Driving Research Security Cooperation Across Europe

Resources to support research security

Friday 15th November

Loughborough University

UNIVERSITY of STIRLING

FORMATION CONSULTANCY LIMITED

UK Science & Innovation Network

Joe Timlin

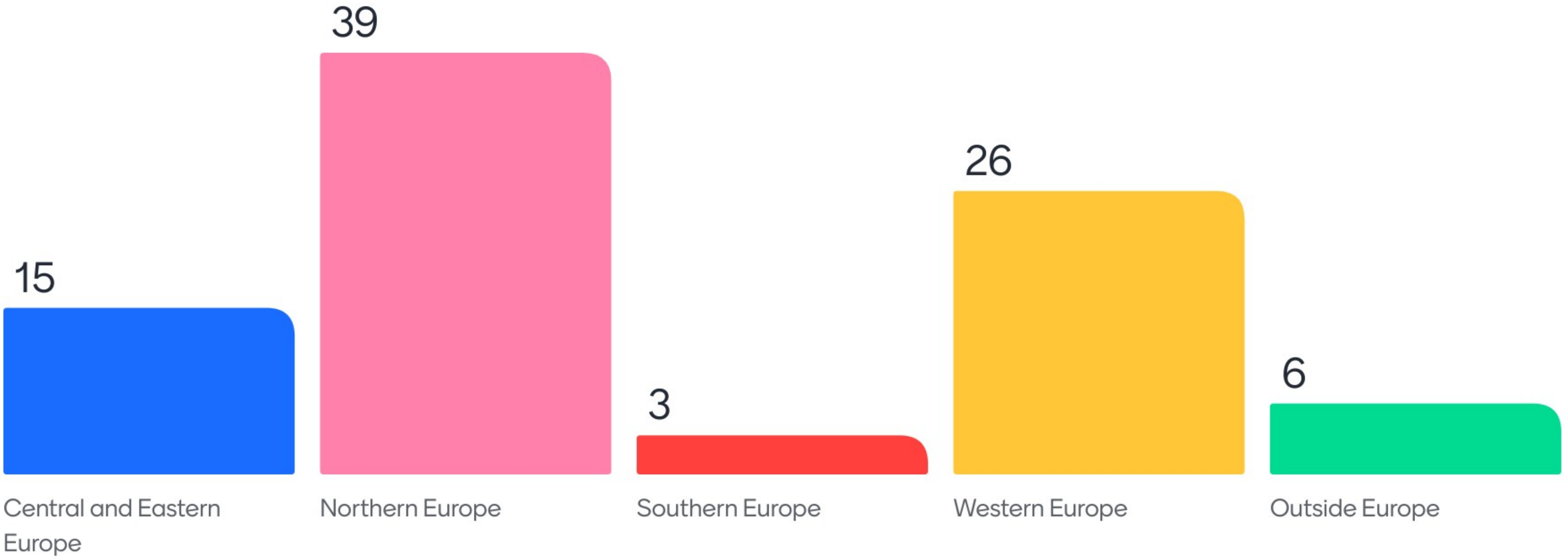
Joe supported the ARMA Complex Collaborations and subsequent FCDO SIN projects and offers a key operational perspective having implemented research security controls at Northumbria and Loughborough universities. He holds institutional relationships with RCAT and NPSA; is an active contributor to ARMA Training and Development and the HEECA Security Sub-Group; and has represented the sector at national and international events including the UUKi and SIN Research Security events in London, Paris and Rome.

Linsey Dickson

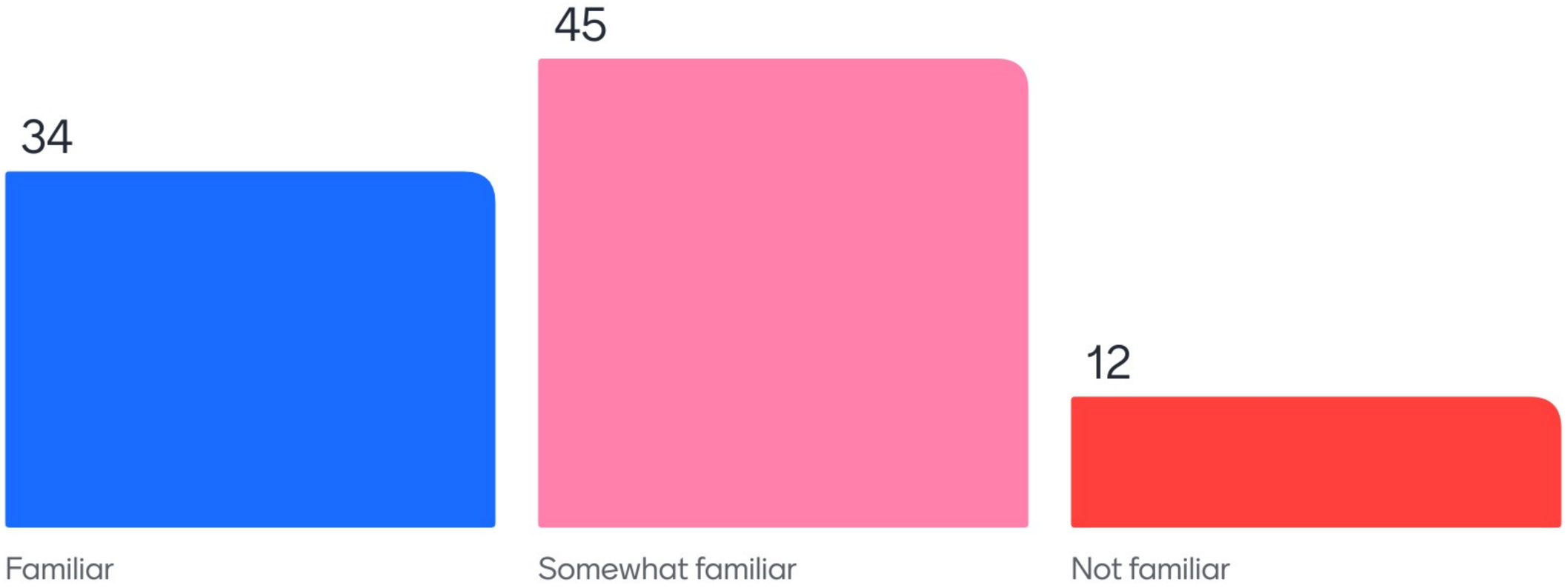
Linsey is Interim Executive Director of Research, Innovation and Business Engagement at University of Stirling. She is also past chair of the INORMS working group and a member of ARMA. Linsey has presented on research security across Europe and internationally and was asked to represent the Young European Research Universities Network (YERUN) as a thematic expert at the stakeholder meeting on Research Security organised by the European Commission and contributed to their advocacy work on Research Security and the EU Framework Programme.

Instructions

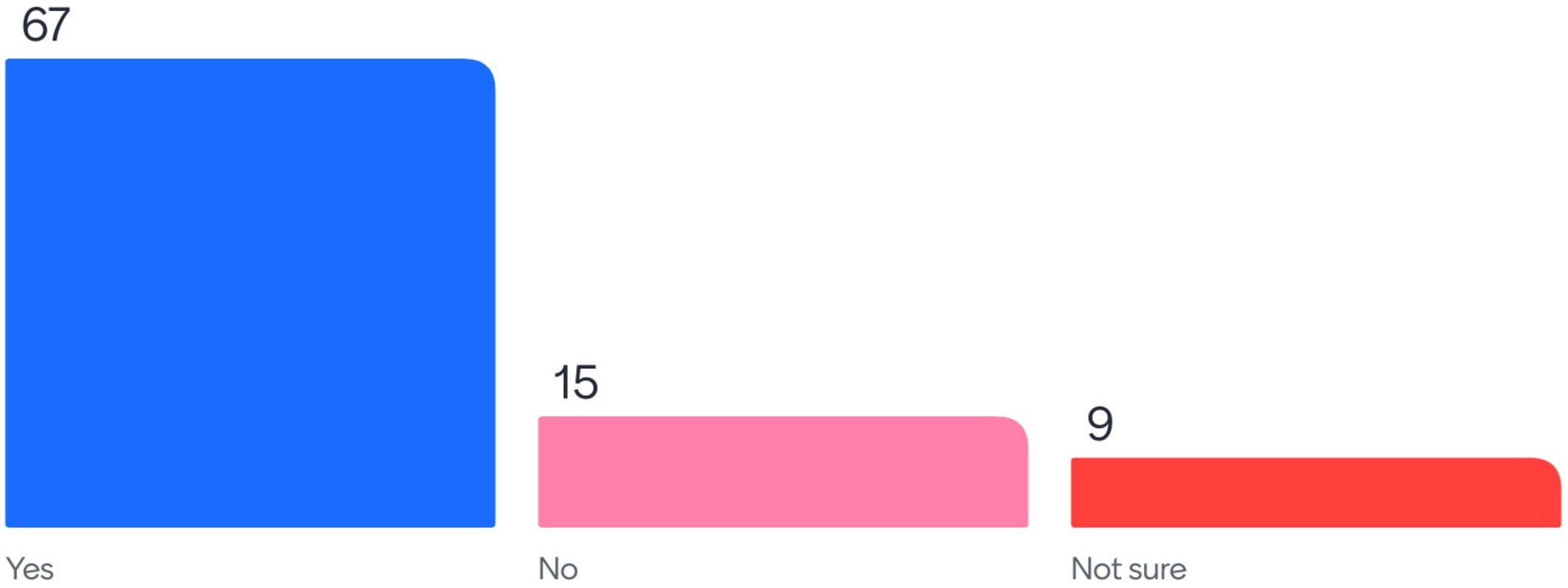
Tell us where you are joining us from today?



How familiar are you with research security?



Has your institution begun to adapt its processes to manage research security?



GUIDANCE PACK

CONTEXT

- The Working Group (WG) on the Security and Integrity of the Global Research Ecosystem (SIGRE) was established in the 2021 G7 Research Compact to "uphold and protect the principles that underpin effective international collaboration that is as open as possible and as secure as necessary."

- The WG was established with three main purposes:
  - To review existing principles of research security and integrity to understand whether they sufficiently account for security considerations.
  - To identify voluntary standards of conduct and best practice by which such principles of research security **and integrity** can be embedded.
  - To strengthen the exchange of best practices across the research community around these considerations by establishing a virtual academy of researchers.

- The WG has completed all of its purposes through the online publication of the "G7 Common Values and Principles on Research Security and Research Integrity:"; **and the** "G7 Best Practices For Secure & Open Research", **and the establishment of a** Virtual Academy.

COMMON VALUES AND BEST PRINCIPLES PAPER

The common values of research integrity and security apply broadly to all members of the research community, including governments, research funders, research institutions, and researchers themselves. These values include academic freedom, institutional autonomy, and the ethical conduct of research

A finalized version was signed-off by ministers at the G7 Science Ministerial in May 2022.

June 2022

G7 Common Values and Principles on Research Security and Research Integrity[1]

Vision

The 2021 G7 Research Compact states:

> We commit to promoting international research cooperation and the conditions of freedom, independence, openness, reciprocity and transparency under which it flourishes. Our governments have the right and responsibility to effectively ensure the security and integrity of the research ecosystem, in partnership with the research community, preventing the theft, misuse, and inappropriate exploitation of our intellectual property and personal data, and other forms of misconduct.

The G7 members envision the continuation of a collaborative research system where the importance of all talent – domestic and international – is acknowledged. Openness and security are not contradictory but complementary and mutually reinforcing.

To sustain this vision, we have developed and are embracing these principles of research security, which are common to the G7 members and academic communities and consistent with principles of research integrity. We will promote these principles globally.

The G7 members recognize the foundational importance of research integrity to academic discovery and research. Protecting the integrity of our research engages a broad set of considerations, including the need to implement proportionate and risk-appropriate actions in response to research security risks.

The G7 members acknowledge that there are circumstances in which it is justified to control access to research, infrastructure, or technology, and take seriously the risk of research partnerships and collaborations leading to harmful or adverse outcomes. We oppose bad-faith attempts to undermine or circumvent those access controls.

We have developed, and will continuously review, these principles for research security in collaboration with the academic community to provide a common framework, guiding responses to research security risks in domestic and international research.

Why Do Research Integrity and Research Security Matter?

Open and collaborative research underpins domestic and global responses to some of our most challenging and pressing issues. Collaborations include those with other government entities, public-private partnerships, and international science collaborations. We also recognize that collaborations can progress under a variety of formal and informal arrangements and at a variety of scales. These collaborations accelerate the pace of discoveries and increase the dynamism and openness of our research communities.

The G7 is committed to promoting open research while affirming that there are circumstances in which it is appropriate to put proportionate limits or conditions around access to research and associated data. For instance, a preliminary discovery may need protecting while researchers gather data to support publication, or controls might be placed around novel

[1] This Paper has been developed within the Sub-Working Group on Best Practice and Principles of the G7 Working Group on the Security and Integrity of the Global Research Ecosystem (SIGRE); see Annex A for more information.

Figure 1: A graphic depicting how research security and research integrity protect the foundation of research.

Research integrity is the foundation of all research, forming the base on which to collaborate in a fair, innovative, open, and trusted environment. This is represented by the central circle. Bad faith actors use a variety of methods to undermine research integrity. These activities often include methods such as partnerships, physical access and espionage, cyber security, or insider or outsider personnel that access research; all of these activities degrade research integrity. These actions are represented by the red circles. Research security measures and research integrity measures help to protect the foundation of research and are represented by the half circles in shades of blue surrounding the integrity of research.

G7 Principles of Research Security

We – the G7 members – commit to respecting and furthering the stated research integrity common values. At the same time, we will seek to develop and implement our research security actions in line with the following research security principles.

The following list has been created by the G7 members, drawing from existing principles and commitments, as appropriate, and establishing new principles when needed. The list of principles is meant to articulate the shared commitment of G7 research communities, and does not establish these principles as being of equal value across all jurisdictions.

The following list has been created by the G7 members with the goal of clearly outlining the principles that should structure our actions and how we respond to research security risks. As G7 members look to collaboratively identify and respond to issues of research security responses should exemplify and follow these principles of research security (articulated in no specific hierarchy or order):

- **Balancing National and Global Interests:** G7 research funders and governments meet their respective and collective national, economic, and strategic interests by actively pursuing excellence in higher education, research, and innovation. At the same time, these institutions should steward and protect investments in research. Funding for scientific and research partnerships should continue to be guided by scientific merit assessments and excellence, and take appropriate and proportionate consideration and mitigation of risks to national and/or economic security where necessary. Funding should further best interests in a manner that does not compromise research integrity, looking to address global collective interests whenever possible.
- **Maintaining Openness and Research Security:** Open collaboration on research is indispensable to pushing the boundaries of innovation and addressing complex societal challenges. As a driver for greater innovation and inclusion, open science – the practice of making science and research inputs, outputs, and processes available to all with minimal restrictions – should not be an afterthought and governments should commit to making research accessible when there is no justification for it to remain closed. With benefits that include greater reproducibility of scientific results, fostering a public dialogue that engenders public confidence and trust in science, leveraging efforts, accelerating knowledge transfer and the re-use of scientific information for verifiably peaceful uses, and building synergies with international and domestic partners, governments should look to enable the open exchange of research and its results. Enhanced access and openness come with associated risks related to privacy; ideas, research outcomes, and intellectual property; national security; and public interest. As a result, this openness should be maintained to the maximum extent, acknowledging the need for safeguards for research that could have adverse ethical or national security implications.
- **Collaboration and Dialogue:** All entities involved in research should strive to support and engage with one another in the pursuit of a community that upholds security alongside openness. Researchers and institutions cannot be expected to become security experts independent of the support of those entities with the requisite expertise and knowledge. At the same time, national security organizations and governments should strive to remain receptive to the concerns and priorities of those within the research community. Governments should work collaboratively with their research communities to address domestic and international research security risks. They should commit to engaging in meaningful information sharing about the nature of the risks, with the goal of addressing common risks alongside researchers and benefiting from shared approaches. Through sustained and meaningful collaboration and

BEST PRACTICES PAPER

To support the implementation of the identified common values and principles, a list of best practices has been developed by G7 members to provide high-level information on practices that contribute to secure and open research.

