GSF-01 Multilateral Dialogue
on Principles and Values in International Research & Innovation Cooperation
–
Workshop on Research Security
Thursday, 7 December 2023 13:00-16:00 (CET) VIA WEBEX

CONTENT

Concept Note

This workshop is co-designed by the United States, Finland, Belgium, the Netherlands, the International Science Council, CESAER and the European Commission.

Please find below the initial concept note, framing the workshop context, objectives and discussion topics. This concept note was distributed to the registered participants in advance of the event.

Background Information

In July 2022, the European Commission (EC) initiated a Multilateral Dialogue (MLD) on Principles and Values for Research and Innovation (R&I) with the objective of fostering an open discussion of the principles and values that form the foundation of international collaboration on R&I. The seventh online workshop supporting the dialogue was focused on 'research security' and took place on December 7th, 2023. It was co-organised and co-designed by the EC together with the United States, Finland, Belgium, the Netherlands, the International Science Council, and CESAER. It convened around 135 participants from 36 countries, and from international organisations such as the OECD and UNESCO, as well as from several European stakeholder organisations. The list of participating countries and stakeholder organisations can be found in the Annex (page 23).

Against this background, the focus of the workshop will be on undesirable end-use of research results as this is a defining feature of the research security challenge that all aspects of the research community are facing. The undesirable nature of the end-use covers/covert military applications, affecting national security, as well as unethical end-use, notably in ways that are contrary to universal human rights. Addressing undesirable outcomes involves attention to all phases of research process, from development and funding agency review to the forging of responsible collaborations and further through the carrying out of the project and the dissemination of results to safeguard the research from undue foreign influence. It also requires effort by researchers, teachers, and students themselves, by the governments, by large research teams, and by the international community to safeguard research while maintaining academic and scientific freedom. Through these efforts the goal is to enable better and more responsible international cooperation.

The aim of the workshop is not to reach consensus or to bridge or accommodate differences. Instead, the workshop intends to provide a platform for an open dialogue on distinctions and commonalities in the conceptualisation and application of research security in the different national contexts.

Due to its close links to national security and systemic vulnerabilities, the topic is particularly sensitive. We therefore ask participants to be prudent with what they share themselves and treat what is shared by others confidentially (Chatham House rule applies). The virtual setting of this three-hour workshop allows all participants to come together irrespective of their geographical location.

After an introduction on the objectives of the workshop, the discussion will take place in parallel breakout sessions on three different aspects of research security: (1) conceptualisation of research security, (2) application of research security measures/policies by national governments and national funding agencies and (3) the role of research institutions in managing and mitigating risks.

1. **Conceptualisation of research security: How can we understand research security among international partners?** This topic includes a discussion of what are the key elements of

research security in each country/organisation. Questions to consider in addressing this topic include:

- What are the key elements of research security in your country?
- How are potentially undesirable end uses of research identified in your country/organisation?
- Are there areas where the benefits of international collaboration outweigh research security concerns?

2. **Application of research security measures/policies by national governments and national funding agencies** determining the processes and rules needed across all stages of the review and funding processes, while maintaining academic and scientific freedom and respecting institutional autonomy of the research institutions. This topic includes a discussion of specific safeguards and security measures related both to basic and applied research. Questions to consider in addressing this topic include:

   - In your country/organisation, how do you maintain the essential principles of openness and transparency while also safeguarding research?
   - How is your country/organisation considering actions to safeguard against potentially harmful end uses of research?
   - How does your country/organisation differentiate between stages of research (from basic to applied) when applying safeguards to research?
   - What training and outreach opportunities are provided in your country to the research community to build a culture of research security and by whom?

3. **The role of research institutions in managing and mitigating risks:** Managing and mitigating risk while emphasising benefits – highlighting existing and missing tools such as decision-making rubrics and trusted-partner approaches to identifying and managing risk and maximising benefit. This topic includes a discussion of tools that research institutions can use to make decisions on research practice and international collaboration to provide benefit given research security concerns in scientific research. Questions to consider in addressing this topic include:

   - How do you/your research institutions make sound decisions on research practice and collaboration, given research security concerns?
   - What are the channels for dialogue between institutions and the authorities about the implementation of policies and guidelines?
   - How do you manage uncertainty of the potential end-use of research?
   - Are there ways to think about trusted partnerships and be more proactive?

Further reading and background material:
(provided by the organising team and complemented by the participants during the workshop)

EU

- Toolkit on R&I foreign interference, DG RTD (2022): Tackling R&I foreign interference - Publications Office of the EU (europa.eu).
- Joint Communication to The European Parliament, The European Council and The Council on "European Economic Security Strategy" (2023).
- Safeguarding Science Tools, EU: https://www.safeguarding-science.eu/tools/operate/
- Council Recommendation on Research security: ec_rtd_council-recommendation-research-security.pdf (europa.eu)

OECD

- OECD policy paper on "Integrity and security in the global research ecosystem" (2022): Integrity and security in the global research ecosystem | EN | OECD.
- National initiatives from the OECD platform: https://stip.oecd.org/stip/research-security-portal.

G7

- G7 Common Values and Principles on Research Security and Research Integrity (2022).

United States

- JASON Report on Fundamental Research Security (2019).
- National Security Presidential Memorandum-33 Implementation Guidance (2022).
- U.S National Institute of Standards and Technology (NIST) "Safeguarding International Science Research Security Framework": https://nvlpubs.nist.gov/nistpubs/ir/2023/NIST.IR.8484.pdf.

Norway:

- Guidelines and Tools for Responsible International Knowledge Cooperation, Norway: https://hkdir.no/en/guidelines-and-tools-for-responsible-international-knowledge-cooperation.

Ireland:

- Principles of Good Practice in Research in Irish Higher Education Institutions https://hea.ie/assets/uploads/2022/12/High-res-links-v3-HEA-Principles-of-Good-Practice-in-Research-within-Irish-Higher-Education-Institutions.pdf

CESAER:

Keeping Science Open, White Paperhttp://doi.org/10.5281/zenodo.8355324

Sweden

- Swedish Technology self-assessment tool: https://www.kometinfo.se/in-english/responsibletech/
- Portal on research security: https://science.gc.ca/site/science/en/safeguarding-your-research
- DFG recommendations "Dealing with risks in international cooperation": https://www.dfg.de/download/pdf/dfg_im_profil/geschaeftsstelle/publikationen/stellungnahmen_papiere/2023/risiken_int_kooperationen_en.pdf
- Checklist Global Responsible: https://suhf.se/arbetsgrupper/expertgruppen-for-internationaliseringsfragor/

France

- French Senate, Rapport: Vade-mecum à l'usage des scientifiques et des experts, 2015: https://www.documentation-administrative.gouv.fr/adm-01859867/document
- French Senate, Rapport GATTOLIN « Influences étatiques extra-européennes dans le monde universitaire et académique français et leurs incidences », 2021 & « Extra-European state influence on French universities and academia and its impact »

Finland

- Finish considerations related to good scientific practices, security and competitiveness are relevant. https://julkaisut.valtioneuvosto.fi/handle/10024/163963

- National Security Guidelines for Research Partnerships, which are country and company agnostic: https://science.gc.ca/site/science/en/safeguarding-your-research/guidelines-and-tools-implement-research-security/national-security-guidelines-research-partnerships

