HEECA The Higher Education Export Control Association

Sharing Best Practice and Lessons Learned: A Collaborative UK & EU Approach to Secure Internationalisation

HEECA & EECARO Collaborative Workshop Report

April 2024

With support from

UK Science & Innovation Network

EECARO European Export Control Association for Research Organisations

About us

Higher Education Export Control Association (HEECA)

The UK Higher Education Export Control Association (HEECA) is a sector led, institutionally agnostic association formed in 2021, by research security professionals at some of the UK's leading research-intensive universities.

Although initially focused on the development and promotion of best practice in export control compliance, HEECA has over time, expanded its activities across the broader research security agenda to reflect the dynamic, complex and ever-changing landscape of UK national security. HEECA acts as a conduit between practitioners, regulators, UK Government, and other stakeholders, enabling collaboration and a consistent approach to security compliance at a national level.

As well as this, HEECA has developed and offers the first UK national training programme for UK Export Controls in the context of Higher Education, which is made freely available for all HE institutions to access and enrol onto, across the UK.

European Export Control Association for Research Organisations (EECARO)

The European Export Control Association for Research Organisations (EECARO) is a network that aims to unite European Union research institutes, universities and their export control compliance officers with a view to address the specific character of export controls in a research context. EECARO provides a platform for exchanging information and sharing experiences on how to comply with export control regulations, with the aim to enhance the quality and effectiveness of partners' internal export control compliance programmes.

Through collaboration with its members, EECARO acts as a source of expertise to European and national governments on export control issues affecting research institutes and universities, analysing and advocating for relevant policies and regulations.

UK Science & Innovation Network (SIN)

As part of the Foreign, Commonwealth & Development Office and Department for Science, Innovation and Technology, The UK's Science and Innovation Network (SIN) leads on developing science partnerships and deploying science diplomacy around the world.

Contents

Introduction

Delivered in collaboration between HEECA and EECARO the UK SIN supported project delivered an in-person 1 day workshop, facilitating the advancement of understanding research security risks (informed by multiple national agendas and institutional approaches), broader UK and EU collaboration and models to mitigate current and future research security risks.

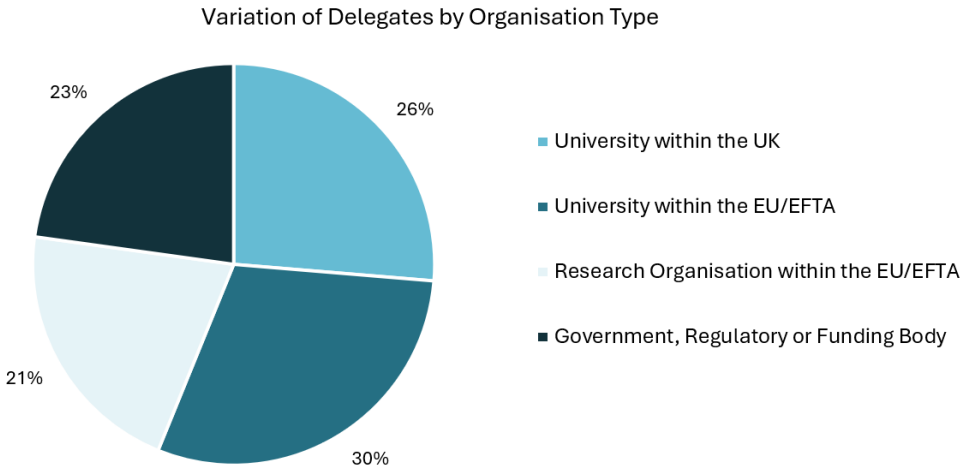
The workshop took place at Fraunhofer-Gesellschaft, Munich on 28th February 2024 and saw attendance from **85+** attendees, across **16** countries.

This report captures the workshop activities and outputs, including the current perceived risks, gaps and challenges associated with secure internationalisation across the UK and EU Higher Education (HE) and Research Organisation (RO) landscape, ways to better support and inform future policy developments through enhanced international collaboration, and exploring the steps needed to enable a step change across the agenda of secure internationalisation.

Workshop Design & Reach

To maximise attendance the workshop was integrated with the EECARO Annual Conference as an additional day to the existing agenda, leveraging momentum and audience of the conference, which was already expected to convene a number of organisations across the EU.

The workshop drew delegates from a diverse range of organisations across the UK, EU and EFTA and relatively equal attendance across Universities, Research Organisations and Government, Regulatory and Funding Bodies:



Composition of workshop groups was considered prior to the event to ensure a balanced representation of organisation type across a spectrum of nationalities to promote diversity of perspectives, foster cross-cultural understanding and facilitate the exchange of unique experiences, leading to a more comprehensive and inclusive set of recommendations.

Throughout the course of the day the Chatham House rule was implemented to allow anonymisation and the freedom for delegates to express varied viewpoints, encouraging openness and candour whilst protecting the privacy and reputation of individuals and institutions.