The paper recognizes that all stakeholders in the research community have a role to play, and is structured to provide guidance to governments, research funders, research institutions, and researchers. The paper will also include examples of best practices being implemented by different G7 members

A finalized version was signed-off by ministers at the G7 Science Ministerial in May 2023

G7 BEST PRACTICES FOR SECURE & OPEN RESEARCH

Security and Integrity of the Global Research Ecosystem (SIGRE) Working Group

This document is a copy of the original document titled G7 Best Practices for Secure & Open Research published by the G7.

November 2023

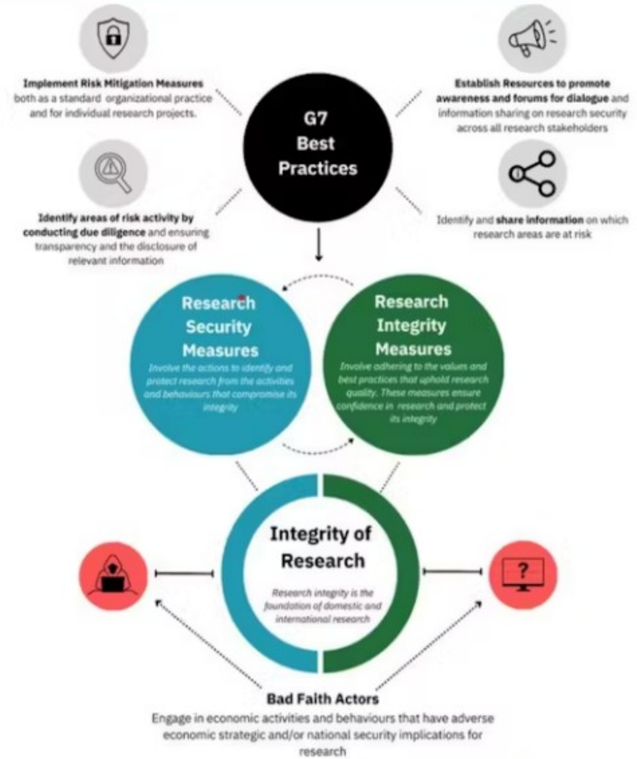


Figure 1: A graphic depicting how the G7 Best Practices support both research security and research integrity.

4. Implement risk mitigation measures, both as standard organizational practice and for individual research projects.

After establishing *where* risk exists and its magnitude, members of the research community are generally better positioned to address and mitigate against it. Risk mitigation aims to reduce the likelihood and impact of risks to a level that is acceptable to the researcher, their institution, the research funder, and the respective government. Risk mitigation measures can be implemented at an organizational level, creating standards that are expected to be followed, and at a project specific level where a more tailored approach to mitigating risk may be appropriate for projects with unique characteristics that may elevate their level of risk. Mitigation measures should be proportionate to the level of risk in order to ensure both secure and open research. Mitigation measures may need to be adapted over time as risks change and will benefit from periodic review to determine if they are still appropriately addressing current risks, or if changes are necessary to respond to new concerns.

Stakeholders such as research funders and research institutions may also wish to consider implementing risk governance both at the organizational and project level. Having in place organizational policies and processes to assess and mitigate risks associated with organizational risks as well as with individual research projects is critical to ensuring consistency in the decision-making process.

Governments: Governments have a valuable role to play in providing guidance on risk mitigation. Governments can develop resources and information sharing mechanisms to help other members of the research community with this best practice.

Research Funders: Research funders may wish to consider implementing specific requirements within their application process related to research security and integrity, or set policies or conditions that certain risk mitigation measures be a standard expectation for funding. Funders may wish to consider encouraging or requiring applicants to ensure that participants on a specific program meet certain training requirements in relation to securing their research, have cybersecurity plans in place, and control measures for the management of data, in accordance with existing and evolving research community best practices. In addition, by virtue of being in receipt of research proposals submitted by applicants, research funders are likely able to identify and develop broad risk mitigation best practices. In turn, they can circulate guidance on risk mitigation measures broadly across the research community (in conjunction with governments).

Research Institutions: Research institutions can consider implementing a variety of measures to protect themselves and their researchers. For example, institutions may consider employing appropriate cyber security practices, physical access controls, ensuring adherence to the relevant legal obligations of their country, and developing protections for intellectual property.

PURPOSE OF THE VIRTUAL ACADEMY

To raise awareness among the research communities of the G7 (and possibly other) countries on the challenges related to security and integrity of the research ecosystem.

To **help** research actors (i.e. governments, research funders, research institutions and researchers) develop, from their respective points of view, **a shared understanding and a deeper knowledge of research integrity and security, allowing for international collaboration to continue with confidence.**

To **facilitate information sharing** among research actors on common risks and forms of misconducts and on proportionate, **and** appropriate measures **to** protect the security and integrity of the local and/or global research ecosystem.

VIRTUAL ACADEMY

The Virtual Academy and Toolkit sub-working group was chaired by Italy and the UK

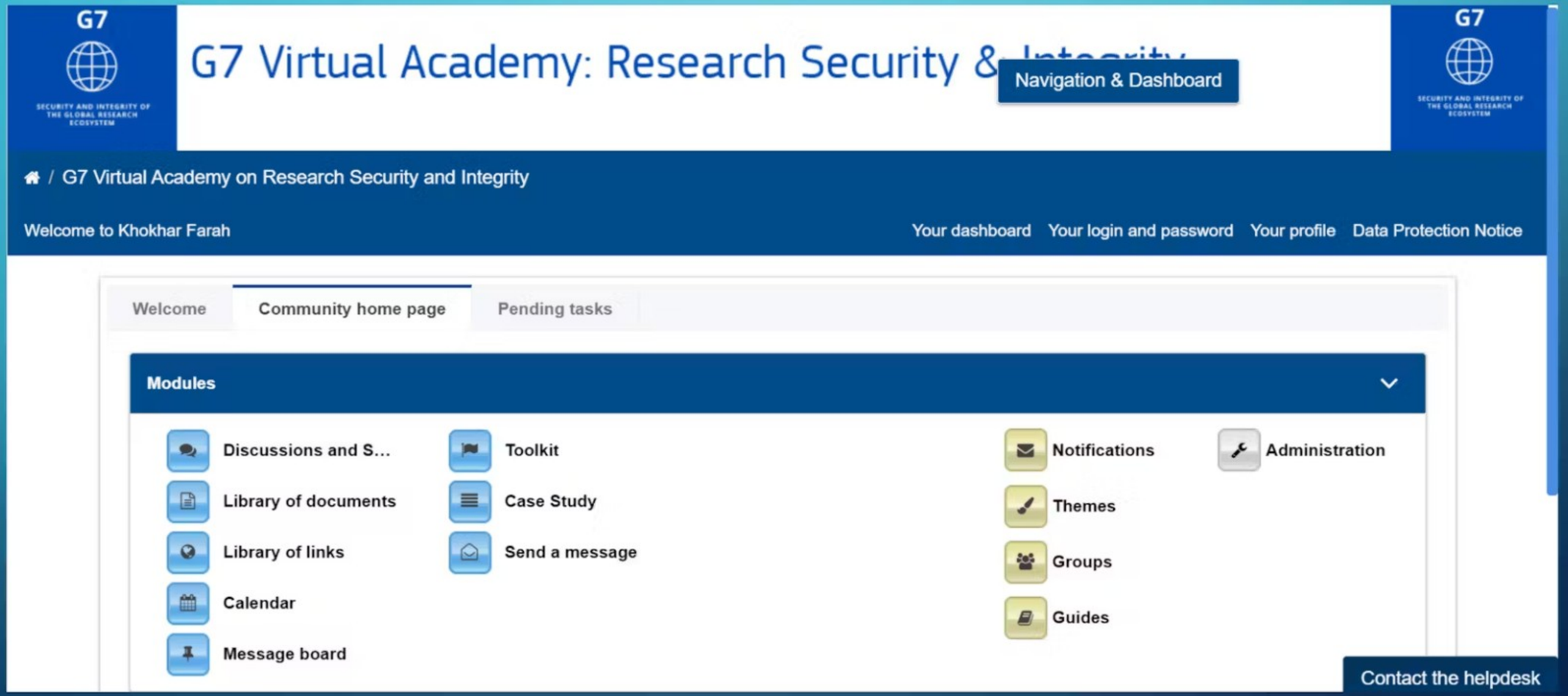
All G7 countries held domestic stakeholder workshops with members of their domestic Research Community to guide the design and development of the Virtual Academy

Since the working groups conception, a concept plan **was agreed to** design and delivery the Virtual Academy and Toolkit, **and to** establish an Oversight Board which will continue to **manage** the Virtual Academy

The Virtual Academy was launched in May 2023 for G7 Research communities

In 2024 the platform **will be open to a pilot group of non-G7 countries**

Functions



Department for Science, Innovation & Technology

Mentimeter

GOVERNANCE

G7 Validators: Each G7 member must nominate **up to 2** validators to validate uploads and membership requests from their country. They will be called 'G7 Validators'. They **can be** either governmental and/or sector representatives **and will remain on duty as validators** for as long as their country is a member of the G7.

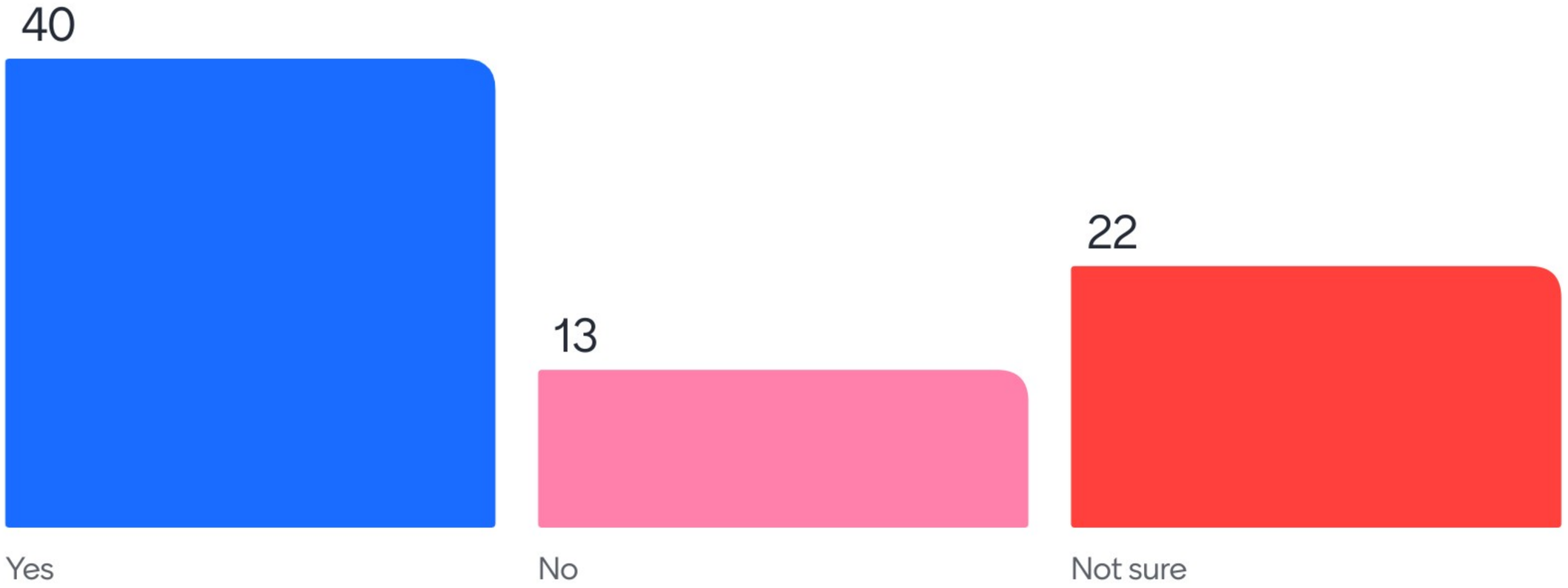
G7 Administrators: The administrators **– nominated by each G7 member -** will be responsible for updating the platform, its graphics, folders and functions, monitoring the platform and they will be called 'G7 Administrators'. **They will be governmental representatives and will remain on duty as administrators for as long as their country is a member of the G7.**

Oversight Board: Comprised of the current, incumbent and previous G7 presidents with the UK as an English language expert and European Commission as a permanent observer, this group will meet every three months to regulate and update the Virtual Academy

How to Join

1. Click this link: https://europa.eu/sinapse/directaccess/sigre
2. Apply to join the *G7 Virtual Academy on Research Security and Integrity* community
3. Ensure that you select your country and upload a CV with references
4. Your countries/partner countries validator will review your membership and accept you onto the platform
5. Once accepted go to the Toolkit Module and review the User Manual for guidance on how to upload documents/messages etc onto the platform

Do you have national research security guidelines in your country?



Discussion: please ask any questions

Are educational Securitas included? If not, why?

Can multiple people from one institution join the G7 Virtual Academy?

The platform seems to be hosted on an EU site. Will it be open to all EU members eventually?

Mentimeter

USE OF TIM-DATABASE AT AARHUS UNIVERSITY

AARHUS UNIVERSITY

15 NOVEMBER 2024

JOHN WESTENSEE
ADVISOR

1

TIM Dual-Use | Knowledge for

https://knowledge4policy.ec.europa.eu/text-mining/tim-dual-use_en

TIM's database contains 3 types of documents, updated annually:

- **Scientific publications in Scopus**, 40,000 journals by Elsevier and other publishers, with more than 50 million abstracts (in English, also if the full paper is e.g. in Chinese)
- **Patents** (European Patent Office - PATSTAT, containing about 25 million patents from more than 90 worldwide patent authorities including all the major countries
- **EU funded projects** (CORDIS): more than 77,000 research projects, including also partners from third countries

Dual-use technologies might be included in the contents of SCOPUS abstracts, patents and EU-funded research projects, which therefore could be subject to export authorisations prior to publication or sharing, as required by Regulation 2021/821.

TIM DU's mapping of **Dual-use technologies** is performed by means of search algorithms based on keywords related to the **"EU dual-use control list"** text, as well as emerging technologies, with their scientific and technical synonyms. The choice of keywords and Boolean combinations has been designed to maximise the results while striving for the best possible relevance.

TIM Dual-Use applications can be multiple:

- Mapping of a country's R&D international cooperation networks related to dual-use;
- Mapping of specific research institutes, companies, Universities, researchers' scientific publications with regard to potential dual-use technologies;
- Monitoring of emerging technologies (technological development and trends, as appearing from chronological and geographical developments).