Canada

- Canada risk assessment process under this framework, which only applies for a very small number of funding opportunities: https://science.gc.ca/site/science/en/safeguarding-your-research/guidelines-and-tools-implement-research-security/risk-assessment-review-process
- Guidelines, tools, and resources (including courses, risk assessment forms, etc): https://science.gc.ca/site/science/en/safeguarding-your-research

United Kingdom

- UK trusted research guidance for academia: https://www.npsa.gov.uk/trusted-research-academia
- UK RCAT Update report (2023): https://assets.publishing.service.gov.uk/media/654a2f1be2e16a000d42aae4/research_collaboration_advice_team_update_report.pdf
- UK National Security and Investment Act: guidance for the higher education and research-intensive sectors: https://www.gov.uk/government/publications/national-security-and-investment-act-guidance-for-the-higher-education-and-research-intensive-sectors/national-security-and-investment-act-guidance-for-the-higher-education-and-research-intensive-sectors.
- Complex Collaborations, Efficiency, Equity, Quality, and Security: https://arma.ac.uk/wp-content/uploads/2023/03/Trusted-Report_Booklet_v7.pdf

Netherlands

- Dutch national contact point for knowledge security: https://english.loketkennisveiligheid.nl/knowledge-security.
- Dutch national guidelines: https://english.loketkennisveiligheid.nl/knowledge-security

Switzerland

- Guide Towards Responsible International Collaborations, Swiss Universities: https://www.swissuniversities.ch/fileadmin/swissuniversities/Dokumente/Internationales/Guide_Towards_responsible_international_collaborations2.pdf
- Swedish university checklist: https://suhf.se/arbetsgrupper/expertgruppen-for-internationaliseringsfragor/
- Web-based self-assessment tool for technology development developed by a previous Swedish government committee for technological innovation and ethics: https://www.kometinfo.se/in-english/responsibletech/

The Guild (European Research-Intensive Universities)

- The Guild's Statement on Responsible Internationalisation: https://www.the-guild.eu/publications/statements/the-risks-of-international-collaboration-must-be-balanced-with-the-risks-of-non-collaboration.html

Agenda

13:00 – 13:05	**Opening and welcome** • Maria Cristina Russo, Director for the Global Approach and International Cooperation in R&I, European Commission
13:05 – 13:10	**Introduction to the workshop** • Martin Penny, Head of Unit, International Cooperation in R&I, European Commission
13:10 – 13:25	**Policy Context of the Workshop:** • Dr Rebecca Keiser, Chief of Research Strategy and Policy, National Science Foundation, USA
13:25 – 14:20	**First breakout sessions** Participants will be asked to give their preference order for the breakout sessions when registering. The breakout sessions are: 1. Conceptualisation of research security 2. Application of research security measures/policies by national governments and national funding agencies 3. The role of research in managing and mitigating risks
14:20 – 14:30	**Coffee break and switch to second breakout session (new Webex link)**
14:30 – 15:25	**Second breakout session** Participants will join new breakout sessions on the second of the topics they have chosen.
15:25 – 15:55	**Plenary report by rapporteurs of the break-out sessions**
15:55 – 16:00	**Closing statement** • Machteld Haaksman – Manager on Knowledge Security in the Ministry of Education, Culture and Science, the Netherlands

The above topics were discussed in three groups of parallel breakout sessions (11 in total) during two rounds. Delegates attended two breakout sessions, giving them the opportunity to discuss two different topics out of the three. Due to its close links to national security and systemic vulnerabilities, the topic was particularly sensitive. In accordance, the breakout sessions followed the Chatham House Rules[1].

[1] Chatham House Rule: https://www.chathamhouse.org/about-us/chatham-house-rule

Summary Report

The Workshop on "Research Security" took place on the 7th December 2023 and was the seventh of a series of workshops as part of the European Commission's Multilateral Dialogue (MLD) on Principles and Values in International Research & Innovation (R&I) Cooperation. The event was co-organised by the European Commission together with the United States, Finland, Belgium, the Netherlands, the International Science Council, and CESAER. It attracted around 135 participants from 36 countries, and from international organisations such as the International Science Council, the OECD, and UNESCO, as well as from several European stakeholder organisations.

Research security is a topic that is receiving increasing attention from public authorities as well as the research community due to the evolving and challenging geopolitical context. It is a concept where there are no commonly agreed definitions yet. Nonetheless, some common understanding is that research security refers to safeguarding research and innovation from interference by or on behalf of foreign state-actors that affects national security and/or are contrary to one's values and principles.

Against this background, the objective of the workshop was to provide a platform for an open dialogue on distinctions and commonalities in the conceptualisation and application of research security in the different national contexts across the globe. After the introduction by Martin Penny, Head of Unit, International Cooperation in DG R&I of the European Commission, Dr Rebecca Keiser, Chief of Research Strategy and Policy at the National Science Foundation, USA, set the policy context of the workshop.

Martin Penny, Head of Unit, International Cooperation in DG R&I of the European Commission:

- Highlighted the participation of more than 135 people from 36 countries, international organisations, and European stakeholders in this workshop.
- Reinforced the aim of the multilateral dialogue of serving as a platform for an open exchange of practices and experiences in international R&I collaboration.
- Informed that six previous workshops have already taken place and this one is the final one of 2023.
- Mentioned that the previous workshops have proven to be a good way of bringing together all research and innovation actors and the value of the multilateral dialogue.
- Underlined that given the global rise of geopolitical tensions and competition, this workshop's topic brings significant challenges to R&I, and that consequently, this workshop's topic – *research security* – is high on many countries' agendas.
- Concluded by highlighting the need of finding a new balance between openness and collaboration on the one hand and security and safeguarding on the other hand.

Dr Rebecca Keiser, Chief of Research Strategy and Policy at the National Science Foundation, USA:

- Set the scene of the workshop by illustrating the example of the US, who have been dealing with issues related to *research security* for some time now.
- Presented a timeline with the most important milestones of the US case:
    - Beginning in 2017, US science agencies started delivering intelligence briefings to the academic community due to concerns about other countries appropriating fundamental research from the US for questionable uses.

- In 2019, the JASON Report on Fundamental Security[2] which highlighted the issues of misappropriation of fundamental research, undisclosed conflicts of commitments, and end uses of research.
- In 2020, the establishment of US *research security* subcommittee, led by the White House's Office of Science and Technology Policy, together with other departments such as Health and Energy, with the objective of understanding and developing policies that maintain openness while addressing *research security* issues.
- In 2021, some international efforts such as the establishment of the G7 Security and Integrity in the Global Research Ecosystem Working Group, and the OECD Global Science Forum Work on Research Security and Integrity.
- In 2022, many international efforts were made in trusted research, responsible internationalisation, and research security.
- Highlighted that, 2023 means a step forward in maintaining openness while paying attention to security in research.