Each workshop group consisted of 14-15 delegates, with 2 facilitators allocated per group. One facilitator being responsible for guiding and managing the group discussions; the other responsible for recording key outputs from the dialogue.

Sessions were purposefully designed with broad and open-ended questions to allow delegates to authentically share their unique perspectives, insights and lessons learned

without being constrained by narrow parameters. This approach helped foster a more organic exchange of ideas, encouraging a wide-ranging discourse and ultimately enriching the collective understanding and dialogue at an individual, institutional, national and international level.

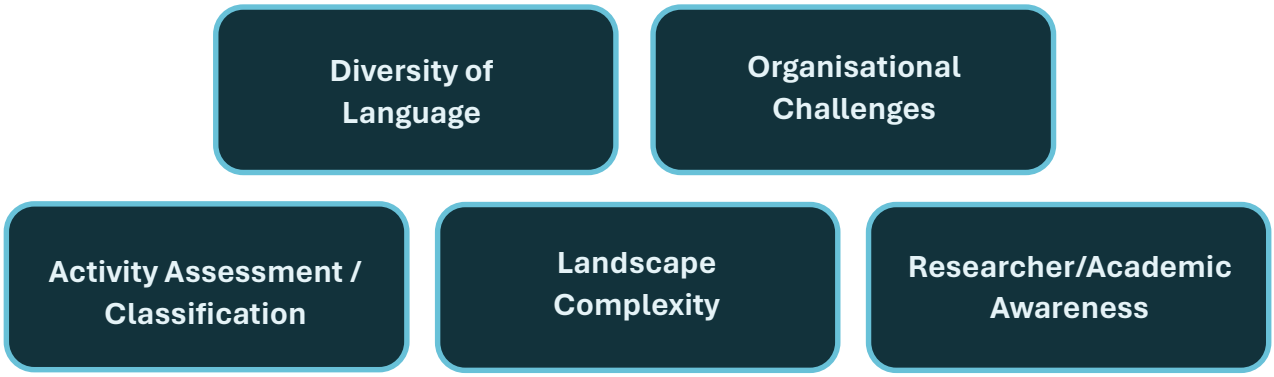
The workshop was split into three key sessions:

- What are the current challenges to ensuring research security and what institutional and national/international resources and tools do we currently use to manage those?
- How can the HE & RO community collaborate with national and international policymakers to support and inform current and future policy developments in this space?
- What is needed to support a step change in this agenda exploring funding, networks, tools and resource needed to enable an effective impact?

The following word cloud highlights the diversity of roles and seniority in attendance, reflecting the growth of engagement in the topic which is now impacting multiple facets of an organisation. It also highlights the variations of where research security responsibility resides within an organisations structure:

What are the current challenges to ensuring research security and what institutional and national/international resources and tools do we currently use to manage those?

Analysis of the consolidated workshop group outputs identified a number of consistently mentioned key themes across the challenges being faced. In some cases, there is evident overlap, however the consistency of occurrence across multiple groups highlights the importance of outlining these areas in their own right:



Diversity of Language

One of the initial challenges outlined was the variety of terminology being used across the international landscape, when in essence referring to the same topic. In the UK this may reflect terms such as 'Trusted Research', or 'Research Security', comparatively referred to by some EU member states as 'Knowledge Security', as well as other uses in the form of 'Secure Internationalisation', 'Research Integrity' or 'Economic Security'. Diversity of language can create a barrier when trying to increase engagement and understanding – if an individual is less familiar with a particular phrasing, they may doubt their knowledge and understanding and in turn this impacts their decision to engage, making it challenging to access and integrate existing knowledge on the subject on an international scale.

One view expressed that the phrasing of 'Trusted Research' appears positive in contrast of the possible negative connotations of 'Security' being restrictive or prohibitive. However, it was highlighted that 'Trusted Research' can on occasion be misinterpreted as questioning the integrity of the research itself or only apply to research and not wider UK HE activities such as teaching or consultancy.

Outside of naming the agenda, challenges were also highlighted in relation to interpreting and applying regulatory language within an academic or research setting, where the diversity of roles now responsible for this topic at an institutional level, may not fall within a legal background – or even those with such expertise, still facing difficulty. Context and impact of the language being used within HE and RO environments, seniority, role and subject matter expertise of recipient has an evidenced impact on its effectiveness.