For research entities in particular:

- Assess the past scientific production to identify articles, patents or EU-funded project results already produced and published, which could have had a potential dual-use content;
- Identification of areas for targeted awareness-raising activities to reinforce internal compliance.

TIM DU has been developed by JRC (STRIKE project - G.II.7 unit; I.3 unit) and University of Liège (European Studies Unit)

Access TIM DU dashboards for:

Technologies related to the EU dual-use control list's categories:

- Cat.0 Nuclear Material, Facilities and Equipment
- Cat.1 Pathogens
- Cat.1 Special Materials and Related Equipment
- Cat.2 Material Processing
- Cat.3 Electronics
- Cat.4 Computers
- Cat.5 Telecommunications and Information Security
- Cat.6 Sensors and Lasers
- Cat.7 Navigation and Avionics
- Cat.8 Marine
- Cat.9 Aerospace and Propulsion
- Global Dual-Use Queries

Emerging technologies:

- Additive Manufacturing
- Artificial Intelligence
- Biotechnology
- Blockchain
- Cyber-Surveillance

TIM Dual-Use | Knowledge for | TIM Dashboard | GLOBAL DUAL

https://www.timanalytics.eu/TimDualUse/dashboard/index.jsp#/space/s_30?ds=480

GLOBAL DUAL-USE QUERIES (New)

Dataset: Global query Cat 0-9 & EmT (2022-2023) | FILTERS 2 | ORDER

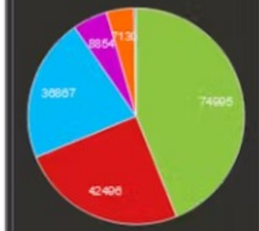
Entity name: The University of Oxford OR University of Oxford

Dataset Info

Dataset name	Global query Cat 0-9 & EmT (2022-2023)
Dataset definition	limit=249999; Full definition
Dataset definition type	merge|merge
Storage model	normal
Definition creation	14-11-2023 09:05:05
Definition modification	04-7-2024 11:50:06
Number of documents	170814

Sort | Stacked | Cumulated | Chart: | Smooth lines

Document Type Distribution



Yearly Distribution

Article | Book chapter | Conference proceedings | EU project | Patent | Review

Documents

Dcouments: 342

Article | Book chapter | Conference | Review

Date, Type | 2022 | 2023 | highlight text

Reconstructing Complex States of a 20 -Qubit Quantum Simulator	ID: S_2-s2.0-85180551410	Year: 2023
Title: experimental realisation of multi-qubit gates using electron paramagnetic resonance	ID: S_2-s2.0-85175794914	Year: 2023
How to Wire a 1000 -Qubit Trapped-Ion Quantum Computer	ID: S_2-s2.0-85174930764	Year: 2023
The ZX-calculus as a language for topological quantum computation	ID: S_2-s2.0-85174238050	Year: 2023
Adaptive surface code for quantum error correction in the presence of temporary or permanent defects	ID: S_2-s2.0-85169700644	Year: 2023
Exploiting subspace constraints and ab initio variational methods for quantum chemistry	ID: S_2-s2.0-85167695038	Year: 2023
Exploring ab initio machine synthesis of quantum circuits		

Publications_per_country

Entries: 10 / 75

Page 1 | Page size 30

Name	First	Last	Total
United Kingdom	2022	2023	342
United States of America	2022	2023	94
Germany	2022	2023	39
China	2022	2023	35
Italy	2022	2023	34
Netherlands	2022	2023	30
France	2022	2023	23
Canada	2022	2023	23
Australia	2022	2023	23
Switzerland	2022	2023	19
Spain	2022	2023	14
Brazil	2022	2023	13
Thailand	2022	2023	12
Austria	2022	2023	12

Time series

Patents_per_country

Entries: 10 / 75

Page 1 | Page size 30

Name	First	Last	Total
United Kingdom			0
United States of America			0
Switzerland			0
France			0
Italy			0
Germany			0
Poland			0
India			0
Japan			0
Norway			0
Spain			0
Canada			0
Sweden			0
Australia			0

Time series

Type here to search

OMXC20-indeks +0,...

14:27
06-11-2024

Dcouments: 342

Article Book chapter Conference Review

Date, Type ↑ 2022 2023 highlight text

Mentimeter

Reconstructing Complex States of a 20 -Qubit Quantum Simulator

Entry type: Article ID: S_2-s2.0-85180551410 Year: 2023

Kurmapu M.K., Lvovsky A.I., Tiunova V.V., Fedorov A.K., Tiunov E.S., Ringbauer M., Blatt R., Monz T., Maier C.

University of Calgary, University of Oxford, Russian Quantum Center, Technology Innovation Institute, Universität Innsbruck, Alpine Quantum Technologies GmbH, Österreichische Akademie der Wissenschaften, National University of Science and Technology

A prerequisite to the successful development of quantum computers and simulators is precise understanding of the physical processes occurring therein, which can be achieved by measuring the quantum states that they produce. However, the resources required for traditional quantum state estimation scale exponentially with the system size, highlighting the need for alternative approaches. Here, we demonstrate an efficient method for reconstruction of significantly entangled multiqubit quantum states. Using a variational version of the matrix-product-state ansatz, we perform the tomography (in the pure-state approximation) of quantum states produced in a 20-qubit trapped-ion Ising-type quantum simulator, using the data acquired in only 27 bases, with 1000 measurements in each basis. We observe superior state-reconstruction quality and faster convergence compared to the methods based on neural-network quantum state representations: restricted Boltzmann machines and feed-forward neural networks with autoregressive architecture. Our results pave the way toward efficient experimental characterization of complex states produced by the quench dynamics of many-body quantum systems.

Title: experimental realisation of multi-qubit gates using electron paramagnetic resonance

Entry type: Article ID: S_2-s2.0-85175794914 Year: 2023

How to Wire a 1000 -Qubit Trapped-Ion Quantum Computer

Entry type: Article ID: S_2-s2.0-85174930764 Year: 2023

The ZX-calculus as a language for topological quantum computation

Entry type: Article ID: S_2-s2.0-85174238050 Year: 2023

Adaptive surface code for quantum error correction in the presence of temporary or permanent defects

Entry type: Article ID: S_2-s2.0-85169700644 Year: 2023

Exploiting subspace constraints and ab initio variational methods for quantum chemistry

Entry type: Article ID: S_2-s2.0-85167695038 Year: 2023

Exploring ab initio machine synthesis of quantum circuits

Entry type: Article ID: S_2-s2.0-85167669556 Year: 2023

Completeness of the ZH-calculus

Entry type: Article ID: S_2-s2.0-85165991969 Year: 2023

Quantum autoencoders for communication-efficient cloud computing

Entry type: Article ID: S_2-s2.0-85164279491 Year: 2023

Looped Pipelines Enabling Effective 3D Qubit Lattices in a Strictly 2D Device

Entry type: Article ID: S_2-s2.0-85164244596 Year: 2023

Quantum Computing is Scalable on a Planar Array of Qubits with Fabrication Defects

Entry type: Article ID: S_2-s2.0-85164115144 Year: 2023

Quantum Low-Density Parity-Check Codes for Modular Architectures

Real-time nanomechanical property modulation as a framework for tunable NEMS

Type: Article | ID: S_2-s2.0-85126720276 | Year: **2022**

Authors: **Ali U.E., Bhaskaran H., Modi G., Agarwal R.**

Organisations: **University of Oxford, University of Pennsylvania**

Phase-change materials (PCMs) can switch between amorphous and crystalline states permanently yet reversibly. However, the change in their mechanical properties has largely gone unexploited. The most practical configuration using suspended thin-films suffer from filamentation and melt-quenching. Here, we overcome these limitations using nanowires as active nanoelectromechanical systems (NEMS). We achieve active modulation of the Young's modulus in GeTe nanowires by exploiting a unique dislocation-based route for amorphization. These nanowire NEMS enable power-free tuning of the resonance frequency over a range of 30%. Furthermore, their high quality factors ($Q > 104$) are retained after phase transformation. We utilize their intrinsic piezoresistivity with unprecedented gauge factors (up to 1100) to facilitate monolithic integration. Our NEMS demonstrate real-time frequency tuning in a frequency-hopping spread spectrum radio prototype. This work not only opens up an entirely new area of phase-change NEMS but also provides a novel framework for utilizing functional nanowires in active mechanical systems.

Experimental quantum key distribution certified by Bell's theorem

Type: Article | ID: S_2-s2.0-85135022610 | Year: **2022**

Authors: **Nadlinger D.P., Drmota P., Nichol B.C., Araneda G., Main D., Srinivas R., Lucas D.M., Ballance C.J., Ivanov K., Urbanke R.L., Tan E.Y.-Z., Renner R., Sekatski P., Sangouard N., Bancal J.-D.**

Organisations: **University of Oxford, School of Computer and Communication Sciences, Institute for Theoretical Physics, University of Geneva, Université Paris-Saclay**

Cryptographic key exchange protocols traditionally rely on computational conjectures such as the hardness of prime factorization1 to provide security against eavesdropping attacks. Remarkably, quantum key distribution protocols such as the Bennett–Brassard scheme2 provide information-theoretic security against such attacks, a much stronger form of security unreachable by classical means. However, quantum protocols realized so far are subject to a new class of attacks exploiting a mismatch between the quantum states or measurements implemented and their theoretical modelling, as demonstrated in numerous experiments3–6. Here we present the experimental realization of a complete quantum key distribution protocol immune to these vulnerabilities, following Ekert's pioneering proposal7 to use entanglement to bound an adversary's information from Bell's theorem8. By combining theoretical developments with an improved optical fibre link generating entanglement between two trapped-ion qubits, we obtain 95,628 key bits with device-independent security9–12 from 1.5 million Bell pairs created during eight hours of run time. We take steps to ensure that information on the measurement results is inaccessible to an eavesdropper. These measurements are performed without space-like separation. Our result shows that provably secure cryptography under general assumptions is possible with real-world devices, and paves the way for further quantum information applications based on the device-independence principle.

DV-QKD Coexistence With 1.6 Terabit/s Classical Channels in Free Space Using Fiber-Wireless-Fiber Terminals

Type: Conf | ID: S_2-s2.0-85146399779 | Year: **2022**

Authors: **Alia O., Wang R., Bahrani S., Kanellos G.T., Nejabati R., Simeonidou D., Schreier A., Faulkner G., O'Brien D., Singh R., Rarity J.**

Organisations: **University of Bristol, University of Oxford, Toshiba Europe Ltd**

We experimentally demonstrate for the first time the simultaneous transmission of a COW-based DV-QKD channel and an 8x200 Gpbs 16-QAM coherent optical channels, both operating in the C-band over 2.5 m of free space enabled by Fiber-Wireless-Fiber terminals.

RegGuard: Leveraging CPU registers for mitigation of control- and data-oriented attacks

Type: Article | ID: S_2-s2.0-85151646149 | Year: **2023**

Authors: **Geden M., Rasmussen K.**

Organisations: **University of Oxford**

CPU registers are small discrete storage units that are used to store temporary data and instructions within the CPU. Registers are not addressable in the same way memory is, which makes them immune to memory attacks and manipulation by other means. In this paper, we take advantage of this to protect critical program data with integrity guarantees that cover register spills. This protection effectively addresses control- and data-oriented attacks targeting the stack, even by adversaries with the full knowledge of program memory. Our solution RegGuard is a software-based mitigation technique that uses existing CPU registers and cryptographic primitives to protect critical variables with hardware-level assurance. Unlike conventional register allocation methods, RegGuard prioritises the security significance of a register candidate over its expected performance gain. Our scheme also deals effectively with saved registers to the stack, i.e., when the compiler frees registers to make room for the variables of a new call. With RegGuard, register values saved to the stack are protected, including strong adversaries with arbitrary read and write access capabilities. While our primary design focus is on security, performance is important for a scheme to be adopted in practice. RegGuard is still benefiting from the performance gain normally associated with register allocations and provides practical protection. Despite being adaptable to different CPU architectures, we showcase the performance of RegGuard using different benchmark programs and the C library on the ARM64 architecture as a proof-of-concept.

Towards the engineering of a quantum key distribution receiver robust to ambient light

Type: Conf | ID: S_2-s2.0-85152768569 | Year: **2023**

Authors: **Lee V., Schreier A., Faulkner G., O'Brien D.**

Organisations: **University of Oxford**

Quantum Key Distribution (QKD) has the potential to secure indoor optical wireless links. In a typical room scenario, an indoor optical wireless link will have a transmitter on the ceiling and a receiver on a desk. Ambient light from room (typically LED) lighting on the ceiling and sunlight coming through the windows present a challenging environment for free-space QKD links to operate, and a key challenge is to mitigate the noise induced by ambient light, particularly sunlight. A combination of spectral and spatial filtering can be used to reduce the effect of ambient light, with a narrowband optical filter typically used. Moreover, the wavelength of operation is key to further reduce the impact of ambient light. Wavelengths in â€ quiet' regions of the solar spectrum, such as the atmospheric absorption bands, are promising candidates. We are currently working on a system that operates at 1370 nm, where water and carbon dioxide absorption band in the atmosphere attenuate the solar spectrum substantially. This paper reports the design and modelling of the system, with a series of validation measurements to characterise the effect of solar radiation on a typical photon-counting detector as would be used in a QKD system. The aim of this work is to show the feasibility of the wavelength region around 1370 nm as a necessary step towards a low noise QKD receiver for indoor optical wireless links in a practical environment.

