Input of the Dutch government for the call for evidence for a Commission proposal for a Council Recommendation on Enhancing research security in Europe

The Netherlands welcomes the initiative of the European Commission to propose a Council Recommendation on enhancing research security in Europe. This is needed for an EU level playing field. Openness and international cooperation are at the heart of European higher education, research, science, technology and innovation. Fundamental academic values such as academic freedom and scientific integrity are the basis of this international cooperation. At the same time, the openness that characterises our scientific international collaboration is at risk of being exploited by foreign powers with the intention of increasing their own military, technological, political and economic power.

We are being confronted with threats from state actors resulting in undesirable transfer of knowledge and technology to third countries and interference and influence in education, research and innovation. In addition, ethical issues may arise from cooperation with countries that do not respect fundamental human rights and academic values, resulting in the misuse of research results and limiting academic freedom and tampering scientific integrity. In the Netherlands we use the concept of 'knowledge security' to describe these elements. Whether the term research security, or knowledge security is being used, there is a clear need for a common definition and uniform terminology to describe these threats.

To mitigate these risks and to keep safe and open international cooperation possible, strong national approaches are necessary. However, these measures can only be effective if we strengthen our cooperation and coordination within the EU. Joint action to create an EU level playing field is needed. The Netherlands recognizes and supports many of the possible principles and measures the Commission presents in the guiding document of the call for evidence. In the list below, the Netherlands first highlights the most important guiding principles and the EU-level initiatives the Council Recommendation should encompass. Finally, it presents a list of Dutch national policy measures that may serve as inspiration for the Commission and other member states.

Guiding principles:
- Our academic values, such as academic freedom, scientific integrity and reciprocity, are the foundation of international cooperation.
- Mitigating measures need to be proportionate. The relation between threats and risks on the one hand, and mitigating measures on the other hand should be in balance.
- The approach should respect subsidiarity. We need a multi-layered approach, in which the different roles of the EU, Member States and subnational authorities need to be respected.
- Institutional autonomy of the knowledge institutions should be a leading principle when enhancing knowledge security. This means that self-governance of the sector is a key element of the national and European approach.
- Strong cooperation with and involvement of the knowledge institutions is essential. They are the experts in their fields of research.
- We should make every effort to achieve that policy measures will not unintendedly lead to discrimination or stigmatisation of certain groups or nationalities. This also means the approach should be country agnostic.
- An integrated approach with cooperation between different ministries, including the security services, on the national level ('whole of government approach') and between the different Directorate Generals on the EU-level is necessary for the success of the national and European measures.
- We should develop and implement actions through a learning approach, on the level of the EU, national and the academic sector. This means we have to organise a continuous exchange of knowledge and experiences on and through all these levels.

Initiatives that should be part of the Commission's EU-agenda on knowledge security:
- Set up a permanent, non-formal structure for EU-cooperation on knowledge security with the member states at the core, in order to work together with all member states on EU-actions, exchange national experiences and good practices in a structural manner and avoid a patchwork of different national measures.
- Work on a shared understanding of state actor threats, collect and share information on risks and opportunities in international cooperation (including development of a country neutral tracker of foreign universities related to risky activities, in line with the 'ASPI-

tracker'), conduct research on knowledge security and increase our knowledge base. For example by setting up an EU-centre of expertise on knowledge security.

- Together with knowledge institutions work towards a greater understanding and clarity on the areas of research that may be vulnerable, as their researchers know best what the vulnerabilities are in their respective fields of research.
- Develop tools and guidance for Member States to take measures to monitor the access of persons to those areas of knowledge where the risks to national security of the Member States are greatest. This contributes to creating a shared understanding of threats and common interests that require protection, which could be used by member states to set up similar national frameworks for screening in this field and of which the Netherlands is a strong proponent. The Commission should also facilitate exchange of best practices on dealing with high risk technology areas and state/non-state actors with a view to both their effectiveness and proportionate use of capacity and resources.
- Develop and update tools to assist the knowledge institutions in developing policy on knowledge security within their organisations.
- Organise events for knowledge institutions, funding agencies and researchers to raise awareness of the risks of open international cooperation, to share best practices and to discuss dilemma's. For example in a yearly EU-wide conference.
- Look into EU funding programmes, notably Horizon Europe, to see whether existing conditions and checks related to security and ethics are still sufficient or that refinement is needed.
- Strengthen cooperation with international partners on knowledge security and work towards an international level playing field, by for example sharing best practices. Because international cooperation in research and innovation goes beyond the EU.

In the Netherlands we work on several national policy measures on knowledge security:
- The Dutch government will intensify its continuous dialogue with the Dutch knowledge institutions. The government and knowledge institutions meet periodically and share information on knowledge security.
- We will update our National Knowledge Security Guidelines in 2024. The Dutch government drafted these guidelines with knowledge institutions. The aim of the guidelines is to offer a useful set of practical tools to knowledge institutions in designing their knowledge security policy.
- In 2022, the Dutch government and knowledge institutions signed an administrative agreement in which the knowledge institutions agreed to conduct a risk assessment of international collaborative ventures, and to report on the outcome to their supervisory boards. It was also agreed that an external audit would be carried out to review their knowledge security policy. In 2023 a baseline measurement was conducted, which will be followed up by a second measurement in 2025.
- We will further strengthen and expand the National Contact Point for Knowledge Security. The contact point was opened in January 2022 to serve as the national centre for expertise and advice on knowledge security. The aim of the contact point is to increase awareness and self-regulation in the sector, by answering questions about international cooperation, organising meetings with the community and experts and developing useful tools that can be used directly by the knowledge institutions.
- A knowledge security screening framework is currently being drafted. The new law will introduce a preventative form of screening in the case of sensitive technology. The law focuses on non-EU researchers (and possibly master students in the research phase of their studies).