- Presented a diagram of *research security* composed by three main values: Rigor & Reproducibility, Responsible Conduct of Research, and Research Ethics.
- Highlighted the need of ensuring that the research system remains both open and secure at all stages of research.
    - In academic and fundamental research by safeguarding researchers' ideas, performing due diligence on research funding sources, assessing potentially harmful end uses, and collaborating internationally on research security.
    - In applied research by safeguarding IP, performing due diligence on sources of venture capital and investment, assessing potential harmful end uses, and vetting international transactions.
- Mentioned that research security is a joint and shared responsibility of all research actors; from funders to researchers as "*research security is as strong as the weakest link*":
    - Funders need to collect appropriate disclosures, assess research proposals for risk, and work to mitigate those risks.
    - Research institutions need to assess if disclosures are complete, oversee the use of research funding by their institutions, make sure that potential international interactions are true collaboration, and promote a research security safety culture.
    - And researchers need to understand the terms of any proposed affiliation or funding sources, communicate with home institutions and funding agencies, promote a research security safety culture.
- Referred to SECURE[3], a US non-governmental entity whose mission is to empower the research community to make security-informed decisions about *research security* concerns, by providing information, developing tools, and providing services to universities, non-profit research institutions, and small and medium-sized businesses (SMEs).
- Referred as well to the Research-on-Research Security Program (RRSP), an NSF funding programme seeking to fund research that will identify and characterise attributes and distinguish research *security* from research *integrity*; improve the understanding of the nature, scale, and scope of research security risks; provide insights into methods for identifying, mitigating, and preventing research security violations; and develop methodologies to assess the potential impact of research security threats on the US economy, national security, and research enterprise.

[2] https://www.nsf.gov/news/special_reports/jasonsecurity/JSR-19-2IFundamentalResearchSecurity_12062019FINAL.pdf
[3] https://new.nsf.gov/research-security

- Finally, mentioned the Research Security Training Modules, developed together with the Departments of Energy, Health, and Defence, and available to download (for international partners as well) through a public platform[4]. These modules cover *what is research security*, disclosure, management and mitigation of risks, and international collaboration.

After the introductory speeches, the participants discussed, in two rounds of parallel breakout sessions, three different aspects of research security: (1) **conceptualisation** of research security, (2) **application** of research security measures/policies by national governments and national funding agencies, and (3) the **role of research institutions** in managing and mitigating risks.

Some general conclusions that referred to the three topics and were highlighted in the discussions, are that:

- Research security is constantly evolving, requiring policies and practices that can adapt quickly to new challenges and situations.
- It's crucial to maintain a balance between the openness necessary for collaborative research and the measures needed to secure research integrity and manage risks.
- A case-by-case approach, considering each project's unique context, coupled with strong collaboration and communication among all stakeholders, is essential for effective research security.
- Educating and equipping researchers with the necessary knowledge and tools is vital for building a proactive culture of research security.
- Harmonising research security standards internationally and providing clear guidance and support to research institutions are key to managing security risks while promoting global scientific collaboration.

Some key outcomes from the breakout sessions are summarized below:

Topic 1: *Conceptualisation of research security*

The discussions was focused on the following questions:

- What are the key elements of research security in your country?
- How are potentially undesirable end uses of research identified in your country/organisation?
- Are there areas where the benefits of international collaboration outweigh research security concerns?

Main points highlighted in the discussions:

- The area of *research security* is a changing and evolving area, therefore the need for a case-by-case approach.
- Key elements of research security range from a culture of research security to knowledge and awareness building, and ethical dilemmas. Countries need to take this into consideration at the national, institutional, and research (project) level.
- The benefits of international collaboration in areas such as climate change still outweigh research security concerns.
- The right for academic freedom should stay at the forefront as a guiding principle; therefore, the focus of research security should be on risk *management* rather than risk *avoidance*.

[4] https://www.nsf.gov/pubs/2022/nsf22576/nsf22576.htm

Topic 2: ***Application of research security measures/policies by national governments and national funding agencies***

Discussion of specific safeguards and security measures related both to basic and applied research and covered the following questions:

- In your country/organisation, how do you maintain the essential principles of openness and transparency while also safeguarding research?
- How is you country/organisation considering actions to safeguard against potentially harmful end uses of research?
- How does your country/organisation differentiate between stages of research (from basic to applied) when applying safeguards to research?
- What training and outreach opportunities are provided in your country to the research community to build a culture of research security and by whom?

Main points highlighted in the discussions:

- *Research security* should be an integral part of the research flow: e.g. understanding who the partners involved are, how research outcomes will be used, and alignment of research communities' interests.
- Actions, tools, and processes include partnership and mitigation strategies that capitalise on the experiences and collaborative engagement between research communities and governing authorities.
- Various countries emphasised the need for a case-by-case approach for research security and for open cooperation as the default stance.
- The dilemma between open science and research security needs a balance between these principles.
- The EU and international levels need to develop policies to harmonise as much as possible the *research security* concept and its implementation through tools and approaches across nations.
- Training and outreach opportunities are needed to educate researchers on best practices, risk identification, and compliance requirements.
- Some countries put more focus on applied research when talking about research security, but attention to research security aspects in basic research is also needed, especially in areas where *research security* is not so obvious.
- The distinction between basic and applied research remains a grey area that emphasises the need for a case-by-case approach on research security.
- A more active role of research funding agencies to identify potential risks is needed.
- Co-creation and using what is already in place in other countries/organisation should be the approach for many countries/organisations that are starting to work and develop policies on *research security*.
- The universities' decision autonomy and academic freedom are guiding principles that should prevail. This requires close collaboration between research institutes and government authorities for research security related issues.

Topic 3: ***The role of research institutions in managing and mitigating risks***

Discussion of tools that research institutions can use to make decisions on research practice and international collaboration to provide benefit given research security concerns in scientific research.

- How do you/your research institutions make sound decisions on research practice and collaboration, given research security concerns?

- What are the channels for dialogue between institutions and the authorities about the implementation of policies and guidelines?
- How do you manage uncertainty of the potential end-use of research?
- Are there ways to think about trusted partnerships and be more proactive?

Main points highlighted in the discussions:

- Some countries are in an early phase regarding *research security* (e.g., Belgium, Switzerland), while others are more advanced in the development of approaches, guidelines, and tools (e.g., The Netherlands).
- The level of development regarding *research security* depends on the level of the public debate around this topic.
- *Research security* should be discussed at the national and international level. At the international level the debate should focus around creating a playing field (e.g., EU, G7, OECD).
- Some participants suggest the use of the term *"*safeguarding science" instead of '*research security*' to include areas such as political and human sciences where risks are not always so obvious.
- *Research security* has different levels: the transfer of technology, the influence of research scope, the ethical application of research and its results.
- Research security can imply an administrative burden for universities, partly driven by lack of clear guidance from government. Therefore, more support to universities is needed.
- There is a general agreement on employing guidelines, frameworks, and risk assessments to manage and mitigate risks. Efforts are geared towards fostering a culture of research security, providing clear guidance, and striking a balance between academic freedom and the security of research.
- Academic freedom is an absolute right, though, it also involves certain responsibilities related to research security for researchers, and therefore tools and sufficient capacity building for researchers is key so that "scientists can act as ambassadors for research security".
- A case-by-case approach and a constant dialogue between researchers and institutions dealing with research security is needed. This means that each research project should be evaluated on its own merits, considering its unique characteristics and potential risks.
- There is a constant challenge in the field of research security related to 'screening' – determining the precise boundaries of where research security measures should begin and end. This challenge is described as a grey area in terms of geographical elements, stakeholders, and timeframes. As researchers, institutions, and funders often spread across different countries, it becomes challenging to determine which geographic guidelines or legal frameworks to apply. Each stakeholder group may have different priorities, perspectives, and responsibilities related to research security. Moreover, research projects can span various timeframes, from short-term studies to multi-year endeavours. The time-sensitive nature of some research, evolving threats over time, and the long-term impacts of research findings make it challenging to define when research security measures should be implemented and how long they should remain in effect.