Probabilistic Planning for AUV Data Harvesting from Smart Underwater Sensor Networks

Type: Conf | ID: S_2-s2.0-85146341420 | Year: **2022**

Authors: **Budd M., Duckworth P., Hawes N., Lacerda B., Salavasidis G., Karnarudzaman I., Harris C.A., Phillips A.B.**

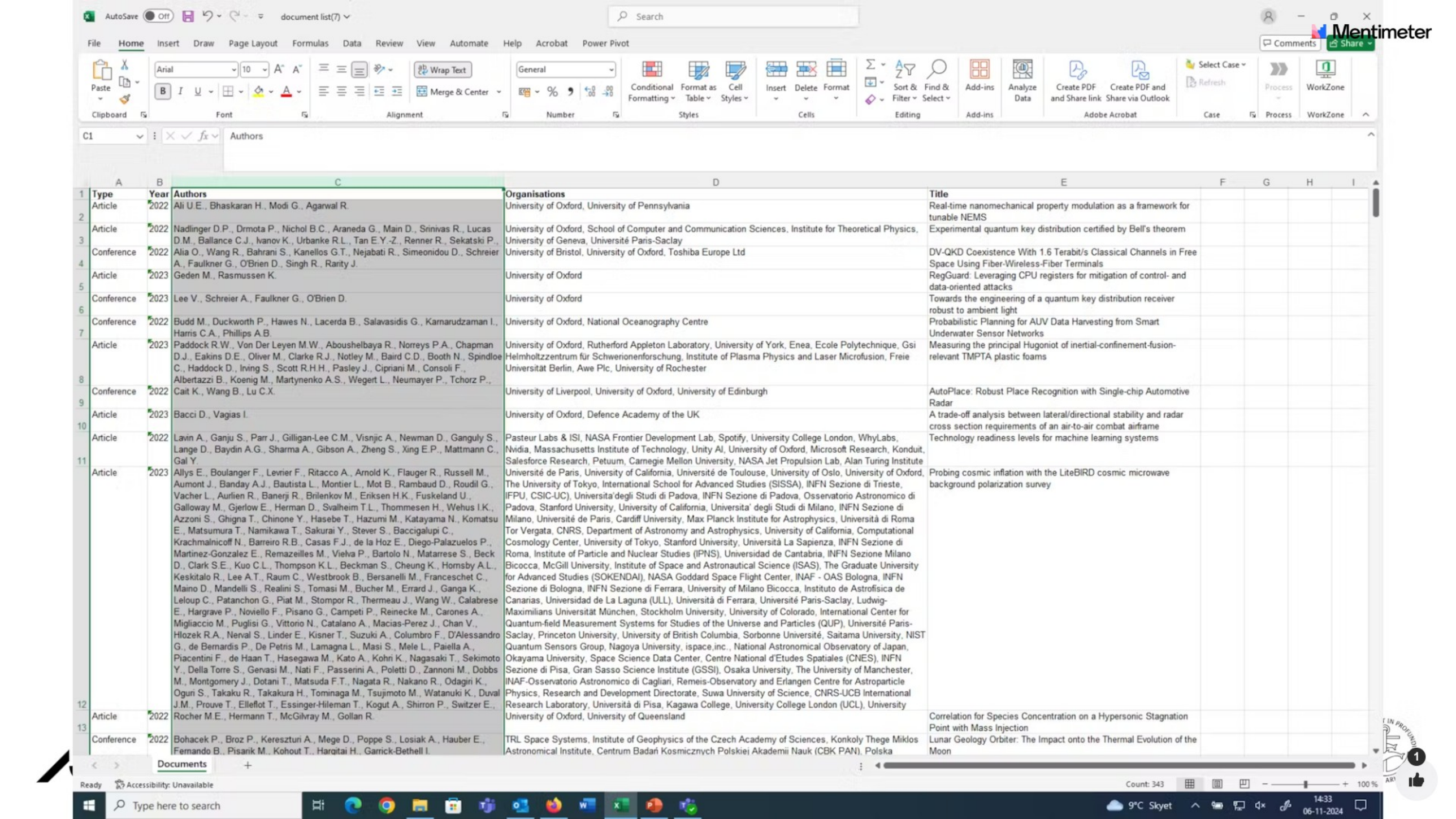
Organisations: **University of Oxford, National Oceanography Centre**

Harvesting valuable ocean data, ranging from climate and marine life analysis to industrial equipment monitoring, is an extremely challenging real-world problem. Sparse underwater sensor networks are a promising approach to scale to larger and deeper environments, but these have difficulty offloading their data without external assistance. Traditionally, offloading data has been achieved by costly, fixed communication infrastructure. In this paper, we propose a planning under uncertainty method that enables an autonomous underwater vehicle (AUV) to adaptively collect data from smart sensor networks in underwater environments. Our novel solution exploits the ability of sensor nodes to provide the AUV with time-of-flight acoustic localisation, and is able to prioritise nodes with the most valuable data. In both simulated experiments and a real-world field trial, we demonstrate that our method outperforms the type of hand-designed behaviours that has previously been used in the context of underwater data harvesting.

Measuring the principal Hugoniot of inertial-confinement-fusion-relevant TMPTA plastic foams

Type: Article | ID: S_2-s2.0-85149563545 | Year: **2023**

Authors: **Paddock R.W., Von Der Leyen M.W., Aboushelbaya R., Norreys P.A., Chapman D.J., Eakins D.E., Oliver M., Clarke R.J., Notley M., Baird C.D., Booth N., Spindloe C., Haddock D., Irving S., Scott R.H.H., Pasley J., Cipriani M., Consoli F., Albertazzi B., Koenig M., Martynenko A.S., Wegert L., Neumayer P., Tchorz P., Raczka P., Mabey P., Garbett W., Goshadze R.M.N., Karasiev V.V., Hu S.X.**



document list(7)

Search

Mentimeter

Authors

Type	Year	Authors	Organisations	Title
Article	2022	Ali U.E., Bhaskaran H., Modi G., Agarwal R.	University of Oxford, University of Pennsylvania	Real-time nanomechanical property modulation as a framework for tunable NEMS
Article	2022	Nadlinger D.P., Drmota P., Nichol B.C., Araneda G., Main D., Srinivas R., Lucas D.M., Ballance C.J., Ivanov K., Urbanke R.L., Tan E.Y.-Z., Renner R., Sekatski P.,	University of Oxford, School of Computer and Communication Sciences, Institute for Theoretical Physics, University of Geneva, Université Paris-Saclay	Experimental quantum key distribution certified by Bell's theorem
Conference	2022	Alia O., Wang R., Bahrani S., Kanellos G.T., Nejabati R., Simeonidou D., Schreier A., Faulkner G., O'Brien D., Singh R., Rarity J.	University of Bristol, University of Oxford, Toshiba Europe Ltd	DV-QKD Coexistence With 1.6 Terabit/s Classical Channels in Free Space Using Fiber-Wireless-Fiber Terminals
Article	2023	Geden M., Rasmussen K.	University of Oxford	RegGuard: Leveraging CPU registers for mitigation of control- and data-oriented attacks
Conference	2023	Lee V., Schreier A., Faulkner G., O'Brien D.	University of Oxford	Towards the engineering of a quantum key distribution receiver robust to ambient light
Conference	2022	Budd M., Duckworth P., Hawes N., Lacerda B., Salavasidis G., Karnarudzaman I., Harris C.A., Phillips A.B.	University of Oxford, National Oceanography Centre	Probabilistic Planning for AUV Data Harvesting from Smart Underwater Sensor Networks
Article	2023	Paddock R.W., Von Der Leyen M.W., Aboushelbaya R., Norreys P.A., Chapman D.J., Eakins D.E., Oliver M., Clarke R.J., Notley M., Baird C.D., Booth N., Spindloe C., Haddock D., Irving S., Scott R.H.H., Pasley J., Cipriani M., Consoli F., Albertazzi B., Koenig M., Martynenko A.S., Wegert L., Neumayer P., Tchorz P.,	University of Oxford, Rutherford Appleton Laboratory, University of York, Enea, Ecole Polytechnique, Gsi Helmholtzzentrum für Schwerionenforschung, Institute of Plasma Physics and Laser Microfusion, Freie Universität Berlin, Awe Plc, University of Rochester	Measuring the principal Hugoniot of inertial-confinement-fusion-relevant TMPTA plastic foams
Conference	2022	Cait K., Wang B., Lu C.X.	University of Liverpool, University of Oxford, University of Edinburgh	AutoPlace: Robust Place Recognition with Single-chip Automotive Radar
Article	2023	Bacci D., Vagias I.	University of Oxford, Defence Academy of the UK	A trade-off analysis between lateral/directional stability and radar cross section requirements of an air-to-air combat airframe
Article	2022	Lavin A., Ganju S., Parr J., Gilligan-Lee C.M., Visnjic A., Newman D., Ganguly S., Lange D., Baydin A.G., Sharma A., Gibson A., Zheng S., Xing E.P., Mattmann C., Gal Y.	Pasteur Labs & ISI, NASA Frontier Development Lab, Spotify, University College London, WhyLabs, Nvidia, Massachusetts Institute of Technology, Unity AI, University of Oxford, Microsoft Research, Konduit, Salesforce Research, Petuum, Carnegie Mellon University, NASA Jet Propulsion Lab, Alan Turing Institute	Technology readiness levels for machine learning systems
Article	2023	Allys E., Boulanger F., Levrier F., Ritacco A., Arnold K., Flauger R., Russell M., Aumont J., Banday A.J., Bautista L., Montier L., Mot B., Rambaud D., Roudil G., Vacher L., Aurlien R., Banerji R., Brilenkov M., Eriksen H.K., Fuskeland U., Galloway M., Gjerlow E., Herman D., Svalheim T.L., Thommesen H., Wehus I.K., Azzoni S., Ghigna T., Chinone Y., Hasebe T., Hazumi M., Katayama N., Komatsu E., Matsumura T., Namikawa T., Sakurai Y., Stever S., Baccigalupi C., Krachmalnicoff N., Barreiro R.B., Casas F.J., de la Hoz E., Diego-Palazuelos P., Martinez-Gonzalez E., Remazeilles M., Vielva P., Bartolo N., Matarrese S., Beck D., Clark S.E., Kuo C.L., Thompson K.L., Beckman S., Cheung K., Hornsby A.L., Keskitalo R., Lee A.T., Raum C., Westbrook B., Bersanelli M., Franceschet C., Maino D., Mandelli S., Realini S., Tomasi M., Bucher M., Errard J., Ganga K., Leloup C., Patanchon G., Piat M., Stompor R., Thermeau J., Wang W., Calabrese E., Hargrave P., Noviello F., Pisano G., Campeti P., Reinecke M., Carones A., Migliaccio M., Puglisi G., Vittorio N., Catalano A., Macias-Perez J., Chan V., Hlozek R.A., Nerval S., Linder E., Kisner T., Suzuki A., Columbro F., D'Alessandro G., de Bernardis P., De Petris M., Lamagna L., Masi S., Mele L., Paiella A., Piacentini F., de Haan T., Hasegawa M., Kato A., Kohri K., Nagasaki T., Sekimoto Y., Della Torre S., Gervasi M., Nati F., Passerini A., Poletti D., Zannoni M., Dobbs M., Montgomery J., Dotani T., Matsuda F.T., Nagata R., Nakano R., Odagiri K., Oguri S., Takaku R., Takakura H., Tominaga M., Tsujimoto M., Watanuki K., Duval J.M., Prouve T., Elleflot T., Essinger-Hileman T., Kogut A., Shirron P., Switzer E.,	Université de Paris, University of California, Université de Toulouse, University of Oslo, University of Oxford, The University of Tokyo, International School for Advanced Studies (SISSA), INFN Sezione di Trieste, IFPU, CSIC-UC), Universita'degli Studi di Padova, INFN Sezione di Padova, Osservatorio Astronomico di Padova, Stanford University, University of California, Universita' degli Studi di Milano, INFN Sezione di Milano, Université de Paris, Cardiff University, Max Planck Institute for Astrophysics, Università di Roma Tor Vergata, CNRS, Department of Astronomy and Astrophysics, University of California, Computational Cosmology Center, University of Tokyo, Stanford University, Università La Sapienza, INFN Sezione di Roma, Institute of Particle and Nuclear Studies (IPNS), Universidad de Cantabria, INFN Sezione Milano Bicocca, McGill University, Institute of Space and Astronautical Science (ISAS), The Graduate University for Advanced Studies (SOKENDAI), NASA Goddard Space Flight Center, INAF - OAS Bologna, INFN Sezione di Bologna, INFN Sezione di Ferrara, University of Milano Bicocca, Instituto de Astrofisica de Canarias, Universidad de La Laguna (ULL), Università di Ferrara, Université Paris-Saclay, Ludwig-Maximilians Universität München, Stockholm University, University of Colorado, International Center for Quantum-field Measurement Systems for Studies of the Universe and Particles (QUP), Université Paris-Saclay, Princeton University, University of British Columbia, Sorbonne Université, Saitama University, NIST Quantum Sensors Group, Nagoya University, ispace,inc., National Astronomical Observatory of Japan, Okayama University, Space Science Data Center, Centre National d'Etudes Spatiales (CNES), INFN Sezione di Pisa, Gran Sasso Science Institute (GSSI), Osaka University, The University of Manchester, INAF-Osservatorio Astronomico di Cagliari, Remeis-Observatory and Erlangen Centre for Astroparticle Physics, Research and Development Directorate, Suwa University of Science, CNRS-UCB International Research Laboratory, Università di Pisa, Kagawa College, University College London (UCL), University	Probing cosmic inflation with the LiteBIRD cosmic microwave background polarization survey
Article	2022	Rocher M.E., Hermann T., McGilvray M., Gollan R.	University of Oxford, University of Queensland	Correlation for Species Concentration on a Hypersonic Stagnation Point with Mass Injection
Conference	2022	Bohacek P., Broz P., Kereszturi A., Mege D., Poppe S., Losiak A., Hauber E., Fernando B., Pisarik M., Kohout T., Hargitai H., Garrick-Bethell I.	TRL Space Systems, Institute of Geophysics of the Czech Academy of Sciences, Konkoly Thege Miklos Astronomical Institute, Centrum Badań Kosmicznych Polskiej Akademii Nauk (CBK PAN), Polska	Lunar Geology Orbiter: The Impact onto the Thermal Evolution of the Moon

Documents

Ready

Accessibility: Unavailable

Count: 343

100 %

Type here to search

9°C Skyet

14:33

06-11-2024

WHAT DID WE DO WITH THE DATA

- The database has a narrow focus on export control – 0,6% of all AU publications turned up in TIM. A total of 240 hits in 2020-2023 out of 40,000 publications.
- We downloaded in excel and pdf and added columns to sort/insert data like PI from AU, department/school, foreign institutions, countries. I then analysed how critical they were and color-coded them red, yellow and green depending on topics/research field.
- I then looked at cooperation with risk countries including looking for cooperation patterns.
- Took me 8-9 days full time to sort and add data.
- https://knowledge4policy.ec.europa.eu/text-mining/tim-dual-use_en

HOW DO WE USE TIM

- The dataset turned out to be a good starting point for a dialogue with each department because we started by looking at concrete data. They did not know much.
- Physical or virtual meetings with all 32 departments (17 completed now) on export control.
- All TIM hits were discussed – expect only 5-10 cases where we maybe need to license.
- The discussions went on to cover upcoming mapping of critical technologies, vulnerable research groups, background checks of staff, guest and ph.d.s, physical security, cyber security, new policy for accepting research projects/cooperation. Covers most of EU's ICP structure. Need to look at audit and documentation.
- Identifying what we consider to be our own critical infrastructures.
- Starting to look at bibliometric data on all cooperation with China, Russia and Iran.
- Next steps: diving into critical cases; visit all departments next year to do critical technologies mapping and local training.

AARHUS
UNIVERSITY

What open-source resources have you found useful in developing your own response to research security challenges?

ASPI tracker

John, fascinating work. How do you present all this data to stakeholders at your institution? Do you use the spreadsheets, or do you combine the info into a dashboard?

https://unitracker.aspi.org.au/defence-laboratories/

UK, EU and US Sanctions Lists

TIM, Aspiii, Freeform house

Dimensions, for publication dataDimensions security app (paid)

https://www.aspi.org.au/report/picking-flowers-making-honey

Aspi and SciVal

1 8

What open-source resources have you found useful in developing your own response to research security challenges?

Sources: opensactions.org, ASPI tracker, iranwatch, the website of the partner research group in their original (!)language (use a browser extension to translate), Bing Copilot (yes...)

Dimensions - a commercial tool that includes publications, patents, clinical trials and funds, that our Library subscribes too. You can map researchers collaborations over time.

Discussion: please ask any questions

Was the number of papers higher or lower than you expected?

What limitations have you come across in terms of the data?

Did you highlight the legal (compliance) rules, or did you go broader than the legal restrictions and discussed broader research policy (institutional) restrictions?

What an amazing database! How do you approach things like doing background checks on staff and students without running into problems?

