloud storage, email or dedicated collaboration platforms).

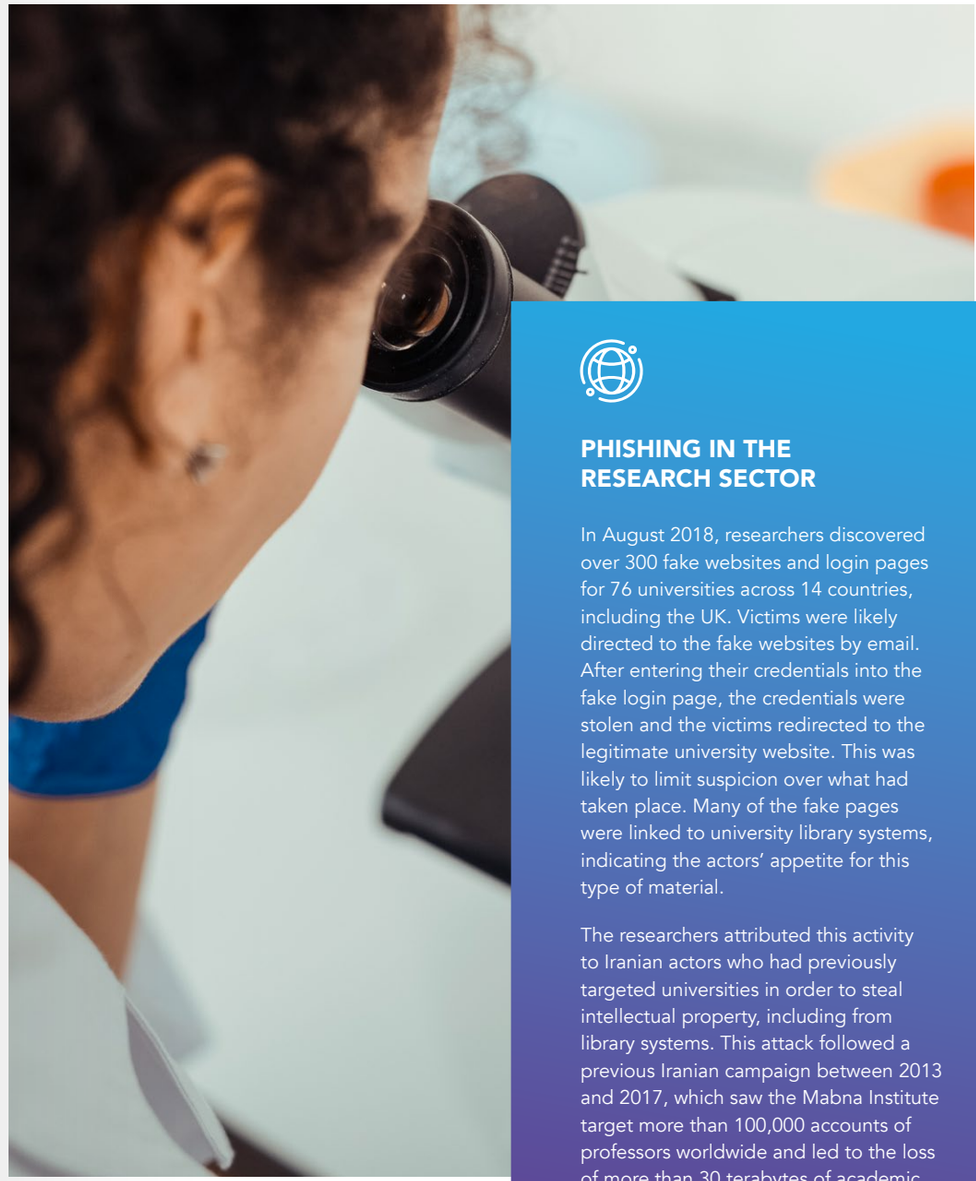
## PREVENTING PHISHING ATTACKS

Phishing attacks are one of the most common ways of obtaining personal and other data, so it is worth doing whatever you can to defend yourself against them. Phishing emails appear genuine but are actually fake. They might try and trick you into revealing sensitive information or contain links to a malicious website or an infected attachment.

Below are some of the actions you can take to reduce the likelihood of being phished. For more details please refer to the NCSC guidance on avoiding phishing attacks that can be found in the *Further Information* section.

- Phishers use publicly available information about you to make their emails appear convincing. Review your privacy settings and think about what you post and what has been posted about you, such as conference or organisational bios
- Know the techniques that phishers use in emails. This can include urgency or authority cues that pressure you to act
- Phishers often seek to exploit 'normal business' communications and processes. Make sure you understand your organisation's policies and processes to make it easier to spot unusual activity
- Anybody might click on a phishing email at some point. If you do, tell someone immediately (e.g. your IT team or line manager). Prompt reporting will massively reduce the potential harm caused by cyber incidents, so don't assume that someone else will do it





### PHISHING IN THE RESEARCH SECTOR

In August 2018, researchers discovered over 300 fake websites and login pages for 76 universities across 14 countries, including the UK. Victims were likely directed to the fake websites by email. After entering their credentials into the fake login page, the credentials were stolen and the victims redirected to the legitimate university website. This was likely to limit suspicion over what had taken place. Many of the fake pages were linked to university library systems, indicating the actors' appetite for this type of material.

The researchers attributed this activity to Iranian actors who had previously targeted universities in order to steal intellectual property, including from library systems. This attack followed a previous Iranian campaign between 2013 and 2017, which saw the Mabna Institute target more than 100,000 accounts of professors worldwide and led to the loss of more than 30 terabytes of academic data and intellectual property.