Machteld Haaksman – Manager on Knowledge Security in the Ministry of Education, Culture, and Science, the Netherlands

- *Research security* is a topic with a big momentum in many countries and organisations, that deserves attention to further develop and strengthen it.
- It is a topic underlined by a big sense of urgency to make sure that researchers can collaborate safely and securely in research environments.

- It is an important topic for the societal matters we are facing, and therefore we need to make sure that international research cooperation develops a common understanding and provides more clarity in the complexity of *research security*.
- Three key takeaways: (1) to connect with each other and have conversations about this topic; (2) there are differences between countries in the advancement in this field and therefore there is a need to exchange, learn from each other and help each other; and (3) it is a delicate topic that requires to find the right balance between research autonomy and security and have dialogues and co-creation, as well as having an ecosystem - and governance approach.

Report

Introduction

The Workshop on Research Security took place on 7th December 2023 and was the seventh of a series of workshops as part of the European Commission's Multilateral Dialogue (MLD) on Principles and Values in International Research & Innovation (R&I) Cooperation. The event was co-organised by the European Commission together with the United States, Finland, Belgium, the Netherlands, the International Science Council, and CESAER. It attracted around 135 participants from 36 countries, and from international organisations such as the International Science Council, the OECD, and UNESCO, as well as from several European stakeholder organisations.

Research security is a topic that is receiving increasing attention from public authorities as well as the research community due to the evolving and challenging geopolitical context. It is a concept where there are no commonly agreed definitions yet. Nonetheless, some common understanding is that research security refers to safeguarding research and innovation from interference by or on behalf of foreign state-actors that affects national security and/or are contrary to one's values and principles.

Against this background, the objective of the workshop was to provide a platform for an open dialogue on distinctions and commonalities in the conceptualisation and application of research security in the different national contexts across the globe. After an introduction by Martin Penny, Head of Unit, International Cooperation in DG R&I of the European Commission, Dr Rebecca Keiser, Chief of Research Strategy and Policy at the National Science Foundation, USA, set the policy context of the workshop.

Martin Penny, Head of Unit, International Cooperation in R&I, DG R&I, EC, gave opening remarks to the workshop, introducing the objectives of the MLD and underlining the importance of this topic – research security – amidst the global rise of geopolitical tensions and competition.

Opening

Dr Rebecca Keiser, Chief of Research Strategy and Policy at the National Science Foundation (NSF), U.S., set the context for the workshop introducing the topic of research security and the U.S. perspective in this regard. The U.S. have been dealing with issues of research security for a number of years. Since 2017, U.S. science agencies have begun receiving intelligence briefings in response to concerns about other countries appropriating U.S. fundamental research and using it for questionable purposes. These briefings were also delivered to the academic community. In 2019, a JASON[5] report was issued on Fundamental Security which highlighted the issues of misappropriation of fundamental research, undisclosed conflicts of commitments, and end uses of research. Subsequently, in 2020 the U.S. White House's Office of Science and Technology Policy established the U.S. research security subcommittee together with other departments such as Health and Energy, with the objective of understanding and developing policies that maintain openness while addressing research security issues. These efforts were complemented by international initiatives

[5] JASON Report on Fundamental Research Security (2019): https://www.nsf.gov/news/special_reports/jasonsecurity/JSR-19-2IFundamentalResearchSecurity_12062019FINAL.pdf

such as the establishment of the G7 Security and Integrity in the Global Research Ecosystem Working Group[6], and the OECD Global Science Forum report on Research Security and Integrity[7].

Figure 1 Cell diagram of research security, NSF

Source: U.S. National Science Foundation (NSF), 2023

Dr Rebecca Keiser introduced a research security model from the NSF composed of three main values: Rigor & Reproducibility, Research Ethics, and Responsible Conduct of Research (Figure 1).

She highlighted the need to ensure that the research system remains both open and secure at all stages of research; both in fundamental and applied research. For fundamental research, there is a need to safeguard researchers' ideas, perform due diligence on research funding sources, assess potentially harmful end uses, and collaborate internationally on research security. In a similar way, for applied research, there is a need to safeguard intellectual property (IP), perform due diligence on sources of venture capital and investment, assess potentially harmful end uses, and vetting international transactions.

All actors, from funders to researchers, have responsibilities in the field of research security. Firstly, funders need to collect appropriate disclosures, assess research proposals for potential risks, and work to mitigate those risks. Secondly, research institutions need to verify disclosures are complete, oversee the use of research funding in their institutions, make sure that potential international interactions are based on true collaboration, and promote a research security culture. Finally, researchers need to understand the terms of any proposed affiliation of funding sources, communicate with home institutions and funding agencies, and follow a research security culture.

She referred to SECURE, a U.S. non-governmental entity with the mission to empower the research community to make security-informed decisions about research security concerns by providing information, developing tools, and providing services to universities, non-profit research institutions, and small and medium-size enterprises (SMEs). She also referred to the Research on Research

[6] G7 Common Values and Principles on Research Security and Research Integrity (2022): https://www.bmbf.de/SharedDocs/Downloads/de/2022/220812-g7-sigre-paper.pdf?__blob=publicationFile&v=2

[7] OECD Policy Paper on "Integrity and Security in the Global Research Ecosystem" (2022): https://www.oecd.org/publications/integrity-and-security-in-the-global-research-ecosystem-1c416f43-en.htm

Security Programme (RRSP), an NSF funding programme which seeks to fund research that will identify and characterise attributes and distinguish research security from research integrity. It also aims at improving the understanding of the nature, scale, and scope of research security risks; providing insights into methods for identifying, mitigating, and preventing research security violations; and developing methodologies to assess the potential impact of research security threats to the U.S. economy, national security, and research enterprise.

Dr Keiser concluded by providing information on a series of new Research Security Training Modules on what is research security, disclosure, management and mitigation of risks, and international collaboration. They have been developed together with the US departments of energy, health, and defence, and are available to download through a public platform, for international partners as well.[8]

After the introductory speeches, the participants discussed, in two rounds of parallel breakout sessions, three different aspects of research security: (1) **conceptualisation** of research security, (2) **application** of research security measures/policies by national governments and national funding agencies, and (3) the **role of research institutions** in managing and mitigating risks.

The discussions followed the Chatham House Rule[9] to encourage an open exchange among participants. The discussions were guided by the following sets of questions per topic:

Topic 1: ***Conceptualisation of research security***

- What are the key elements of research security in your country?
- How are potentially undesirable end uses of research identified in your country/organisation?
- Are there areas where the benefits of international collaboration outweigh research security concerns?

Topic 2: ***Application of research security measures/policies by national governments and national funding agencies***

- In your country/organisation, how do you maintain the essential principles of openness and transparency while also safeguarding research?
- How is you country/organisation considering actions to safeguard against potentially harmful end uses of research?
- How does your country/organisation differentiate between stages of research (from basic to applied) when applying safeguards to research?
- What training and outreach opportunities are provided in your country to the research community to build a culture of research security and by whom?

Topic 3: ***The role of research institutions in managing and mitigating risks***

- How do you/your research institutions make sound decisions on research practice and collaboration, given research security concerns?
- What are the channels for dialogue between institutions and the authorities about the implementation of policies and guidelines?
- How do you manage uncertainty of the potential end-use of research?