Organisational Challenges

Challenges faced at an organisational level appeared consistent across the workshop groups. Acknowledging the broadly compartmentalised nature of HE organisations and the diversity of institution size, internal structure, risk appetite and resource there remain commonalities of challenges faced:

- Financial constraints relating to resource, and the growing volume/burden of due diligence requirements outweighing both the existing resource capabilities and capacity within an organisation.
- The impact resource constraints have on the ability to monitor and manage projects once they're 'in-flight'.
- As the regulatory agenda evolves and compliance tasks increase, these additional responsibilities tend to be absorbed by a small handful of individuals – in some organisations this could be a single individual – which in turn creates a Single Point of Failure (SPoF) risk in the event of staff leaving the organisation.
- Sector resilience and staff turnover/retention is a challenge given points above and comparatively higher paid roles within industry. The absence of a professional qualification and development pathway for those delivering this responsibility to mitigate staff turnover or retention issues, is also a concern.
- The cumulative impact of training and responsibility fatigue across target HE and RO audiences, and the broader contextual messaging and engagement with technicians, students, professional services and institutional executive leadership teams.
- With complex HE and RO structures it is often a complicated, time-consuming and resource intensive journey to implement effective and sustainable change even with executive leadership support.
- Access to an accurate and comprehensive list of research staff within an organisation.
- The design of freely accessible sector wide resource and tools reflecting the diversity of institutional application whilst being proportionate and agile. See the HEECA UK National Export Training as a case study in this space.

Activity Assessment/Classification

The prevalent view in the context of export classification is that with Universities and ROs often at the forefront of research and technology, they are encountering significant difficulties identifying sensitive technologies and whether such technologies are considered to be controlled under existing lists or via end use concerns.

It is also felt that the classification of dual-use is persistently challenging, and in some circumstances existing regulations appear to be tailored to suit an industry or traditionally physical regime of controls, opposed to being contextualised for academia or a research-organisation environment and intangible and emerging technologies. This also appeared to reflect a small number of experiences highlighted with licensing

authorities, appearing to lack knowledge of appropriate classification in the context of the HE/RO sector.

Landscape Complexity

One of the key challenges highlighted throughout the session across all groups centred around the complexity of defining, visualising and communicating an understanding of the secure internationalisation landscape. The overarching research security agenda is considered overwhelming and the interplay between institutional autonomy, risk appetite, recommended due diligence and legislation is something institutions are still grappling with. With increasing unilateral national legislative regimes being implemented given the ineffectiveness of international treaties and the need for wider powers to address diverse threat vectors, the national and international landscape continues to become increasingly complex.

Experiences demonstrate that individuals across universities, research organisations, government departments, regulatory and funding bodies are willing to share personal lessons and practices, however there is an absence of a formal structure to enable this and it currently relies on informal networks of collaboration. In some cases, organisations are left deciding which regulations to comply with, because it may not be possible to comply with all. This also poses challenges on the regulatory side, where organisations seek regulator interpretation of something which may not have any legal precedent.

Across some EU member states, the view is that some governments are not yet fully involved in the topic and some are reluctant to engage by way of a national regime due to the topic appearing 'too big to achieve.' This uneven development of EU member states interacting with the agenda may indirectly create an unlevel playing field.

Researcher/Academic Awareness

A lack of awareness of the agenda at an academic/researcher level can pose its own set of challenges and engaging with this community on the topic of research security can be a considerable difficulty.

Collective experiences demonstrate that alongside existing sizeable organisational research policies and ongoing training saturation, often security guidance and information is difficult to embed and is not being considered until it directly applies to an individual or project, by which point, it can run the risk of being too late to establish appropriate due diligence or risk mitigation processes.

Some of the common misconceptions outlined include the belief of low Technology Readiness Levels (TRLs) not being subject to research security risks by default, or if something is non-military related, it is not applicable to the topic.

Among the tools and resources currently in use are...

- Australian Strategic Policy Institute (ASPI) Tracker
- Watchlist screening
- US Dept of Defence Research Security – Foreign Research Institutions of Concern List
- EU Combined Nomenclature tool
- EU Sanctions Map
- Canada - Sensitive Technology Research and Affiliations of Concern (STRAC)
- Federal Office for Economic Affairs and Export Control (BAFA) Manual
- UK - National Protective Security Authority 'Trusted Research' Campaign
- EU Tools for Innovation Monitoring (TIM) Dual-Use Web Platform
- Open access and paywall information sources

Please refer to the summative content of workshop outputs found within the Appendices, for a full view of participant comments.

How can the HE & RO community collaborate with national and international policymakers to support and inform current and future policy developments in this space?

Before exploring how to better collaborate with policymakers (and each other), we first considered existing architectures of collaboration.

The following non-exhaustive list of positive examples were highlighted:

- Higher Education Export Control Association (HEECA)
- European Export Control Association (EECARO)
- Universities of Netherlands (UNL), representing 14 Dutch universities – sector led working group focusing on the topic of research security
- UK Research Collaboration Advice team (RCAT) engaged with UK universities
- Ministry of Education (Denmark) organisation of workshops to universities and technical institutions
- National Austrian research security workshops held
- Netherlands public government point of contact for engaging on Knowledge Security
- Germany Federal Working Group on Export Control in Academia

This later developed into the following suggestions when discussing enhancement of collaboration:

- EECARO representatives for every EU member state – all networks could feed into EECARO at the EU level
- More funding bodies taking part in collaborative workshops and training to enhance their understanding and contribute to sector engagement
- Continuance of HEECA utilising the secretariat and leading collaboration with international partners on behalf of the UK sector, whilst offering additional sub-groups to discuss specific areas
- More working groups with funding bodies in attendance, including more representation at an EU level (not just national level, for member states with lower engagement in the agenda)
- Exploring the possibility of a G7 Security and Integrity of the Global Research Ecosystem (SIGRE) Working Group 2.0
- More policymakers and government/intelligence could embed in Academia and vice versa – in France, there are examples of university secondments into intelligence
- Increasing the number of technical experts involved in working groups implementing the guidelines would be a benefit, where research involvement is currently lacking
- Utilising HEECA and EECARO networks when raising concerns with authorities - priority items can be formed into a proposal on behalf of a larger scale community demonstrating a wider range of inputs and viewpoints consulted
- Exploring engagement with international initiatives like the Erlangen Initiative[1]
- More tangible examples like the 'Norwegian case' in the sector to present real life scenarios with relatable factors to help engage the academic/researcher community
- When large-scale calls are available i.e. European Defence Fund (EDF) Programme 2024 or via UK Research & Innovation (UKRI), workshops should be available alongside, discussing need for export licences, security clearances etc.
- Exploring engagement groups such as the European Association of Research Managers and Administrators (EARMA), The Guild, and Science Europe Working Group

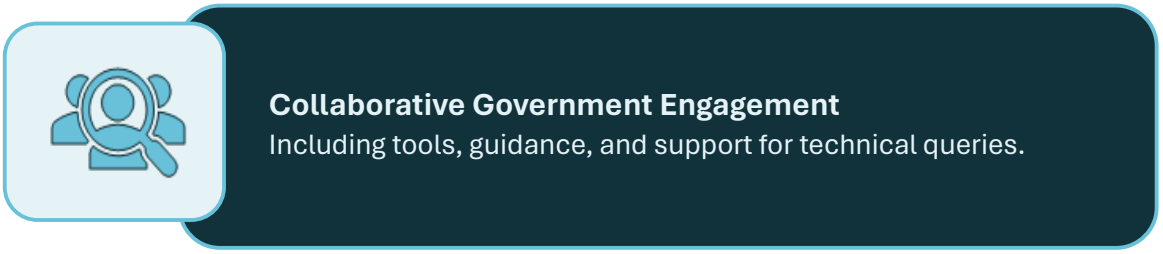
[1]The Erlangen Initiative is an informal outreach process initiated by the German Federal Foreign Office to strengthen implementation of United Nations Resolution 1540 of 2004. The initiative is supported in close cooperation by the United Nations Office for Disarmament (UNODA), the Federal Office for Economic Affairs and Export Control (BAFA), and Fraunhofer-Gesellschaft.

What is needed to support a step-change in this agenda exploring funding, networks, tools and resources needed to enable an effective change?

In order to enable an effective impact, the following key areas highlight the core focusses required for 2024/25 activities:

HEECA and ECCARO are unfunded Associations with outputs (workshops, conferences, guidance materials etc.) delivered by the voluntary in-kind contributions of its membership and Secretariat. This presents a logistical and capacity challenge impacting the scale and immediacy of response to clearly articulated sector needs. Without UK FCDO SIN support the secure internationalisation workshop could not have taken place and still relied heavily on direct and indirect support from HEECA and ECCARO members.

Future funding is critical to empower and enable the HE and RO sector in responding to the challenges of the secure internationalisation agenda. Appropriate funding could support a proactive outreach programme, research to better understand and provide solutions to the barriers of underrepresented member state participation and support wider collaboration with the US, Australia, Canada and Japan who have all expressed a desire and willingness to collaborate on future initiatives.



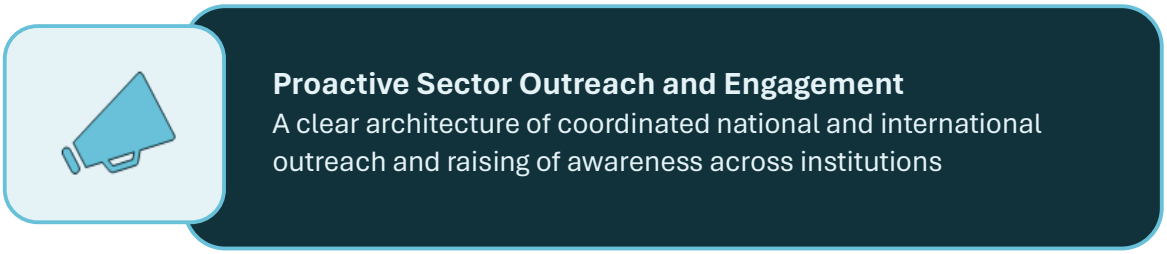
Proactive national government collaboration with their respective HE & RO sectors alongside the appropriate vehicles facilitating this are considered critical to enabling a step change.