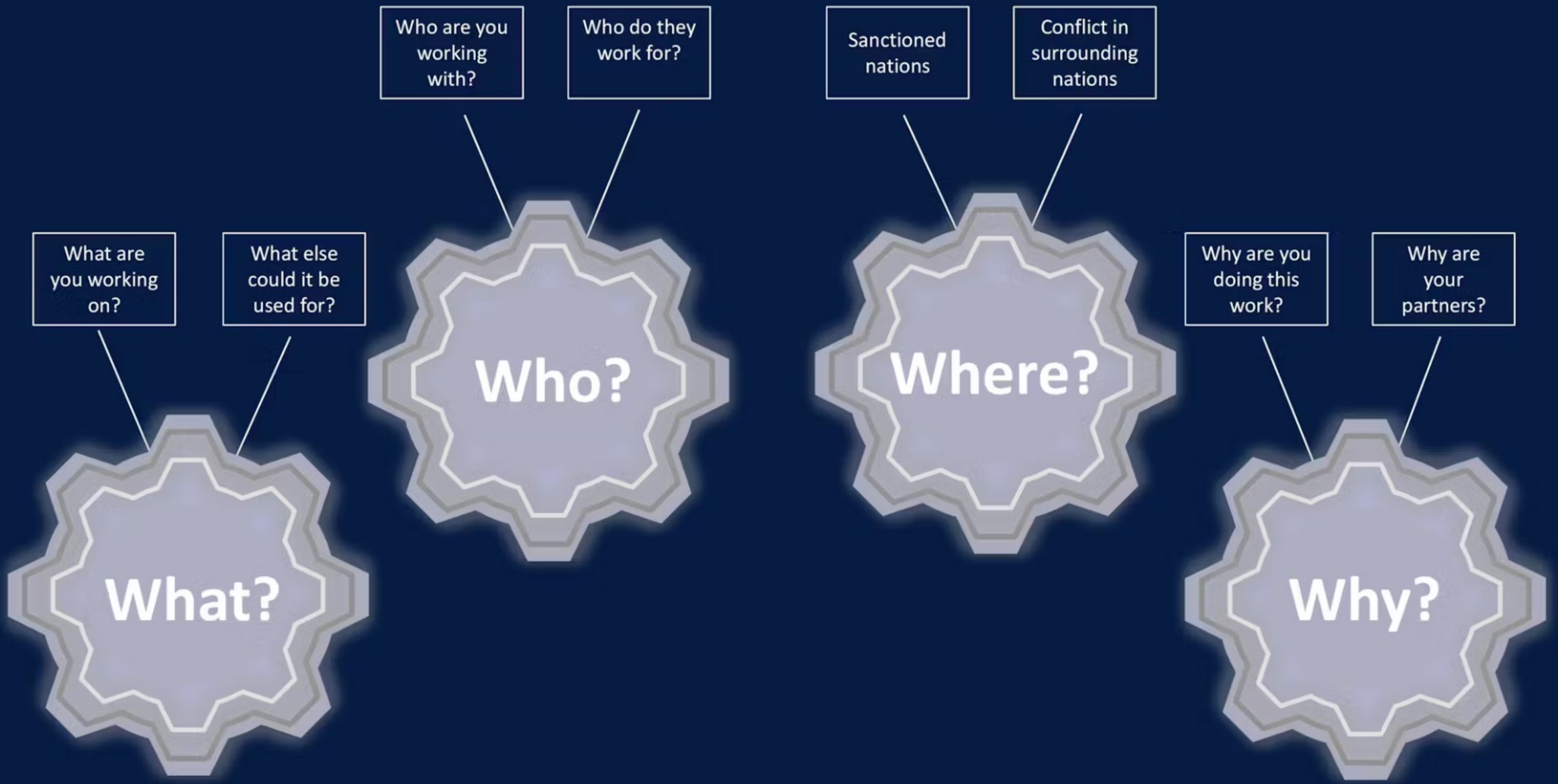
Were there any data quality issues?

Other Options in case not able to find my institution/ university in TIM database?

3 5

Open-source resources to support due diligence

Triage questions for effective due diligence prioritisation



WHAT ?

What are hostile states and actors targeting?

Dual-use and emerging technologies

A dual-use technology can have both a civilian and military use

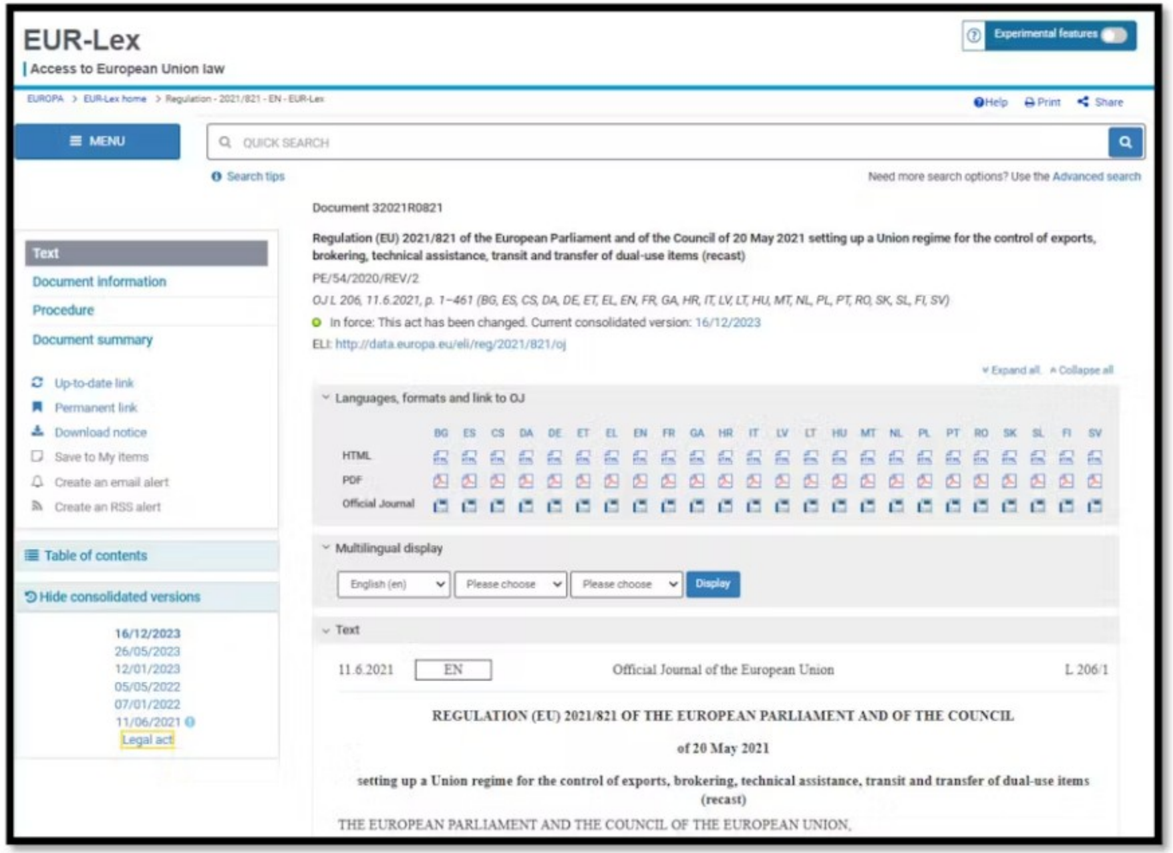
The hallmarks of dual-use and emerging technologies include:

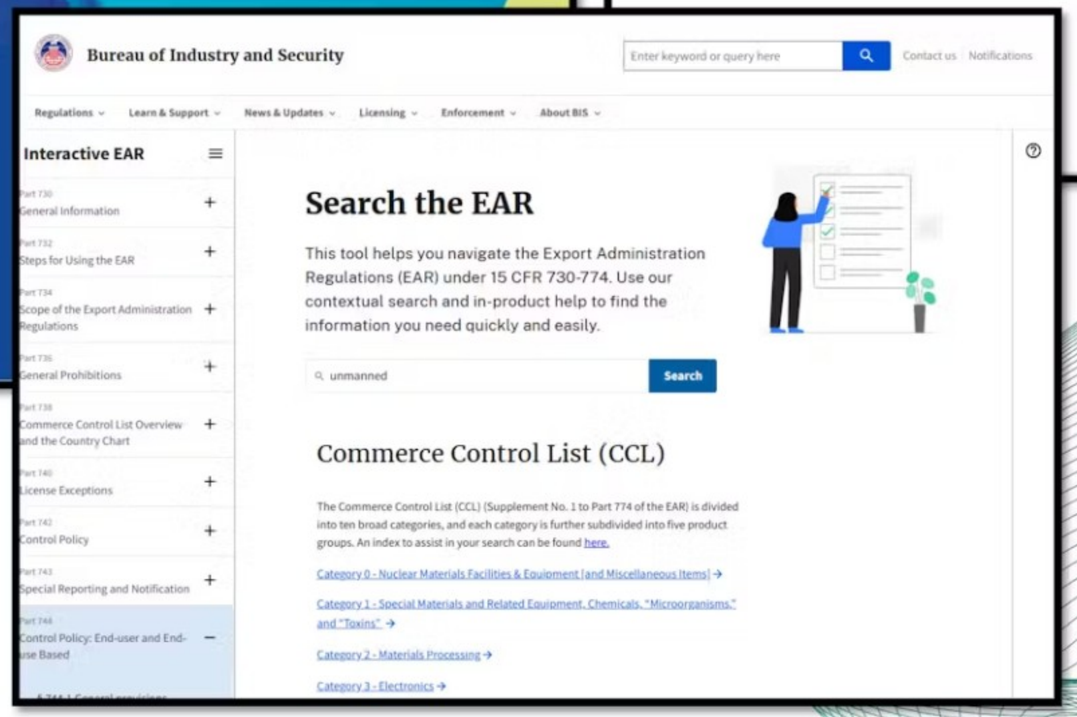
- Versatile
- Cross-disciplinary
- Ambiguous
- Innovative
- Rapid advance

Emerging technology areas include

Advanced Materials	Advanced Robotics	Artificial Intelligence	Autonomous Systems	Civil Nuclear	Communications	Computing Hardware
Critical Suppliers to Government	Cryptographic Authentication	Data Infrastructure	Defence	Energy	Genetic Engineering	Military and Dual-Use
Quantum Technologies	Satellite and Space Technologies	Suppliers to the Emergency Services	Sustainable Technologies	Synthetic Biology	Transport	Virtual and augmented reality

Resources to identify ‘what’