[8] https://www.nsf.gov/pubs/2022/nsf22576/nsf22576.htm?org=NSF
[9] Chatham House Rule: https://www.chathamhouse.org/about-us/chatham-house-rule

- Are there ways to think about trusted partnerships and be more proactive?

Some general conclusions that referred to the topics and were highlighted in the discussions, are that:

- Research security is constantly evolving, requiring policies and practices that can adapt quickly to new challenges and situations.
- It's crucial to maintain a balance between the openness necessary for collaborative research and the measures needed to secure research integrity and manage risks.
- A case-by-case approach, considering each project's unique context, coupled with strong collaboration and communication among all stakeholders, is essential for effective research security.
- Educating and equipping researchers with the necessary knowledge and tools is vital for building a proactive culture of research security.
- Harmonising research security standards internationally and providing clear guidance and support to research institutions are key to managing security risks while promoting global scientific collaboration.

Parallel breakout sessions

This section summarises the main points of discussion for each of the three topics that were discussed in parallel breakout sessions.

Topic 1: Conceptualisation of research security

In the realm of research security, a crucial aspect is the management and protection of diverse intellectual assets that emerge from global research and innovation efforts. These assets extend beyond the traditional framework of intellectual property rights (IPRs), encompassing a wide array of outputs such as data, prototypes, know-how, and publications. The key elements of research security involve safeguarding these assets against potential misuse or undesirable end uses, particularly those that could compromise national security or contradict ethical standards.

Simultaneously, there is a growing recognition of the significant benefits that stem from international collaboration in research. Such collaboration can amplify the value and impact of intellectual assets, driving advancements in various fields. However, this necessitates a balanced approach where the benefits of sharing and collaboration are weighed against the risks of exposure to security threats. Managing research security effectively, therefore, involves not only maximising the value of research but also ensuring their security and ethical use in a global collaborative landscape.

Key elements of research security

The discussion started with many of the participants outlining the lack of a clear definition of *research security* at national level. Some countries are still debating what is included and what is not, and how to develop a coherent approach to the topic. This reinforces the importance of raising awareness about potential risks and dangers while performing research, as it is not always clear what the elements of *research security* are. For the Netherlands, for example, research security has three dimensions: unwanted knowledge transfer, foreign interference on research, and research ethical dilemmas. For France, key elements of research security are the protection of national interests, national defence, and competitiveness. Others have adopted a more pragmatic approach where research security relates to making a risk assessment of international partners' technologies, research areas, joint contracts, and the partner itself (e.g., Denmark and Spain); what some call

"cooperating but being cautious". For OECD, research security has to do with the protection of economic and national interests and preventing undesirable foreign states from interfering in research.

The absence of a common definition of *research security* has so far led to limited discussions and attention to this topic in the universities and research institutions of the participating countries. Against this context, the usefulness of national toolkits and guidelines on research security was highlighted. Participants indicated the need to co-create and involve all actors (ministries, industry, research institutions) in the development of such tools. Nonetheless, participants also raised that sometimes it is difficult to convince researchers that research security are also issues they need to consider. The Netherlands, however, shared its experience with the development of research security guidelines in close collaboration with universities.

In addition, some countries observed the need to incentivise universities to take measures, through direct requests (by government departments, agencies, ministries) and self-regulation. In this regard, participants highlighted that EU-level tools and cooperation actually helps and promotes efficiency in research security, remarking particularly the EU Toolkit on Tackling R&I Foreign Interference.

The discussion finalised by stating the need to maintain a balance between academic freedom, openness, and security in research, and the importance of finding a common ground on which a shared understanding of research security can be built. For this aim, the U.S. stated the need to further develop the conceptualisation of *research security*, and to increase the research on *research security* – which is a cross-cutting topic requiring an interdisciplinary approach.

Potentially undesirable end uses of research

The participating countries and organisations shared some experiences about how they identify potentially undesirable (harmful) end uses of research. One of the main points that came out within this part of the discussion was the dual use of research. To overcome this issue, many of the participant countries have deployed training courses to increase awareness about research security and related risks (e.g., Morocco) and more specific programmes for research managers to make sure they are able to identify projects that could possibly have dual-use purposes (e.g., Sweden).

New Zealand shared its specific example of a research security framework they have been implementing for 4-5 years based on five aspects:

i) Early collaboration with researchers,
ii) technology assessments made by the government,
iii) export controls,
iv) incoming research assessments for national security, and
v) immigration control.

Others, such as France, mentioned the establishment of 'officers' for research issues at universities and research institutions in charge of raising awareness, addressing research security questions and topics, and overseeing a list of sensitive research areas.

Benefits of international collaboration outweighing research security concerns

There was almost unanimity among the participants that, indeed, the benefits of international collaboration outweigh research security risks, particularly in areas such as climate change and agriculture. Participants noted that there is no scientific area where there are zero risks, and that the approach should be one based on risk management rather than risk avoidance. They added that a

single institutional level should not deal with the topic by itself, but that national, supra-national, and research institutions should work together to identify risks and take advantage of international collaboration in research.

This brought up the point of taking a case-by-case approach, which was commonly remarked by the delegates alluding to the need of assessing risks and screening research projects depending on the nature of the project, the collaborators, the science area, among other factors.

Material shared in the discussion:

- Norway
  - Guidelines and Tools for Responsible International Knowledge Cooperation, Norway: https://hkdir.no/en/guidelines-and-tools-for-responsible-international-knowledge-cooperation
- US
  - U.S National Institute of Standards and Technology (NIST) "Safeguarding International Science Research Security Framework": https://nvlpubs.nist.gov/nistpubs/ir/2023/NIST.IR.8484.pdf
- Canada
  - Guidelines, tools, and resources (including courses, risk assessment forms, etc): https://science.gc.ca/site/science/en/safeguarding-your-research
- Ireland
  - Principles of Good Practice in Research in Irish Higher Education Institutions https://hea.ie/assets/uploads/2022/12/High-res-links-v3-HEA-Principles-of-Good-Practice-in-Research-within-Irish-Higher-Education-Institutions.pdf
- CESAER
  - Keeping Science Open, White Paper: https://doi.org/10.5281/zenodo.8355324

Topic 2: Application of research security measures/policies by national governments and national funding agencies

Participants from various nations shared their insights, strategies, and faced challenges in this complex area of research security. Discussions centred around the training and outreach opportunities available to the research community for enhancing research security. Country representatives outlined their methods and the organisations responsible for these initiatives.

Key points from the discussions were the difficulties in maintaining openness and transparency in research while implementing effective security measures. Countries are adopting approaches that are collaborative and multidimensional, stressing the importance of institutional autonomy, ethical considerations, and the involvement of government and security services. These strategies require ongoing learning, adaptation, and the integration of research security into institutional cultures.

The conversations also highlighted the diverse efforts by nations to protect research from potentially harmful uses. These efforts include creating specific guidelines, performing risk assessments, conducting ethical reviews, and enhancing collaboration and information sharing. A key theme was the need to balance openness with security, and the developing cooperation between government bodies and research institutions. Given the global scope of research and its security challenges, continuous adaptation, dialogue, and international cooperation are essential.