There is a diversity of national approach in this regard and whilst many delegates highlighted both the positives and challenges associated with those that currently exist, the majority spoke positively about the intent and ambition behind them.

Mapping of national and international networks and identifying points of contact within governments of each EU member state and sector bodies to direct queries to the right team or department, as well as ensuring national authorities of EU member states effectively communicate with each other on the subject topic to influence and promote consistency at an EU-level. This may also take form in the European Commission providing more guidance, to ensure parity of understanding.

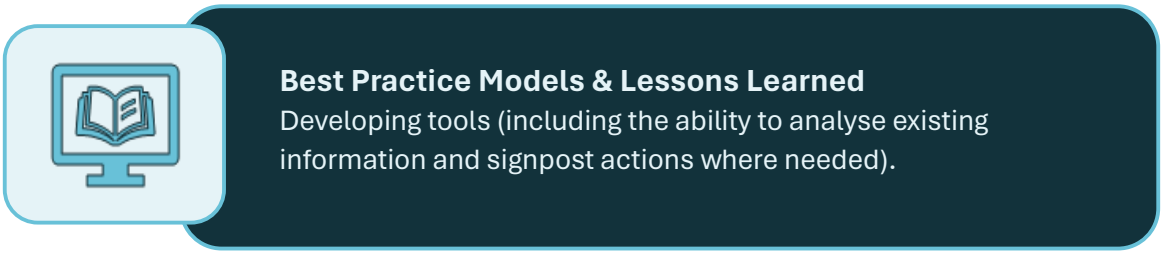
Internationally, there is also a call to action on national models (such as RCAT, Dutch central contact point and Danish Intelligence Services central contact point) to ensure they are consistent and translatable.

In the UK, this may include further collaborative training with ECJU or continuing to leverage HEECA and HESF as a central point of engagement with policymakers, on behalf of the wider sector.



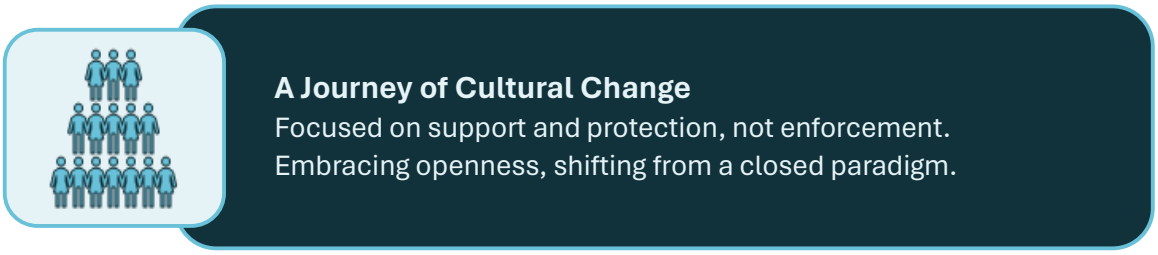
This could include a collection of academic facing workshops that institutions can send key researchers to, helping generate engagement and buy-in at an organisational level, as well as utilising national programmes and campaigns where language is less well defined.

A secure and interactive platform or forum is also needed for communication, to share more information between institutions.



Examples of good practice shared at a national and international level help to advance the collective international landscape, allowing countries less-advanced in the topic to leverage existing experiences, success and lessons learned.

Areas such as developing or using the same screening tool (i.e. on national level so that all universities utilising the same tool) or having a form of scoring mechanism in relation to engagement and risk instead of 'blacklists', allowing more transparency (i.e. a number of contributing factors in this individual case take this over the 'no go' line). Accounting for institutional autonomy remains key and any tools should not appear to make a decision on an institutions behalf rather provide objective information to help inform a decision making process.



Increasing informal conversations with policymakers and embracing a culture of being able to openly discuss issues and experiences, and if something goes wrong, the ability to demonstrate improvement and mitigation without legal repercussions.

The sector and government need to move from a reactive position to a strategic collaborative model which enables the necessary cultural change and provides the roadmap of where we want to be across the short, medium and long term.

Conclusion & Next Steps

Whilst the rich discussions and varied perspectives shared throughout the workshop have illustrated the complexity of the secure internationalisation challenges being faced, they have also demonstrated the immense potential for progress when diverse stakeholders unite around a common vision and there is a clear desire for future workshops to be delivered in a comparative manner, focusing on specific topics.

There is significant commonality in the challenges faced institutionally, nationally and internationally and we are seeing a wider spectrum of roles now conscious of and engaging with research security and the associated collaborative activities.

There is strength in a collaborative response, however in order to tackle these challenges, the HE and RO sector must move from a reactive to a strategic approach – our resilience and effectiveness in meeting this will only be as strong as our weakest link across a national and international stage. Exemplifying this, delegates spoke of projects declined at an institutional level due to security concerns, only for the same project to then be seen through their networks at other institutions.