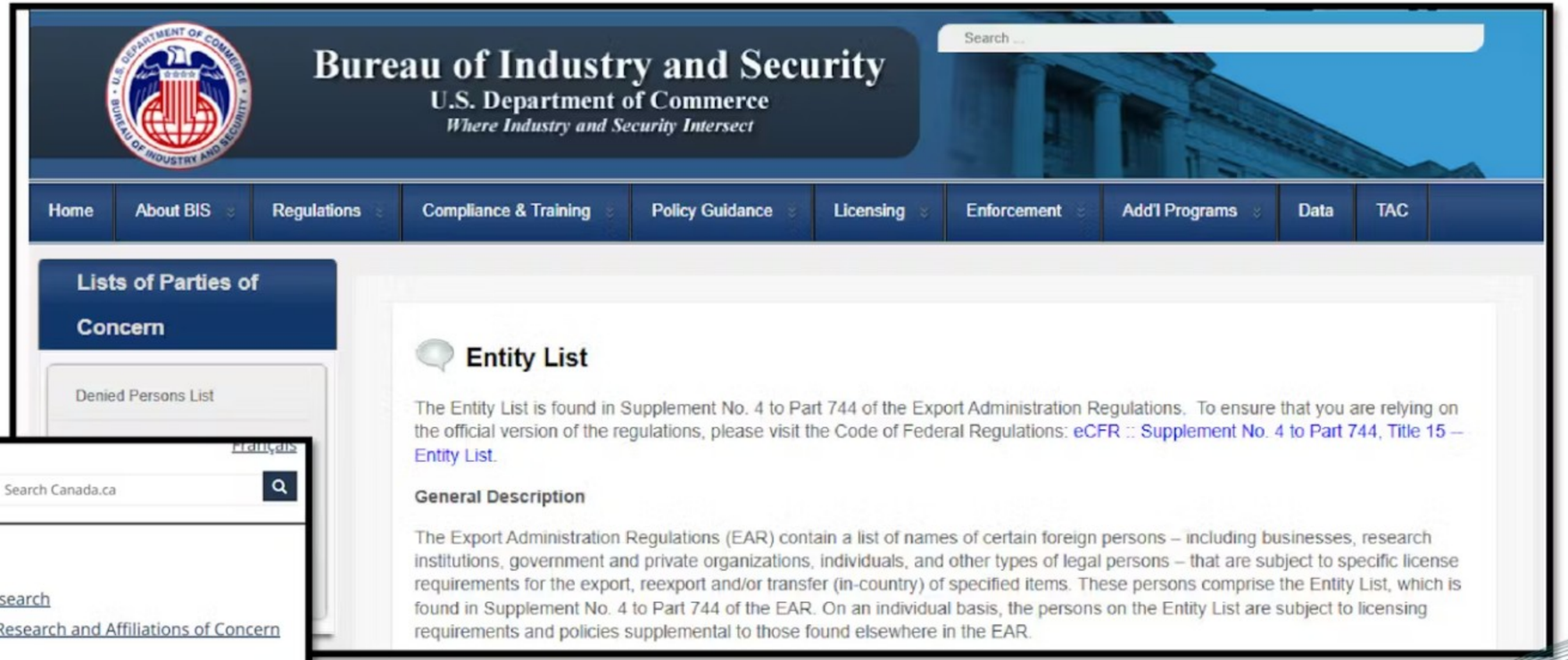


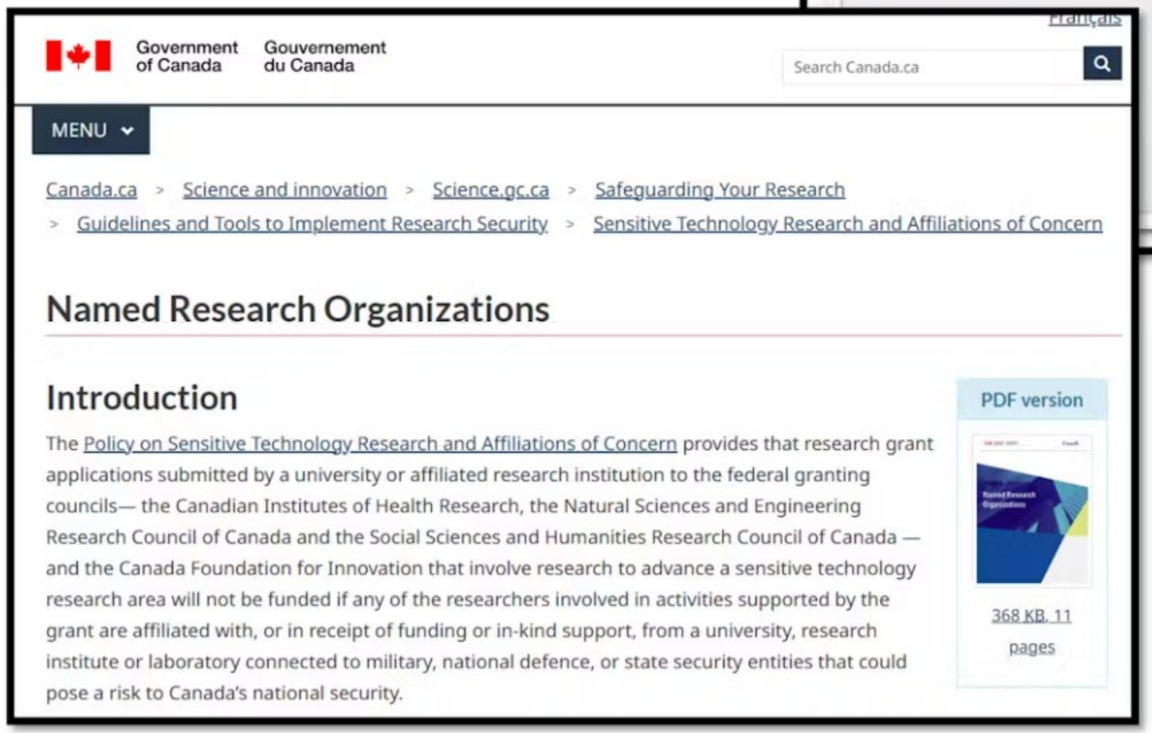
Mentimeter

1

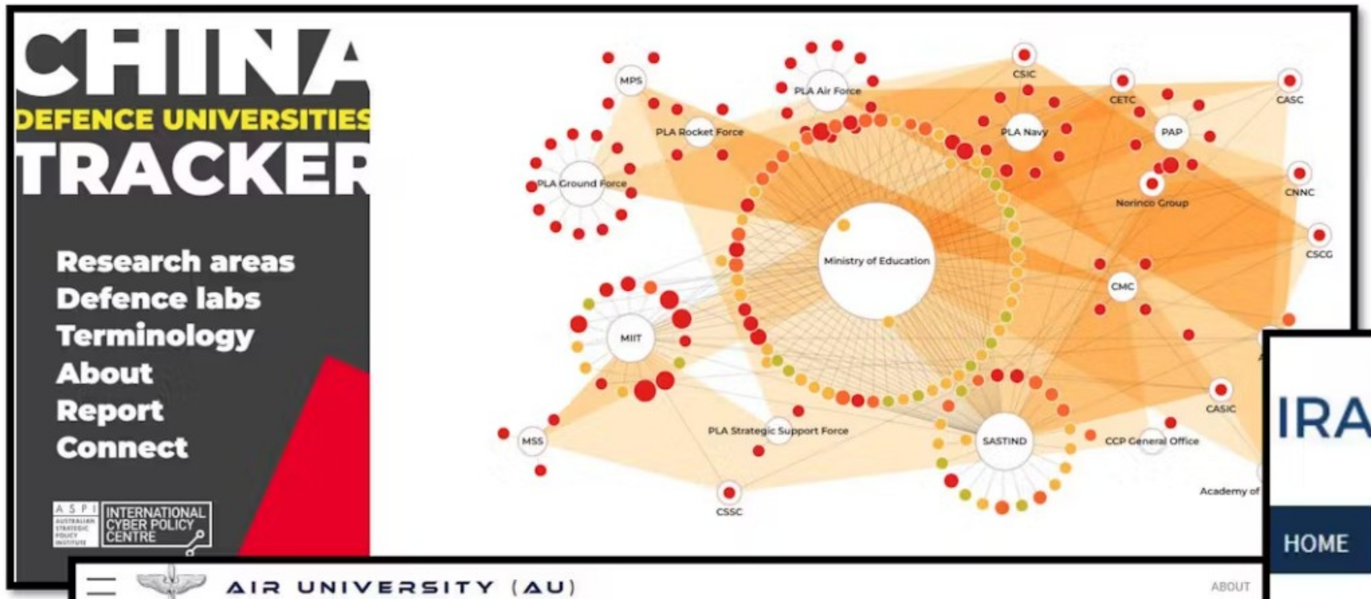
WHO?

Resources to identify ‘who’

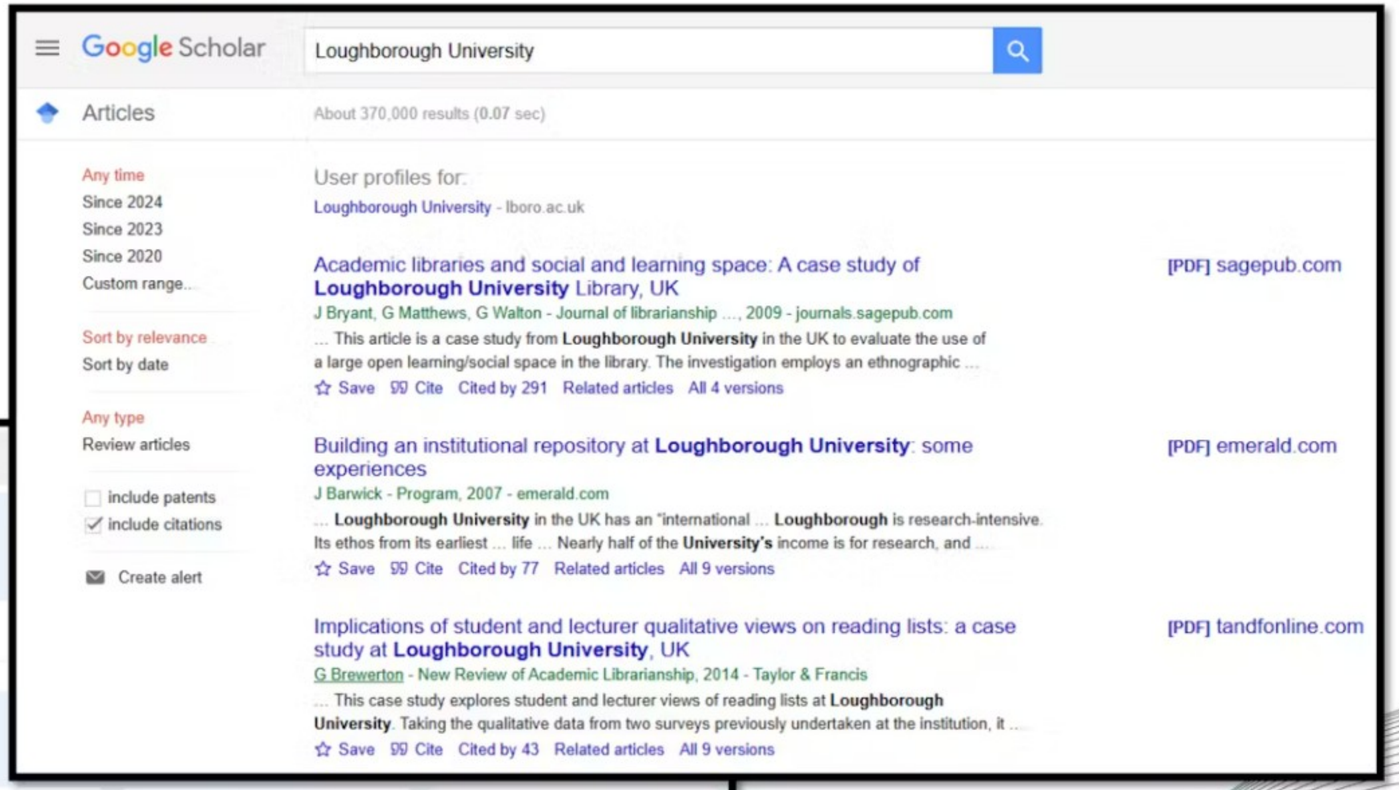


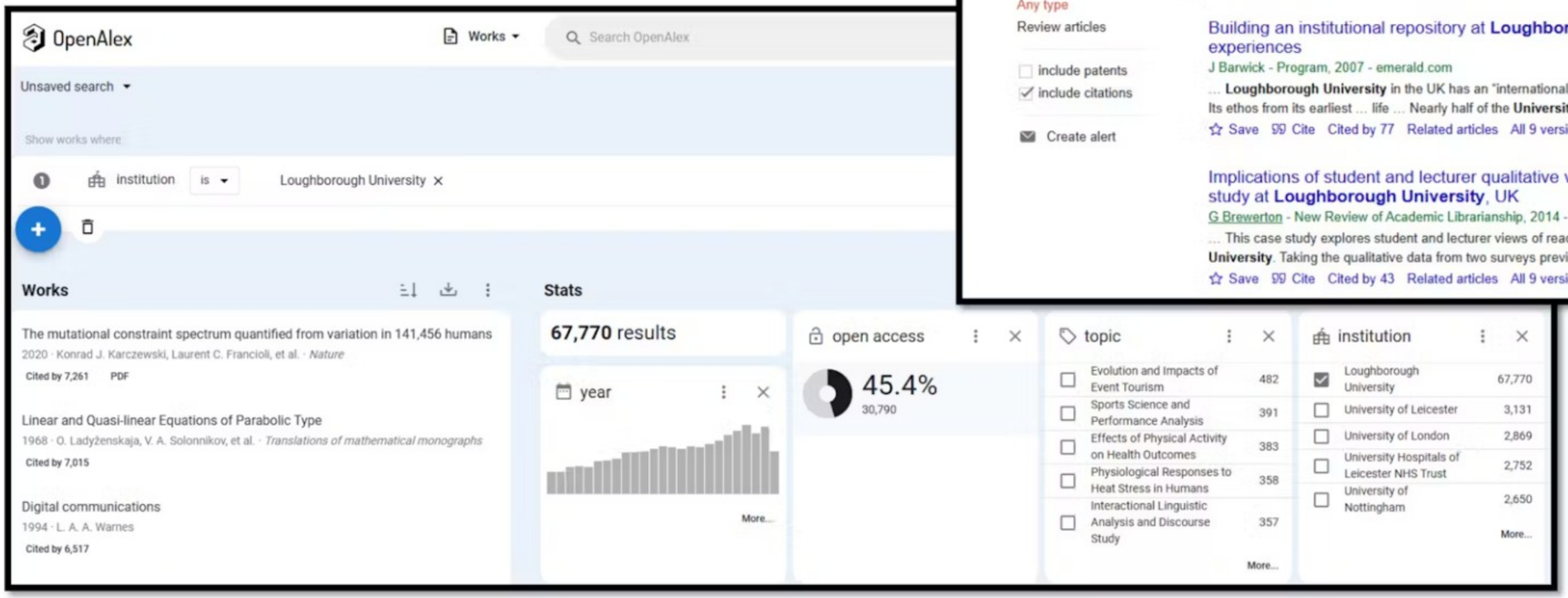


Resources to identify ‘who’



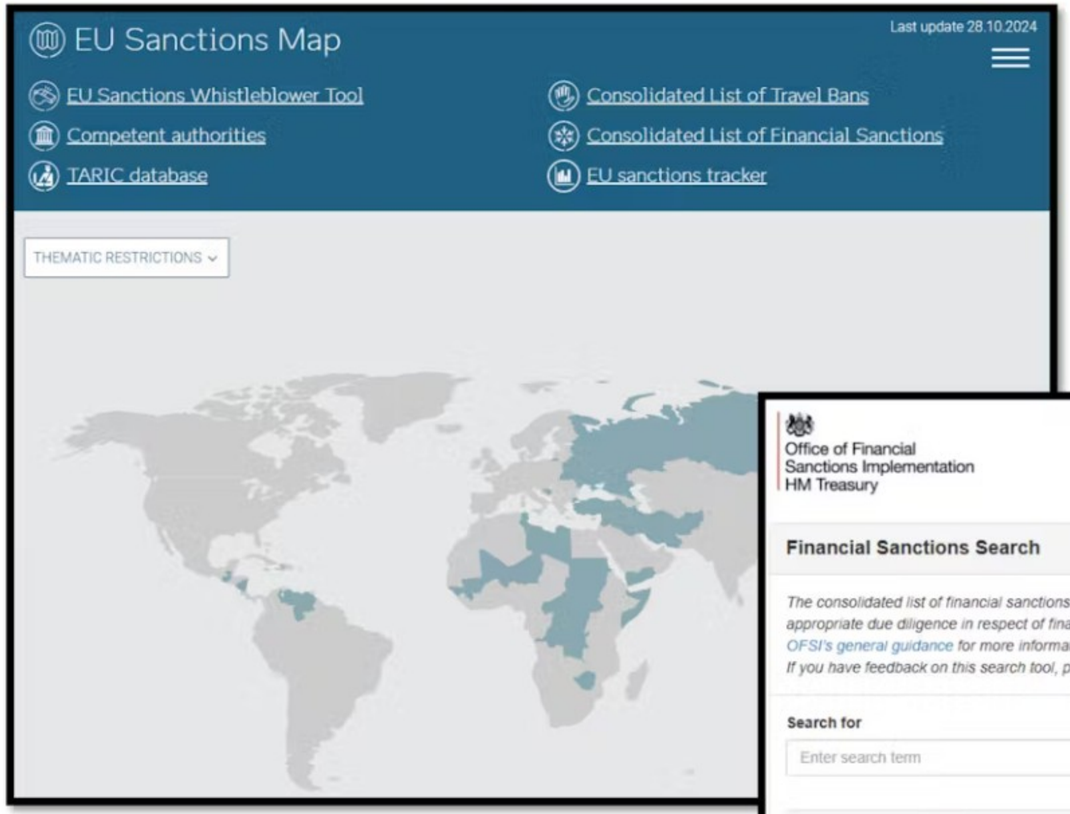
Resources to identify ‘who’

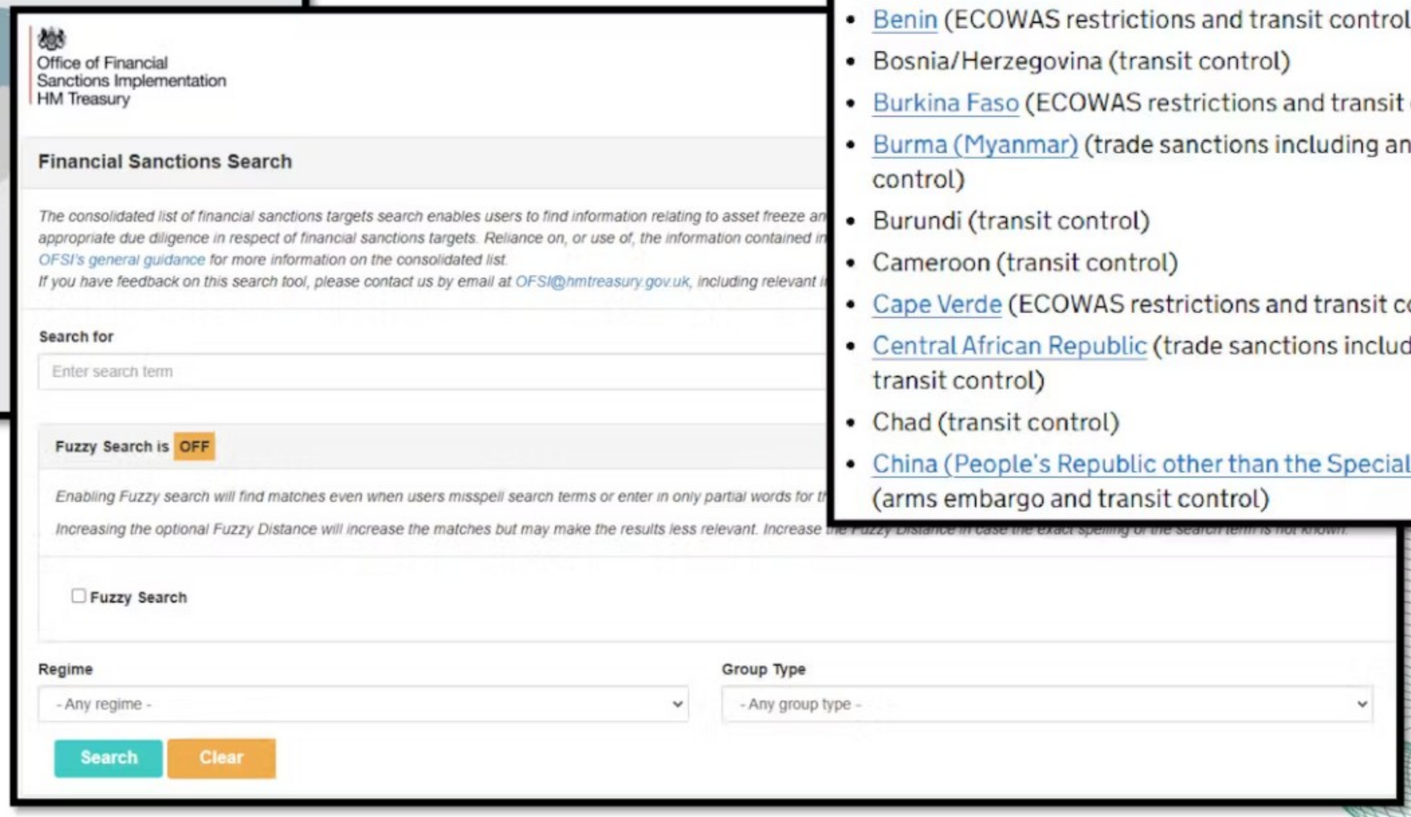




WHERE ?