Finally, the workshop set out the various methods nations use to differentiate between research stages when implementing safeguards. Strategies such as tailored risk assessments, the creation and modification of guidelines, and collaboration with security services are fundamental. The discussion acknowledged the challenges in maintaining openness alongside security, addressing ambiguities in rapidly evolving research fields, and understanding the roles of both governmental and institutional bodies in ensuring research security. The significance of international collaboration and establishing common standards in this area was also emphasised.

Maintaining the essential principles of openness and transparency while also safeguarding research

The workshop discussion on this topic centred around the challenge of maintaining essential principles of openness and transparency in research while also implementing effective safeguarding measures. Discussions revealed a landscape where countries are actively developing and refining their approaches to research security. Emphasising researcher empowerment, balancing openness with security, fostering collaboration, conducting comprehensive risk assessments, and continuously adapting research security measures are prevalent strategies.

Countries are prioritizing institutional autonomy while adapting research security measures. The U.S. focuses on enabling researchers to apply these measures independently, and in Finland, security agencies regularly brief university councils to enhance safety awareness in their organisation. Both Finland and Sweden encourage responsible international collaboration through seminars and discussions. A challenge, shared by several countries is finding the right balance between open research and academic freedom on the one hand and accommodating certain security needs. in this light, The UK, for example, has introduced new university policies for international partnerships since 2019. Sweden is developing proposals to merge scientific openness with security, while France provides targeted research guidelines from its Directorate for Defence and National Security. Switzerland and The Guild stated the need for comprehensive and multi-dimensional risk assessments for research institutes.

Encouraging collaboration and dialogue within and between research institutions and government bodies, as practiced in Austria and Slovenia, is a key strategy. Canada's approach involves designing research security strategies directly with the research community, ensuring the balance of research knowledge with the ecosystem and threats. Acknowledging the evolving nature of research and its associated risks, countries like Canada and Denmark focus on continually adapting their research security measures.

The concept of research security as part of the institutional culture is gaining traction. In New Zealand, for example, there's an ongoing intense review of how research security is balanced with openness, involving both the security agenda and the research sector. Morocco is starting to work on research security with a focus on awareness-raising for students and teachers, with government institutions playing a role in securing research, particularly in intellectual property.

China focuses on ethical reviews, oversight, and public communication to maintain transparency in both domestic and international collaborations. Regular information sharing and involvement of research communities in developing security measures are common across several countries.

Actions to safeguard research against potentially harmful end-uses

The discussion on safeguarding research against potentially harmful end-uses revolved around various national strategies and actions. Countries are exploring various approaches to **training and outreach** on research security, emphasising the importance of awareness, support, and the use of intellectual property as a control tool. The discussions highlighted the need for concrete examples of **tools and practices to better understand, detect and address** research security breaches. Challenges include resource constraints, the complexity of monitoring research security measures, and the need for a more nuanced understanding of research stages and their associated risks. International cooperation and the adoption of common standards and principles, as seen in the G7 principles, are considered vital in addressing the global nature of research security threats.

Country participants discussed various National Strategies and Actions to safeguard harmful end-uses of research, spanning from development of **guidelines, risk assessment and ethical reviews, to collaboration and information sharing**.

Many countries have developed specific guidelines to prevent harmful end-uses of research. For instance, France utilises guidance provided by its Directorate for Defence and National Security, distributed through different ministries to the research community. Sweden is working on proposals to refine existing guidelines, aiming to include considerations for both security threats and the potential misuse of research. The Netherlands provide a national contact point (NCP) where cases can be discussed with researchers upon request. This NCP provides advice and supports the intelligence research assessment.

The importance of conducting risk assessments and ethical reviews is emphasised across several countries. China, for example, has recently published legislation to guide ethical, social, and legal risks in life sciences. Canada adopts a collaborative approach to risk assessment, co-developing strategies with the research community to balance knowledge, ecosystem, and threats.

Countries including the UK have set up new screening services for international partnerships, fostering a culture of information sharing and collaboration to identify and manage risks. Germany's Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) highlighted the role of collaborative experience in raising awareness among researchers to act responsibly in international cooperation. Germany also expressed the challenge of finding criteria to monitor and evaluate the effectiveness of research security measures. A systemic approach, incorporating continuous learning and adaptation, is crucial. New Zealand highlights the need for ongoing monitoring and reviewing to ensure that safeguards remain effective and relevant across different research stages.

Recognising that different research types have varying risk levels, countries like Canada tailor their research security measures accordingly. This includes distinguishing between fundamental research and research conducted in universities versus colleges. In February 2024, Canada will launch a new policy that will include a list of sensitive projects and/or technology to further clarify their risk-based approach.

The use of technology and intelligence services in risk mitigation is evident in countries like Austria, where security services provide information to aid decision-making in research labs. In Finland, the national security and intelligence service is invited to give briefings on research security, indicating a proactive approach to threat awareness.

The discussion highlighted the need for a multidimensional approach that includes not just security but also ethical and sustainability considerations, as indicated by Sweden's work in this regard.

The role of government bodies in advising and guiding research institutions is crucial, as seen in France and the UK. The collaboration between government and institutions forms a significant part of the strategy.

Emphasising the evolving nature of threats, countries like New Zealand and Canada focus on continuous adaptation and updating of their strategies, involving regular dialogues with research communities.

Differentiating between stages of research (from basic to applied) when applying safeguards to research

Differentiating between fundamental and applied research presents a significant challenge, especially concerning export controls and the application of research security measures.

The discussions revealed a complex landscape in differentiating between research stages and applying appropriate safeguards. Countries are employing diverse strategies, such as risk classifications, self-regulation, and collaboration with other countries, to address this complexity.

The Netherlands raised concerns about differentiating fundamental from applied research and the applicability of general exceptions for fundamental research. They noted the difficulty in identifying risks in fundamental research due to its broad application potential. The Netherlands is working on developing a law for screening non-EU personnel working in sensitive research areas. Austria highlighted the challenge in distinguishing basic from applied research, particularly in the context of export restrictions. The difficulty in fitting researchers within the framework of export controls was discussed.

Recognising the diverse nature of research stages, countries including Canada notably emphasised tailoring risk assessment measures. Fundamental research often entails different risks compared to applied research conducted in universities or colleges. In the UK, there's an acknowledgment of the need for a nuanced understanding of what constitutes basic and applied research, especially in rapidly evolving fields like Artificial Intelligence (AI).

Sweden discussed the importance of refining guidelines to address the balance between security and openness in both basic and applied research stages. Germany highlighted the role of guidelines in guiding researchers to responsibly navigate international cooperation, taking into account the different stages of research. Countries like Austria and Finland utilise engagements with national security and intelligence services to inform the application of safeguards, ensuring that the unique aspects of each research stage are considered.

Ethical reviews and sustainability considerations play a significant role in differentiating research stages. For instance, China's approach to ethical reviews in life sciences reflects a keen awareness of the varying risks across research stages.

Addressing grey areas in differentiating research stages, especially in rapidly evolving fields like AI and biotechnology, is a challenge acknowledged by many participants, including the UK and Sweden. Collaborative efforts in developing safeguards are emphasised, with countries including Canada and the UK involving research communities in the formulation and adaptation of security strategies.

The roles of government bodies and research institutions are pivotal in identifying and applying appropriate safeguards. This includes advisory roles, as seen in France, and decision-making roles in specific cases.

Training and outreach opportunities to build a culture of research security

The workshop participants engaged in a detailed discussion about the various trainings and outreach opportunities available to the research community to foster a culture of research security. Representatives from different countries shared their approaches, highlighting the entities responsible for these initiatives and the methods employed.