Challenges notwithstanding there are clear short term and immediate opportunities to deliver tangible changes that would support the sector in this space. The sector is proactively engaging where it can in collaborating to deliver such change but is impacted by limited financial support and constrained resource.

Future Roadmap

EECARO and HEECA will continue to collaborate going forward and subject to future funding, propose a short-term programme of activity (below) which will:

- Facilitate continued sector collaboration and address the delegate requested future workshop topics; and
- Inform development of a coherent future strategy report output to facilitate the substantive step change needed to address this topic.

In parallel, the programme would be underpinned by proactive outreach to underrepresented EU member states/institutions and more widely the convening of regional, national and international (Australia, Canada, Japan and US) bodies active in this space.

Delegate-recommended topics for future events:

- National employment law in the context of end use/security concerns
- Managing publications and unfunded/informal collaborations
- Processes and procedures from recruitment through to knowledge transfer
- The four pillars of Economic Security
- Pros & Cons of an International (Legal) Base for Knowledge Security
- Visiting posts (Professors, Secondments, PDRA's etc.)
- Research Security & the International Approaches to Screening
- Managing Research Security: Cross-Jurisdictional Collaborators
- Dual-use Assessments & Emerging Technologies

Workshop Delivery Lessons Learned

1. Diversity of delegate stakeholder composition has a demonstrably positive impact on the content of group discussion and diversity of perspective. Ensuring future activity can retain that same engagement profile whilst still reflecting value to attendees is key.

2. Having initially envisaged engagement to reach a maximum range of 30-40 attendees, 85+ delegates presented a logistical delivery challenge, as well as cost impact. This led us to minimise promotion of the event to ensure we did not exceed capacity of the hosting venue. Integrating flexibility of venue size, or clearly prescribing delegate numbers will help mitigate the same occurrence for future events.

3. Proactive outreach is required to engage underrepresented EU member states and inclusion of international partners (US, Canada, Australia and Japan) who expressed interest in attending and supporting the event. Leveraging existing and other complimentary network relationships is key to delivering the required participation and engagement expansion.

4. Academic/researcher and technician attendance should be sought at future events as it reflects a historic and ongoing gap of participation when engaging on this topic.

5. Post-workshop engagement with delegates is critical to gauge the reception and impact of an event, as well as informing lessons learned and maintaining the momentum of future network activities. The request for delegate feedback following our event was issued sometime after the general EECARO Annual Conference request for feedback and in the future, consideration will be given to merging these kind of requests to strengthen the volume of delegate response.

The 5-week period in which this report was produced also reflects the limit of this timeframe and we should target 2-3 weeks going forward.

6. Leveraging existing planned events and networks was critical to the immediacy of successful delegate reach, response and workshop engagement.

HEECA The Higher Education Export Control Association

96% of attendees said they would be keen to attend future HEECA & EECARO collaborative events in 2024/25.

Read some of the delegate feedback of the event here:

"Hearing the views of external regulators were very helpful in break-out sessions"

"Getting to know other professionals in the field, understanding shared challenges and learning from successful implementation"

"All topics of discussion and meeting our European colleagues"

"Seeing the network mature into a platform with experienced professionals trying to solve compliance challenges in the field of export control and knowledge security"

"Networking, discussing 'live' matters that are applicable across nations and institutions."

"Discussing similarities of challenges in managing secure research legislation internationally; it is comforting to know the same barriers and lack of clarity features in a widespread way and considering options for combating this collectively."

With support from

UK Science & Innovation Network

EECARO European Export Control Association for Research Organisations

Appendices

A. Summative comments of all five workshop groups – What are the current challenges to ensuring research security and what institutional and national/international resources and tools do we currently use to manage those?

- The complexity of procedures incapsulated by the agenda
- Lack of management knowledge and then awareness at researcher level
- Organisation turnover creates a knowledge gap
- Sometimes academics don't pay attention to information until it applies to them, then it's too late
- There is not currently a widely used method to log research projects at an institutional level, unless they are funded and will navigate through central teams by default
- There are too many initiatives launched by researchers, without awareness by those who need to know
- Classification of dual-use
- There can be negative connotations of 'Security' being restrictive or prohibitive – the UK example of 'Trusted Research' appears more positive
- Sometimes legal wording of regulation is difficult to interpret even in the legal profession. How can researchers be expected to understand
- Proposals can often flow too close to deadlines to incorporate due diligence prior to submission
- In some EU member states, universities will not align to a national regime as it appears too within infancy stage at the national level
- UK use of the term 'Trusted Research' can be misinterpreted as a question of the integrity of the research itself
- In our roles, we are the middle person between regulators and academics – sometimes academics can feel intrusion in the decisions to declare, or that we are going against their self-assessment of whether they are subject to regime or control
- Government departments do not appear to align their own language and terminology consistently
- Low TRLs are not considered to be subject to research security risks in the researcher view
- There is currently no formal sponsorship of a compliance tool in the EU
- 'Dual-use Potential' is difficult terminology for daily compliance measures
- There are existing language barriers between regulators and academics – who interprets this and brings together to identify. Academics will not think they are relevant to regulatory material.
- In the UK, the feeling is that responsibility continues to sit at an institutional level
- Difficulties in identifying sensitive technology in academia and determining whether it's controlled
- Obtaining and assessing the information needed for substantial due diligence can be a challenge
- Understanding the legal concept of technical assistance as set out in EU regulations
- Need for more tools beyond ASPI, knowing where to find resources, and which methods to use