## WORKING WITH RESEARCHERS FROM OVERSEAS

Academic institutions will want to attract visitors and researchers from overseas. You have a duty of care to all staff and need a degree of understanding of visiting staff's backgrounds, previous work and ongoing obligations in order to help them to avoid conflicts of interest.

It is critical to follow your institution's human resources procedures so that anyone working on research for the university (with access to its facilities and IT network) is recorded as a member of staff or a student. Even short-term research attachments must comply with your institutional policies. Also consider what expectations you or sponsors may have from staff at the end of their work, particularly around confidentiality and non-disclosure.

You also have a responsibility to ensure that they are working on an appropriate visa whilst at the university. Visas for overseas students applying for certain courses in the UK may be subject to the Academic Technology Approval Scheme (ATAS). Your visa office at the university will be able to advise. For more information on working with overseas researchers please visit the CPNI website.

## STAFF WORKING OVERSEAS

If you have staff working in a country whose democratic and ethical values are different from our own, your broader risk assessment of staff working overseas should include the following:

- If something happens to one of your colleagues when they are working overseas, who should they report it to?
- How often do you check up on whether they have any concerns or issues?
- What agreements are there with the institution that will be hosting them overseas?
- What are the rules and laws that they are required to comply with in that country?
- Do any laws conflict with any of the agreements that you have made with that institution?
- Will the work that they conduct be subject to UK export control?
- Are your colleagues aware of the export control laws, national security laws or intellectual property arrangement in the country that they are working?

### PROTECTING STAFF

A university identified that there were a large number of individuals with access to its facilities and IT network that were not recorded as members of staff at the university. In many cases this had occurred because individual academics at the university were informally approached by researchers based at overseas institutions, who had come to the university for a short-term placement which they had funded themselves. Although they had access to the university site and network, the visiting academics had not applied for appropriate visas for the research work that they were undertaking at the university.

## COUNTRIES NOT CONFERENCES

With overseas conferences being a normal part of academic life, researchers will understandably focus on their presentations and potential research opportunities, rather than the security issues associated with travelling to a different country. Part of your preparation for any overseas conference should be to:

- Consider the country that you are travelling to, and be aware of local laws and customs
- Think carefully about what information you share or present
- Make sure you understand your host's attitude to academic freedom and discussion
- Ensure that any payments you accept for attendance won't create a conflict of interest, or place you in a contractual breach or breach of university policies
- Be clear on the areas of research that you can, and cannot, talk about
- Be polite but firm if pressed to share more information
- Report any suspicions to your manager and the appropriate university authority

[7] https://www.justice.gov/opa/press-release/file/1099876/download



# In summary

1

### AWARENESS

Ensure that you and your colleagues are aware of the measures that you can take to protect you and your research online. Good cyber security practices will reduce the likelihood of the loss or compromise of your research data.

2

### VISAS

Ensure that individuals with access to your facilities and IT network are centrally recorded as members of staff and that overseas visitors have appropriate visas.

3

### TRAVEL ADVICE

When travelling overseas for a conference or longer period, consider local laws and custom as well as how you protect intellectual property and sensitive data. If relying on IT, make sure it can be used/accessed overseas.

## FURTHER INFORMATION

Please see the following websites for more detailed information on the advice in this document:

**CPNI and NCSC websites**

*www.cpni.gov.uk*
*www.ncsc.gov.uk*

**Guidance**

Risk Management: *www.ncsc.gov.uk/collection/risk-management-collection*

Identity and Access Management: *www.ncsc.gov.uk/guidance/introduction-identity-and-access-management*

Cloud security: *www.ncsc.gov.uk/collection/cloud-security*

Security Monitoring: *www.ncsc.gov.uk/guidance/introduction-logging-security-purposes*

Supply Chain Security: *www.ncsc.gov.uk/collection/supply-chain-security*

Online security: *www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online*

Phishing: *www.ncsc.gov.uk/collection/small-business-guide/avoiding-phishing-attacks*

**Department for International Trade Export Control Joint Unit (ECJU)**

Your Technology Transfer Office, legal department or other relevant supporting corporate services should be able to help with advice on export control issues. ECJU also provides a support point of contact which is able to advise on whether a particular end user is likely to be of concern or not. You can contact the ECJU on 020 7215 4594 or by email on eco.help@trade.gov.uk.

US export entity control list:
*https://www.bis.doc.gov/index.php/documents/regulations-docs/2326-supplement-no-4-to-part-744-entity-list-4/file*

UN sanctions list: *www.un.org/securitycouncil/sanctions/information*

Country corruption index: *https://www.transparency.org/research/cpi*

Trade restrictions on export: *https://www.gov.uk/topic/business-enterprise/importing-exporting*

ITAR (US International Traffic in Arms Regulations *https://www.gov.uk/guidance/exporting-military-goods-to-the-united-states#itar-uk-companies-and-dual-and-third-country-nationals*

EAR (Export Administration Regulations): *https://www.export.org.uk/page/UKUSExportControls*

**Compliance**

ICO (GDPR/DPA): *https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/*

University and business collaboration agreements: Lambert Toolkit: *www.gov.uk/guidance/university-and-business-collaboration-agreements-lambert-toolkit*

IPO: *https://www.gov.uk/government/collections/ip-protection-abroad-country-guides*

ATAS Academic Technology Approval Scheme: *www.gov.uk/guidance/academic-technology-approval-scheme*

**Travel**

FCO Travel advice: *https://www.gov.uk/foreign-travel-advice*