Countries, notably Canada and the UK, emphasised the importance of collaborative training programs. These involve various stakeholders, including federal departments, research funders, and post-secondary institutions, co-developing training material. In Canada, for instance, a portal with regularly updated courses on various research security topics is a key resource for the research community.

In China, scientific ethics are incorporated into the university curriculum, and ethical review standards are issued for specific research areas such as stem cell research. France conducts awareness campaigns at the local level in universities, schools, and research labs, often built with the help of security services. South Africa discussed their preventative approach, scrutinising all research through disciplinary and ethics level committees.

In Finland, the national security and intelligence service regularly provides briefings to university councils. National seminars and open discussions, such as responsible international cooperation seminars, play a crucial role in small countries like Finland.

The development and dissemination of guidelines are key tools for training and outreach. Sweden, for instance, proposes to work further on existing checklists and guidelines to include various aspects of research security. Germany issued a set of recommendations on mitigating risks in international cooperation, helping to raise awareness among researchers.

Research institutions and government bodies play a pivotal role in training and outreach initiatives. For example, in the UK, universities set up new services and policies for international partnerships, while government bodies like ARCAP provide valuable advice. A recurring theme in the discussion was the challenge of balancing the need for security training with the preservation of academic freedom, as emphasised by countries like Austria and the UK. Adapting training and outreach programs to the rapidly changing research environment, especially in fields such as Artificial Intelligence (AI), is a challenge acknowledged by several countries.

Engaging diverse research communities in training and outreach efforts, considering the varying needs and levels of understanding across different fields, is a crucial aspect, as highlighted by Canada and Germany. The use of digital platforms and resources for training and outreach, such as the Canadian portal for research security courses, is an effective strategy for broad dissemination and accessibility.

International collaboration in developing training and outreach programmes is seen as beneficial. Sharing best practices and learning from the experiences of different countries contributes to a more robust global research security culture.

Material shared in the discussion:

- Sweden
  - Checklist Global Responsible: https://suhf.se/arbetsgrupper/expertgruppen-for-internationaliseringsfragor/
  - Swedish Technology self-assessment tool: https://www.kometinfo.se/in-english/responsibletech/
- Canada
  - Portal on research security: https://science.gc.ca/site/science/en/safeguarding-your-research
- Germany
  - DFG recommendations "Dealing with risks in international cooperation": https://www.dfg.de/download/pdf/dfg_im_profil/geschaeftsstelle/publikationen/stellungnahmen_papiere/2023/risiken_int_kooperationen_en.pdf
- France
  - French Senate, Rapport: Vade-mecum à l'usage des scientifiques et des experts, 2015: https://www.documentation-administrative.gouv.fr/adm-01859867/document
  - French Senate, Rapport GATTOLIN « Influences étatiques extra-européennes dans le monde universitaire et académique français et leurs incidences », 2021 & « Extra-European state influence on French universities and academia and its impact »
- Finland
  - Finish considerations related to good scientific practices, security and competitiveness are relevant. https://julkaisut.valtioneuvosto.fi/handle/10024/163963
- Canada
  - National Security Guidelines for Research Partnerships, which are country and company agnostic: https://science.gc.ca/site/science/en/safeguarding-your-research/guidelines-and-tools-implement-research-security/national-security-guidelines-research-partnerships
  - Canada risk assessment process under this framework, which only applies for a very small number of funding opportunities: https://science.gc.ca/site/science/en/safeguarding-your-research/guidelines-and-tools-implement-research-security/risk-assessment-review-process
- United Kingdom
  - UK trusted research guidance for academia: https://www.npsa.gov.uk/trusted-research-academia
  - UK RCAT Update report (2023): https://assets.publishing.service.gov.uk/media/654a2f1be2e16a000d42aae4/research_collaboration_advice_team_update_report.pdf
  - UK National Security and Investment Act: guidance for the higher education and research-intensive sectors: https://www.gov.uk/government/publications/national-security-and-investment-act-guidance-for-the-higher-education-and-research-intensive-sectors/national-security-and-investment-act-guidance-for-the-higher-education-and-research-intensive-sectors

Topic 3: The role of research institutions in managing and mitigating risks

How research institutions make sound decisions on research practice and collaboration

This discussion emphasised the central role that researchers play in making sound decisions on research practice and collaboration. However, participants emphasised that risk assessment should not be only the responsibility of researchers, as they may not see all the potential risks in research collaborations. It was stressed that proper risk assessment requires extra knowledge about dual use of research, IP legislation, and science diplomacy, and that consequently, researchers should be supported by tools and capacity building from governments and international institutions, particularly in those areas that are more sensitive than others, such as nuclear energy.

In the process of screening research for potential risks, there are always grey areas, complicating the research security aspects; delegates shared experiences and examples from their countries/organisations regarding this issue. The UK, for example, shared its experience of producing guidelines on 'managing risks in international collaboration' and organising awareness campaigns. This has been done by Universities UK – the association of UK universities – but also other agencies such as the UK Research & Innovation (UKRI) which has specific guidelines and principles. The UK representative added that despite these advances, a challenge remains regarding monitoring and reporting, since an agency such as UKRI is not a compliance body. On the other hand, in Canada, national research security guidelines focus mostly on sensitive technologies and those that can be subject to dual use. Particularly, Canada has issued specific guidelines for cybersecurity and data protection to help researchers screen their partners before entering into a collaboration.

In contrast, in Japan there is not a single "central" guideline for risk assessment; it is up to each institution how they assess risks and screen research collaboration. This is mainly to respect academic freedom and research autonomy. Similarly in Germany, research freedom is protected by law, and therefore the government does not involve too much, leading to a more bottom-up approach where research institutions try to 'regulate themselves'. It was noted also that for some countries, the screening process of each research collaboration project and the verification of the profiles of the collaborators may be easier than for others due to the size of the country (e.g., New Zealand).

The discussion triggered a point on how countries/organisations conceptualise differently the concept of *research security*. In France, for example, this process is called 'protection of scientific and technological progress', while in Germany they prefer to call it 'safeguarding science and scientific cooperation' to cover all science fields, from natural sciences to political sciences. On its hand, in Sweden it is called 'responsible internationalisation'.

Finally, the existing disparities between institutions were mentioned, which make it difficult to internalise the importance of research security in certain institutions. In addition, during this discussion, it was also acknowledged that research security also became more important after Ukraine's aggression by Russia.

Channels for dialogue between institutions and authorities about the implementation of policies and guidelines

In terms of bridging the gaps between institutions and authorities regarding the implementation of research security policies and guidelines, it was commonly agreed that the dialogue between governments and research institutions is paramount. Participants highlighted the need to have a 'whole country approach'; one that covers researchers, higher education institutions, and

governments, and that considers the specific cultural background of the country in question. This approach requires the establishment of new structures in universities and ministries. Japan, for example, exposed its perspective where researchers are responsible for disclosures, research institutions for risk management and linking with the government, and the government for providing guidelines and sharing best practices. Nonetheless, this type of approach still represents a challenge in the sense of keeping a wide variety of actors involved and informed – as set out by a UK delegate.