Resources to identify ‘where’





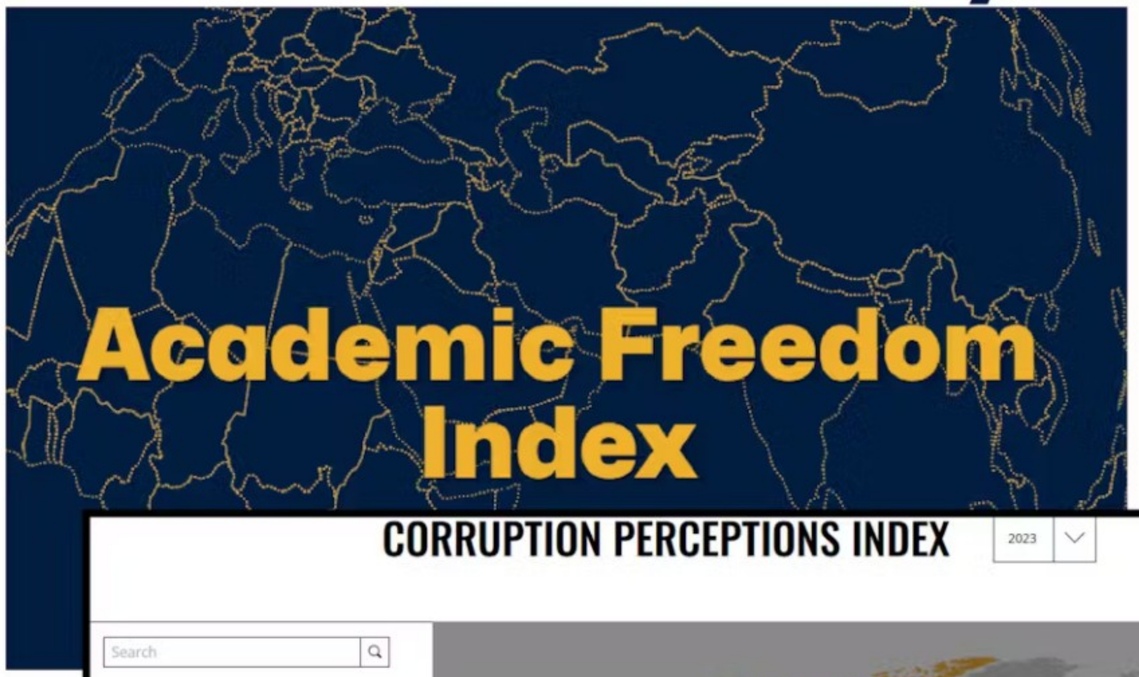
Countries subject to arms embargo, trade sanctions and other trade restrictions

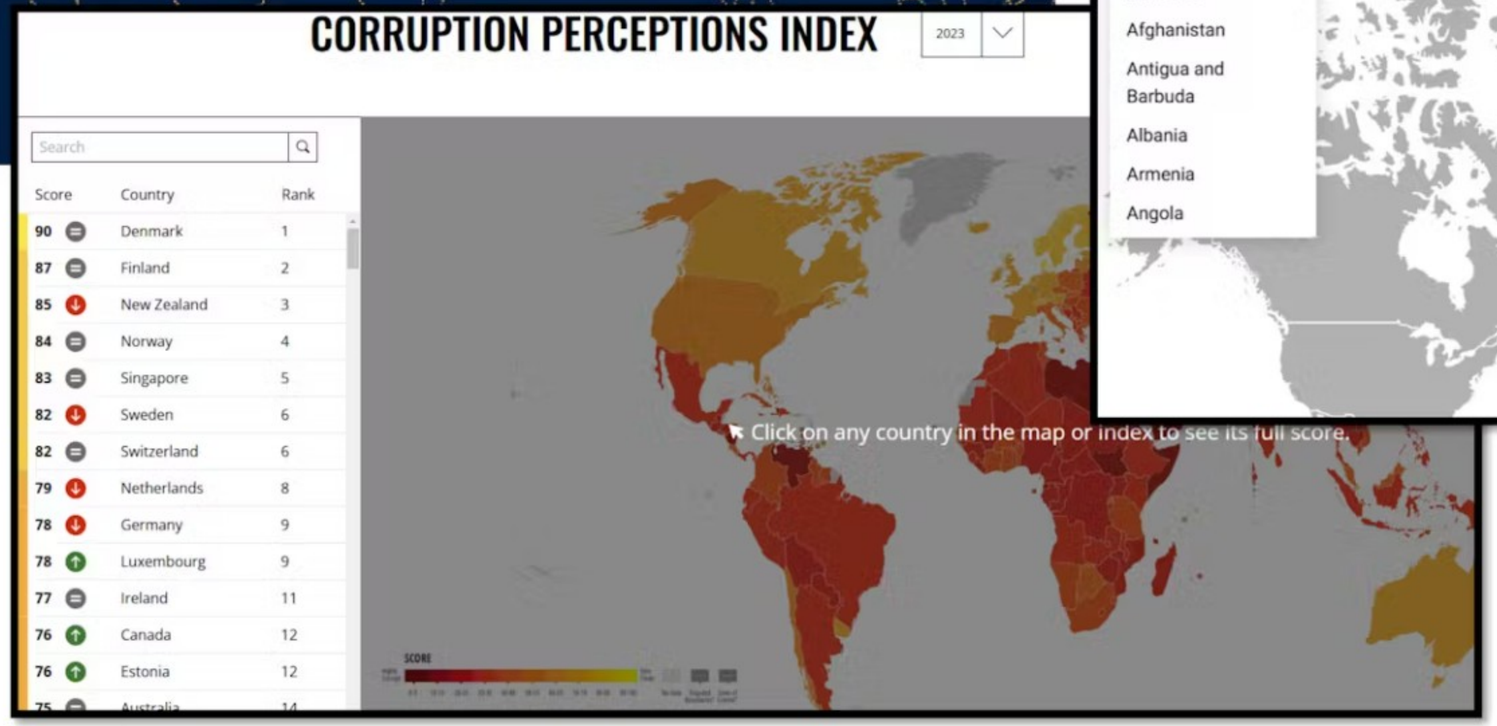
This list details specific countries where arms embargo, trade sanctions and other trade restrictions have been imposed. This list does not include countries subject to only financial or other types of sanctions.

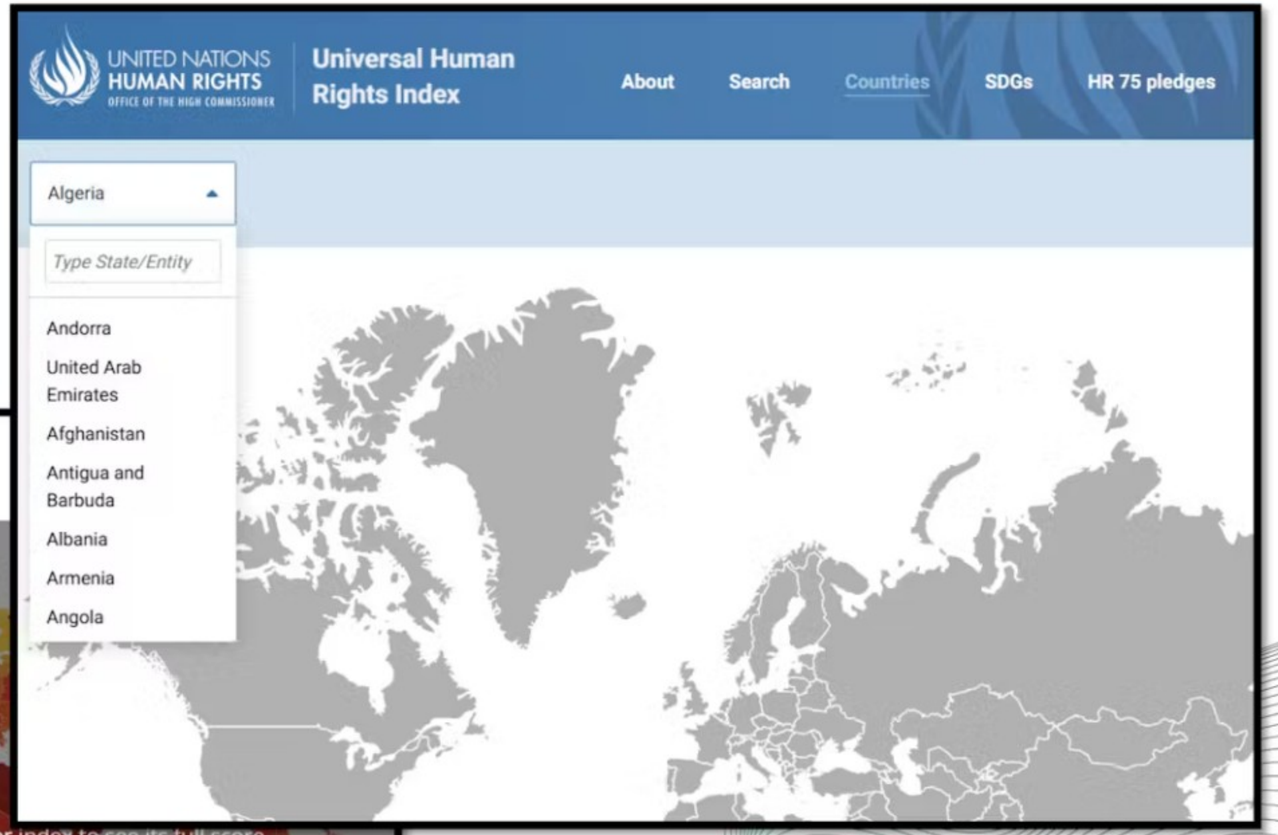
List of countries:

- Afghanistan (trade sanctions including an arms embargo, and transit control)
- Albania (transit control)
- Argentina (trade restrictions and transit control)
- Armenia (arms embargo, trade controls, and transit control)
- Azerbaijan (arms embargo, trade controls, and transit control)
- Belarus (trade sanctions including an arms embargo, and transit control)
- Benin (ECOWAS restrictions and transit control)
- Bosnia/Herzegovina (transit control)
- Burkina Faso (ECOWAS restrictions and transit control)
- Burma (Myanmar) (trade sanctions including an arms embargo, and transit control)
- Burundi (transit control)
- Cameroon (transit control)
- Cape Verde (ECOWAS restrictions and transit control)
- Central African Republic (trade sanctions including an arms embargo, and transit control)
- Chad (transit control)
- China (People's Republic other than the Special Administrative Regions) (arms embargo and transit control)

Resources to identify ‘where’

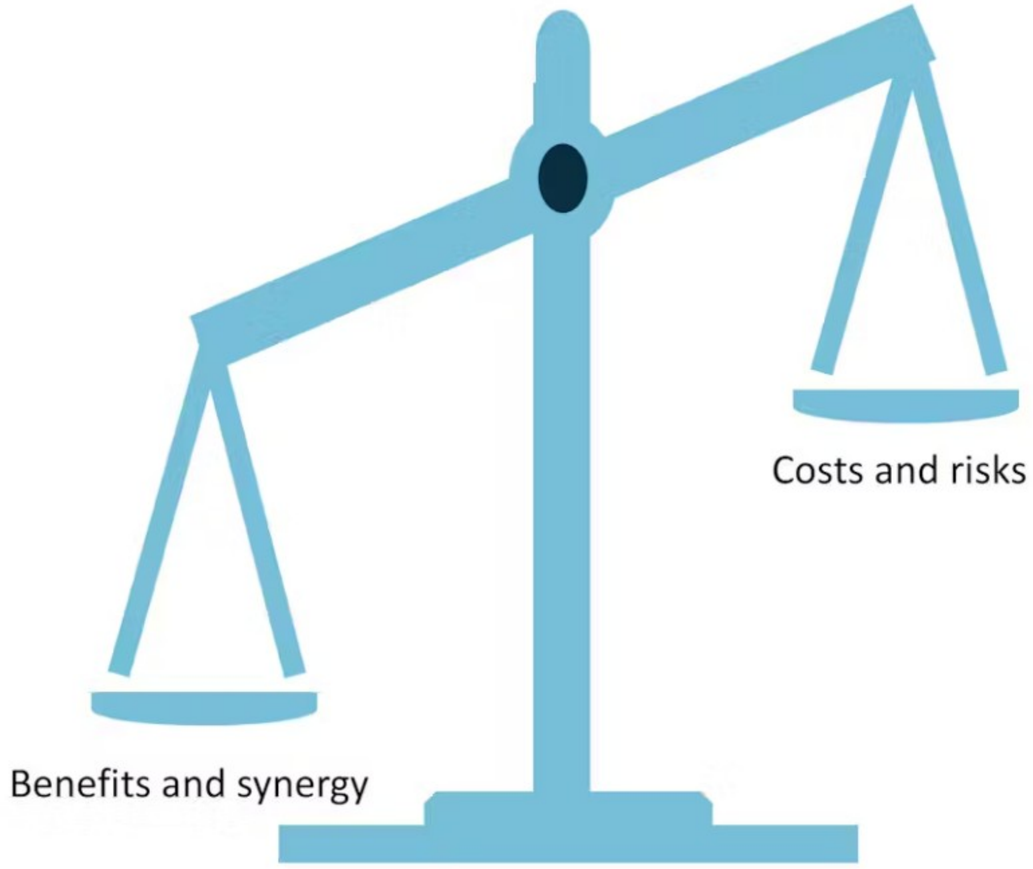






WHY?