- Challenges in managing reputational risks nationally and internationally
- Considerations from ethical and moral perspectives
- Dual-use regulations are not tailored for research organizations
- Difficulty in having specialized personnel for classifying technologies within every organisation
- Challenges in complying with multiple regulations; seeking regulators' interpretation when there's no legal precedent
- Financial resource constraints
- Challenges in efficient communication without causing alarm
- Regulators appear to focus elsewhere rather than on research organisations, lacking understanding of handling these issues in the appropriate context
- Difficulties in understanding sanctions, exemptions, and allowances
- Limited access to information; suggesting a national-level solution
- Challenges in addressing catch-all issues
- Divergence in catch-all regulations at national levels
- End-use determination
- Knowledge and awareness of researchers
- More requirements means more knowledge requirements and tasks, increasing workload
- The need to determine risk appetite at an organisational level
- Starting with the subject, where to begin?
- Determining Dual-use classification (i.e. of a prototype)
- Cooperation with entities in China (when they are not sanctioned), navigating the grey zones
- The wide range of research of research institutes and universities (in comparison to companies that often focus on only one or a few areas)
- Different countries use different terms/language for similar topics (knowledge security, research security); it’s important to use the same definitions
- Countries are recognising the need to protect emerging tech and regimes are being implemented at a national level, however this is resulting in differing configurations to other allies
- Lack of knowledge of the export control/licensing authorities (in some countries), regarding classification as well as the research/university sector itself
- The culture and context of Academia cannot keep up with the everchanging geopolitical situation
- Export control is legally framed but trusted research doesn’t fit to export control rules - everything is becoming more complex
- Globalisation is impacting he Academia now must investigate those collaboration. Very difficult for academic institutions to understand. We are playing catch up with the globalization and we need culture change
- There is less belief in export control now and awareness raising has to be seen in the context of the international treaties
- Tools like the ASPI tracker are not legally binding and are no longer kept up to date
- There is currently more focus on export controls but the Agenda is wider
- Funding agencies are still not focusing on research security topics
- Not all Governments appear to be fully involved in the topic yet, and awareness in funding agencies is at a similar level to universities
- Internally it can be difficult to find the right person/department in charge of this topic, due to the diverse areas of an organisation that appear to be responsible

- It is unclear what the consequences for research security breaches are, unlike the case for the export compliance
- The number of different legislations and policies applicable to research organisations and universities in this context are not very well coordinated – sometimes we have to decide which regulations to comply with, because we may not be able to comply with all
- Research security is soft law and a moving target, and you need to find a way to address it without breaching other laws
- The people at the ministry don't know how to deal with our sector, they are used to industry, they don't know what is going on at universities, it takes time to educate them
- There is a lack of resources at both sides
- A lot of the risk is outsourced to us as organisations by Government
- There aren't any strict rules to apply, but they still come and audit us afterwards
- In Denmark it has been developed together, but the ministry of education is not the most important voice, foreign affairs or business is – we just have to follow, internal power struggles are sometimes reflected down to universities
- There are a lot of different interests, matched with a lot of unclarity of what research security is and how it interacts with academic freedom
- Universities are the ones that know about the technology – we need to find a common interest, and a way to work together
- Difference between countries and roles that stakeholders take
- Authorities have so many other things to do and have no resources, and high fluctuation of people
- Regulators are required to decide on something they don't understand
- Procedures at customs are focused on tangible goods
- Knowledge is even different from intangibles
- Researchers say "we are not doing anything military"
- Embedding security mindedness within the academic community is not easy, researchers should not be focusing on security, they should be focusing on their work
- Researchers cannot be the expert in everything
- It feels like there is not always enough room for ethical compliance
- Funding models should be different so that researchers have more room not to have to follow the money – they are free to take the ethical route
- Difficulty to continue to support projects as they develop, they may take other directions, new partners may come in, situation might change. There is no capacity to keep monitoring
- Risk analysis and how that is understood – how are lists of technologies translated into university practice – how to find the risks and focus on those
- If government allows you to make mistakes if you try to do your best, and if something goes wrong you try do to better, then you will speak up – if this does not happen, you will not speak up
- Very slow to progress to have a law, and when you get it, it is already outdated
- Some member states have clear distinctions on restrictions on the type of military funding they can apply for.

B. Summative comments of all five workshop groups – How can the HE & RO community collaborate with national and international policymakers to support and inform current and future policy developments in this space?