A common practice mentioned across the discussion was raising awareness among scientists, emphasising why research security regulations are put in place, so that researchers understand what is at stake, what is being protected and why. The Netherlands shared their experience which they base on three key aspects: raising awareness, establishing security measures (e.g., ICT and cybersecurity), and safeguarding the research organisations. In addition, as mentioned before (in Topic 2), the Netherlands have 'national contact points' who work together with the intelligence services on research security issues. The Netherlands' representative added that recognition and rewards are also important for researchers to guarantee they mitigate risks correctly. Germany added that they have drawn on the Netherlands' approach by linking the different ministries and establishing a dialogue with universities. Meanwhile, Morocco focuses its mitigation on four main points: training researchers, securing data, limiting remote access to data, and limiting research against certain defined values.

In addition to formal dialogue, guidelines, policies and regulation, the importance of having constant informal interactions between the government and research institutions and researchers – of spaces for dialogue and co-creation of solutions to common challenges, were highlighted.

At the EU level, the importance of having a common approach between all EU Member States was mentioned; one that establishes a same level of analysis and understanding and where tools and guidelines are shared between countries. Delegates stated that the EU economy is mainly knowledge-based and that, therefore, EU-level collaboration in this field is paramount.

Finally, it was mentioned that currently there is paradox regarding research security policies, guidelines, and regulations. In the sense that the level that has the biggest responsibility to tackle/ implement research security issues is the level with the least resources and least incentives to deal with these risks – namely the universities and research institutions. It was added that a cultural change in both research institutions and governments need to happen in order for measures to be effective.

Ways to think about trusted partnerships

In terms of establishing long-term trust and partnerships in research security, participants pointed to governments as key actors in building these partnerships and engaging in international networks for science diplomacy. Nonetheless, they also remarked that national intelligence or defence services may not be the best actors to establish a trusted partnership with researchers, and that therefore, it is important to find a common ground between research institutions and governments when developing stable relationships.

Two interesting examples were presented in this regard. First, Swiss Nex[10], a guideline with tools for facilitating collaboration in both basic and applied science in international collaborations. And second, the function of a 'science attachés' in Germany which consists of officers in the embassies

[10] Swiss Nex: https://swissnex.org/

responsible for keeping contact with researchers in other countries. These science attachés have become a vehicle for developing trusted partnerships and enhancing international collaboration and openness in research.

In addition, it was remarked that cultural differences may create risk averseness of doing international collaboration in research; and that that's why it is important to consider the different national contexts, values, and languages while engaging into R&I collaborations.

Material shared in the discussion:

- The Netherlands
  - Dutch national contact point for knowledge security: https://english.loketkennisveiligheid.nl/knowledge-security.
  - Dutch national guidelines: https://english.loketkennisveiligheid.nl/knowledge-securitySwitzerland
  - Guide Towards Responsible International Collaborations, Swiss Universities: https://www.swissuniversities.ch/fileadmin/swissuniversities/Dokumente/Internationales/Guide_Towards_responsible_international_collaborations2.pdf
- Sweden
  - Swedish university checklist: https://suhf.se/arbetsgrupper/expertgruppen-for-internationaliseringsfragor/
  - Web-based self-assessment tool for technology development developed by a previous Swedish government committee for technological innovation and ethics: https://www.kometinfo.se/in-english/responsibletech/
- United Kingdom
  - Complex Collaborations, Efficiency, Equity, Quality, and Security: https://arma.ac.uk/wp-content/uploads/2023/03/Trusted-Report_Booklet_v7.pdf
- The Guild
  - The Guild's Statement on Responsible Internationalisation: https://www.the-guild.eu/publications/statements/the-risks-of-international-collaboration-must-be-balanced-with-the-risks-of-non-collaboration.html
- EU
  - Safeguarding Science Tools, EU: https://www.safeguarding-science.eu/tools/operate/
- OECD
  - National initiatives from the OECD platform: https://stip.oecd.org/stip/research-security-portal

Annexes

Annex 1: Organizing team

This workshop was co-organised by the United States, Finland, Belgium, the Netherlands, the International Science Council, CESAER and the European Commission. Special thanks go to the following persons for their active involvement in drafting the concept note for the workshop together with the EC:

US

- Keiser, Rebecca Lynn, National Science Foundation
- Rollins, Evette, National Science Foundation

The Netherlands

- Irna van der Molen, University of Twente
- Nora Van Bracht, Ministry of Education, Culture and Science

Belgium

- DECADT Brigitte, Belgian Science Policy Office
- Cindy Du Bois, Royal Military School

Finland

- Vihma-Purovaara Tiina, The Ministry of Education and Culture
- Jukka Tanskanen, The Ministry of Education and Culture

CESAER

- Mattias bjornmalm

International Science Council

- Vivi Stavrou

Annex 2: Moderators and notetakers

With special thanks to the moderators and notetakers that volunteered for the workshop.

Moderators

- Gaia Airulo, EC DG RTD
- Vivi Stavrou, International Science Council
- Sarah Stalker-Lehoux, The US
- Mattias Björnmalm, CESAER
- Kleitia Zeqo, Technopolis Group
- Max Bueno de Mesquita, The Netherlands
- Cind Du Bois, Belgium
- Louise Drogoul, CESAER
- Wouter Verheij, The Netherlands
- Sophie Ratcliff, CESAER
- Jukka Tanskanen, Finland

Notetakers

- Maria Arzamaskova, EEAS
- Ibeas Rodriguez De Acuna Maria, EC DG RTD
- Elise Agdestein, International Science Council

- Irna van der Molen, University of Twente
- Anissa Zeroual, EC DG RTD
- Jonathan Puerta, Technopolis Group
- Nora van Bracht, The Netherlands
- Maud Fichet, EC DG RTD
- Justine Moynat, CESAER
- Marte Boonen, The Netherlands
- Alexa Baumer, The US

Annex 3: Participants and stakeholder organisations

Countries represented in the workshop:
Australia, Austria, Belgium, Canada, China, Czech Republic, Denmark, Estonia, Faroe Islands, Finland, France, Germany, Hungary, Ireland, Japan, Jordan, Lithuania, Luxembourg, Malta, Mexico, Morocco, Netherlands, New Zealand, North Macedonia, Norway, Portugal, Romania, Slovenia, South Africa, Spain, Sweden, Switzerland, Tunisia, Turkey, United Kingdom, USA

Stakeholder – and international organisations represented in the workshop:
ALLEA, AURORA, CESAER, COST Association, EARTO, EUA, Euroscience, INGSA, Initiative for Science in Europe, International Science Council, OECD, Science Europe, The Guild, UNESCO, Universities of the Netherlands, YERUN

European Commission
DG R&I

Annex 4: List of abbreviations

Abbreviation	Full Form
MLD	Multilateral Dialogue
R&I	Research & Innovation
EC	European Commission
US	United States
OECD	Organisation for Economic Co-operation and Development
UNESCO	United Nations Educational, Scientific and Cultural Organization
NSF	National Science Foundation (U.S.)
DG R&I	Directorate-General for Research and Innovation (European Commission)
IP	Intellectual Property
RRSP	Research on Research Security Programme
DFKI	German Research Center for Artificial Intelligence (Deutsches Forschungszentrum für Künstliche Intelligenz)
IPR	Intellectual Property Rights
NCP	National Contact Point
NIST	National Institute of Standards and Technology (U.S.)
UKRI	UK Research and Innovation
DFG	Deutsche Forschungsgemeinschaft (German Research Foundation)