Resources to identify ‘why’



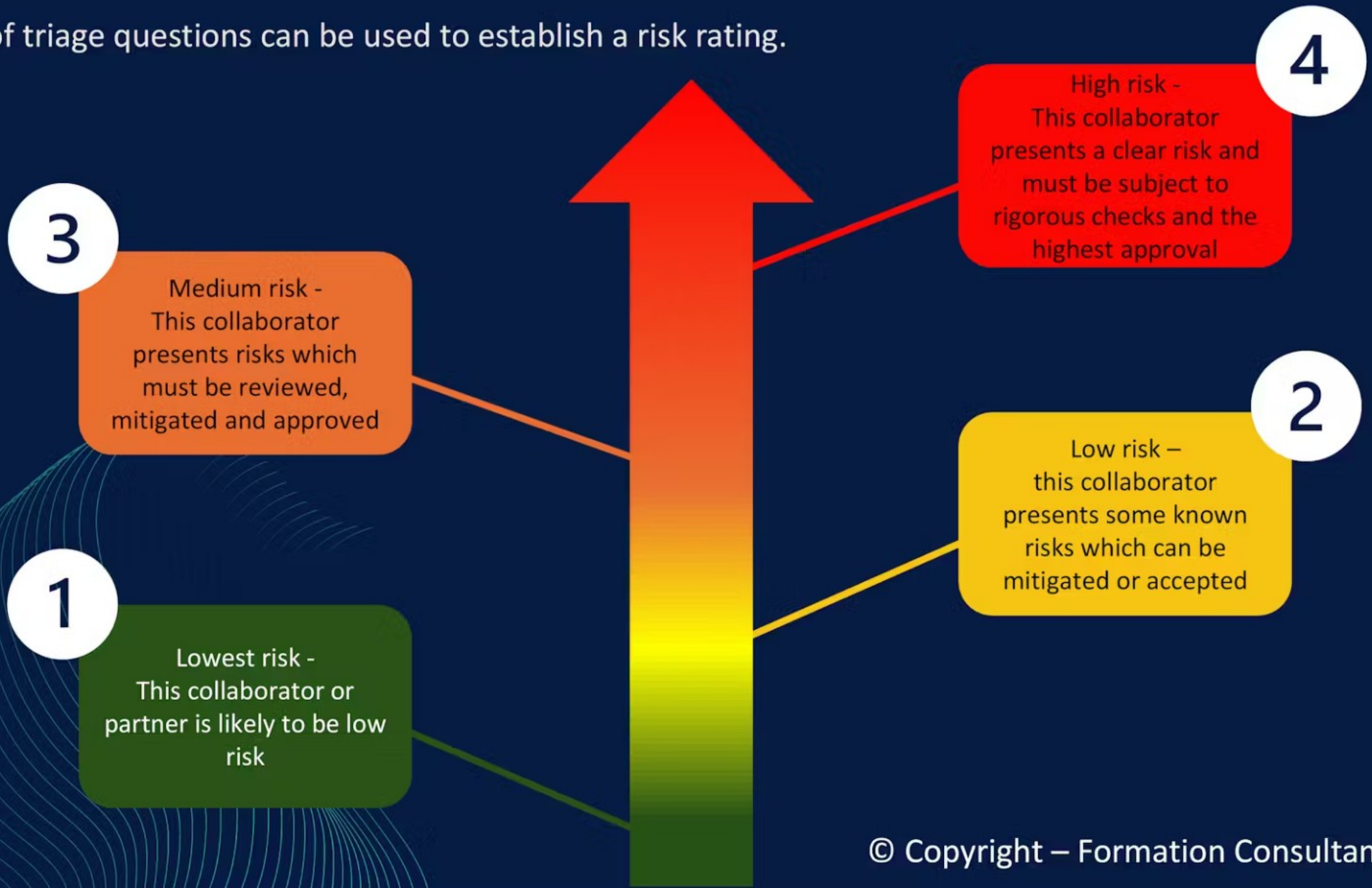
There is a balance between providing assurance and creating excessive burdens on your organisation’s resources.

This means making decisions around your organisational appetite for risk, financial assurance, reputational and political standing and horizon scanning.

IMPLEMENTATION

Establishing risk levels

A simple set of triage questions can be used to establish a risk rating.

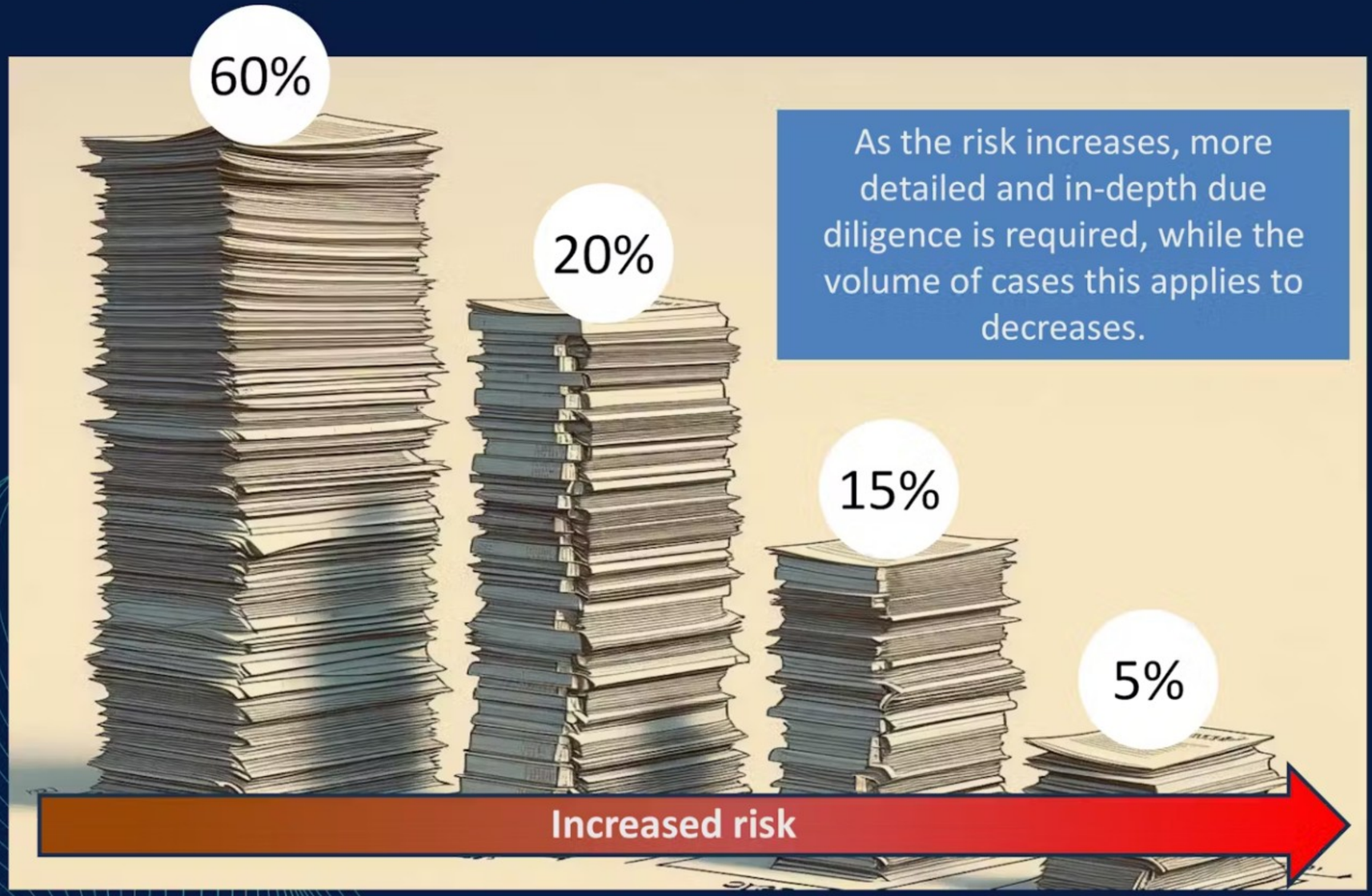


Tailoring Due Diligence with Risk Ratings

Once this risk rating has been established, you can use a standard due diligence template, increasing the areas reviewed according to the risks identified.

This ensures that you focus the maximum amount of our resources on the highest-risk activities.

Due diligence caseloads in relation to the risk level



Mentimeter

UNIVERSITY of STIRLING

OTOR Analysis

Opportunities

Asks what benefits or opportunities does this present for the University of Stirling?

Technology area

Considers the technology, sector or subject area that is included within the proposed research or partnership.

O T

O R

Organisations

Considers the organisations in a proposed partnership, any links to other organisations and identifies conflicts of interest.

Region

Considers the geopolitical factors of regions of operation; including sanctions, human rights and corruption.

Mentimeter

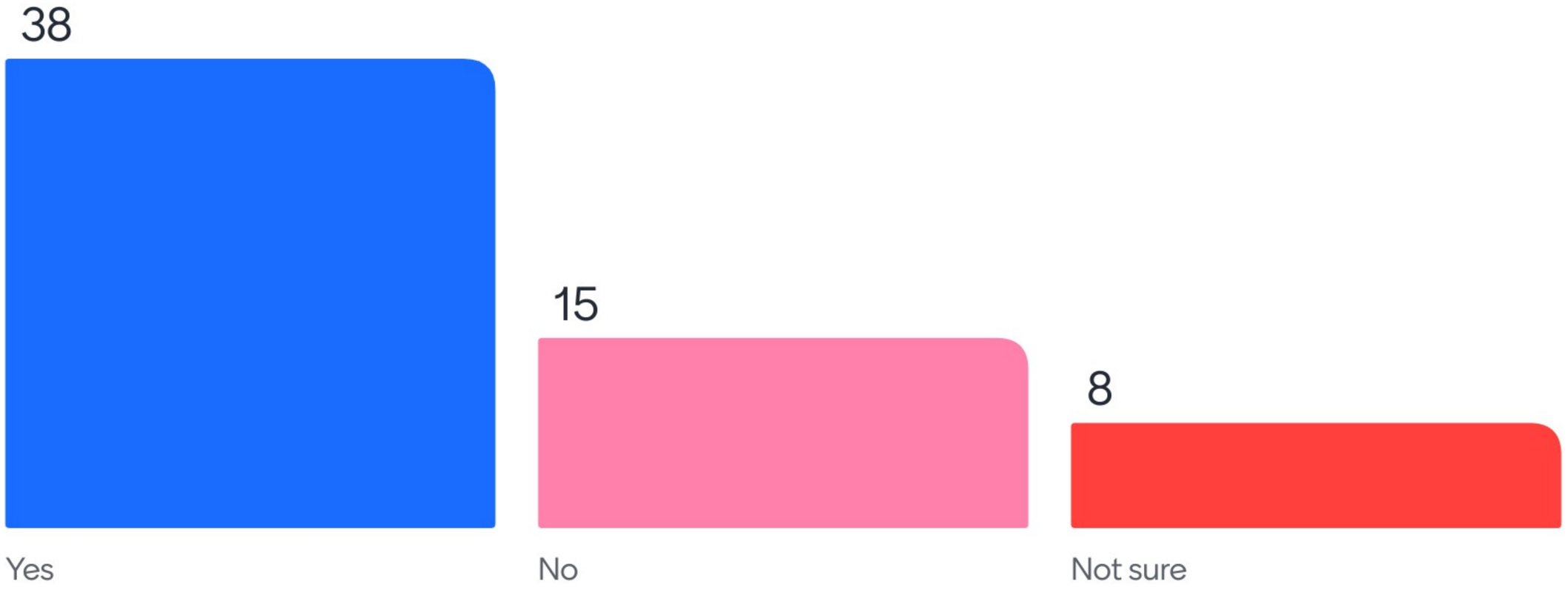
UNIVERSITY of STIRLING

Risk categories:

Risk appetite levels will vary, in some areas it will be ‘averse’ or ‘cautious’, in others it will be ‘open’ or ‘eager’. Challenge can still be found in this approach i.e. adverse risk appetite for legal and compliance risks but open on partnerships.

BE THE DIFFERENCE

Do you have processes in place to triage research security risks at your organisation?



What open-source resources have you found useful to triage research security risks?

ASPI tracker

OpenCorporates for checking company ownership, directors and subsidiaries

Iran watch

Dimensions (for publication data)Dimensions security app (paid)

Bellingcat

Canada, US, Japan, EU and UN sanctions

Dimensions

Xapien , Open Corporate , Company House

What open-source resources have you found useful to triage research security risks?

CreditSafe for financial risk analysis

University subscription to Dow Jones for Factiva

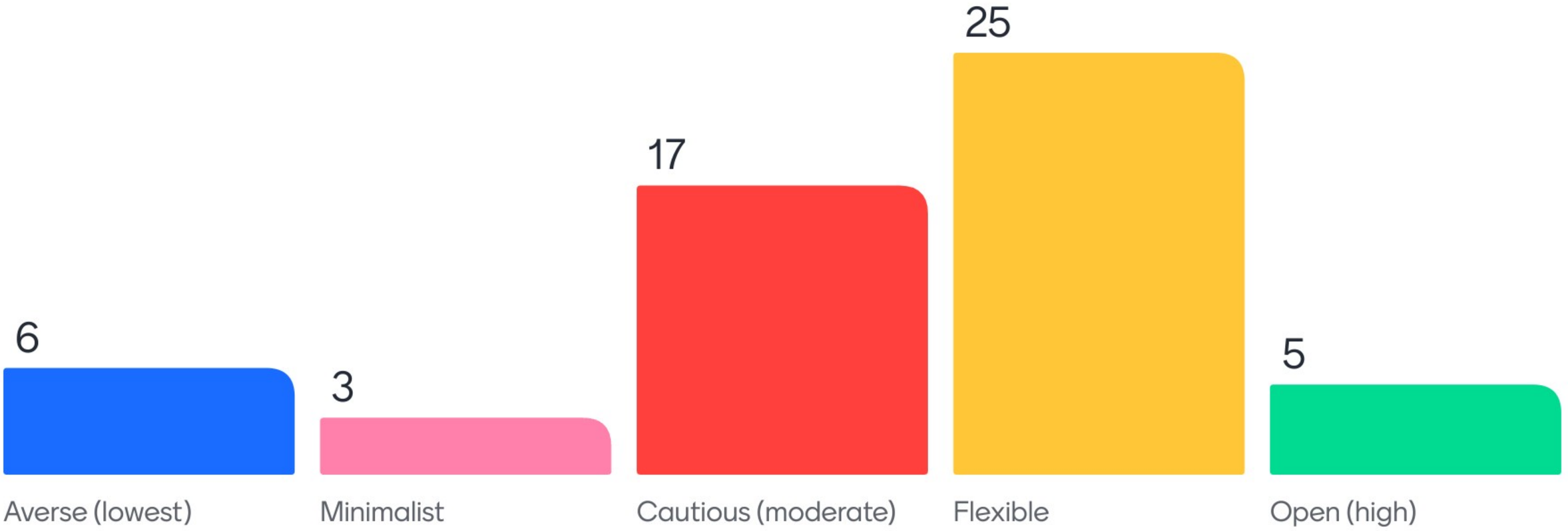
Companies House/Government business registration- checking persons with significant control and whether they are based overseas

Open Sanctions

Trademo for private companies (free)

IndueD

How would you describe your organisation's risk appetite?



Discussion: please ask any questions or add any comments or reflections on today's session

Thank you for joining us today!

Final events in this series:

- Products to support research security management (December 12th 2024, 09:30-11:00)

Loughborough University

UNIVERSITY of STIRLING

FORMATION CONSULTANCY LIMITED

UK Science & Innovation Network