- More collaborative training with ECJU
- Leading EU member states to initiate at National level so that other EU member states can follow-suit
- National authorities of EU member states need to effectively communicate with each other on the subject topic to influence and promote consistency at an EU-level
- Having points of contact within governments of each member state is important and would mitigate messages or questions not always reaching the right team or department. For example, when navigating a desired change through the system (especially at an EU-level)
- EECARO representatives for every EU member state would be a good idea
- Working on making EECARO more known to Governments, but at the same time clear that there is still a need for Governments to communicate with Universities on a National level
- More working groups with funding bodies in attendance
- Use the same screening tool (i.e. on national level all universities could use the same screening tool)
- Exploring possibility of development an EC classification tool together?
- More focus on the funding of research collaborations from a research security perspective
- Clear need of common position in the EU and to bring that position to paper
- More HEECA and EECARO joint events – utilising existing partnership of associations on behalf of members
- Having a form of scoring mechanism in relation to engagement and risk instead of 'blacklists' allows more transparency (i.e. a number of contributing factors in this individual case take this over the 'no go' line)
- Increasing informal conversations with policy makers
- Action on national models (RCAT, Dutch contact point, Danish central contact point at intelligence services) to ensure they are consistent and translatable
- More invaluable UK and EU Collaborative events to continue understanding of positioning and interpretation of national legislation across countries
- Consolidation with EU list in relation to key word searches - (i.e. graphene and graphite) to ensure everything is flagged correctly
- Use a common training programme (with respect to awareness)
- Clear need of the framework for research security and then work on the exemptions
- Utilising HEECA and EECARO communities when raising issues with authorities – high priority items could be formed into a proposal on behalf of a larger scale community, demonstrating that a wider range of inputs and viewpoints were consulted before raising – would this have an increase on the effectiveness of outcome?

C. Summative comments of all five workshop groups – What is needed to support a step-change in this agenda exploring funding, networks, tools and resources needed to enable an effective change?

- Collaborative training with ECJU
- Funding bodies taking part in workshops and training
- Need more invaluable UK and EU collaborative events to understand positioning, interpretation
- Engaging with Science Europe working group
- UN and Germany initiative
- Possible SIGRE 2.0
- Possibility of a new tool to provide regulations to be aware of per country – it would say something like "here are the relevant links please read"
- Something similar to the Nagoya website, "here is what to consider"
- Perhaps a tool additional to EU sanctions map
- Actions on EECARO to improve on data collection
- Academic and researcher faced workshops
- Economic security 4 areas workshops internationally
- A new tool to input: this is what I want to export, this is where, this is the TRL, output to be yes do this, no unlikely, or seek advice
- Could have better words to match the EU list for being able to check
- More examples like the Norwegian case
- Embrace openness
- Share documents such as questionnaires and forms
- Access high-quality risk information
- Advocate for public funding and resources
- Foster collaboration among organizations
- Engage with institutions
- Engage in international initiatives like the Erlangen process and SIGRE G7 virtual meetings
- Use a common training programme (with respect to awareness)
- Use the same screening tool
- Is it possible to develop a EC classification tool together?
- We need continued interaction
- With respect to EECARO: to develop further, we need funding (preferably from governments/EU). This would allow creating i.e. training materials, tools, guidance documents, white papers, internet page, outreach, etc.
- Funding for training, future events (HEECA and EECARO - networking is key), coordination of input to white papers, additional support, websites updates and longer term the development of tools
- Awareness Raising – 'connecting the dots' internally to ensure messaging gets to the right places across institutions. Increase general awareness, including 'unconscious awareness'.
- Developing tools
- Ask for more from Governments

- Culture Change
- More focus on the funding of research collaborations from the research security perspective
- More national guidelines and outreach events
- Advisory desk from the government (e.g., in UK: very useful service, give you an insight on what is critical).
- Clear need of the framework for research security and then work on the exemptions
- Need for a common position in the EU and to bring that position on paper
- More conferences like this every year where the government will be engaged
- Approach The Guild
- Talk to the European Commission – if we as universities are going to work together to create a level playing field, they need to fund us - Together with HEECA, AUECO and Australian counterparts
- Collect information on e.g. issues with open access in Horizon and feedback through EECARO
- More interactive platform is needed – need to share more information
- An event like this every year
- More concrete workshops – e.g. EDF projects, needs export licenses, needs security clearances etc., this should be better dealt with in the Commission
- Aim of meetings more concrete, drafting a proposal
- Use platform for awareness raising? Do we develop a platform for communication?
- The platform environment needs to be secure
- Feedback on the results of particular discussions that took place between 2 or 3 people, ideally indexed
- Would communication within our community have an effect on the communication with authorities? Identify issues where we can come together, or that need more attention, or that can be formed into a proposal towards authorities, also recognizing that we will not always see things the same way, this will only grow when we get more involved in defence research