



This article was published as focus article in the 1st EURAXESS ASEAN Quarterly Newsletter (April 2024).

Research implications on Europe’s Economic Security Package update

With increased uncertainty surrounding global trade and foreign investment, and calls for more clarity from industry and research sectors on terms like “strategic autonomy” and “dual use”, a key update to the [European Economic Security Package](#) has been proposed just six months after the original document was agreed by the European Parliament and Council.

As one of its first outputs to start the new year, the European Commission has issued the update to “strengthen the EU’s economic security at a time of growing geopolitical tensions and profound technological shifts”.

The new package of [five initiatives](#) seeks to: (1) tighten inbound investment screening rules, (2) advance export control conformity throughout the European Union, (3) contemplate the establishment of an outbound investment screening mechanism, (4) scale up dual-use and advanced technology research, and (5) protect research and advanced technology from leaking to strategic competitors.

The revision to the Strategy thus adds a wider geopolitical dimension to what was a largely “economic growth” focused policy goal laid out in the June 2023 agenda. The new Commission proposals are considered integral to the EU’s comprehensive approach to economic security as characterised by three key pillars: fostering competitiveness, mitigating risks, and forging partnerships with countries where economic security interests are aligned.

This tacitly reinforces the EU’s [Global Approach](#) to research and innovation in a changing world, elements of the main pillars of the Horizon Europe flagship R&I funding programme, as well as efforts to widen and strengthen the European Research Area.

Open and outward-looking, mutually beneficial relationships with like-minded partners are the centre point of Europe’s Global Approach to international R&I cooperation, launched in May 2021, while at the same time safeguarding strategically important sectors.

What sort of risks does the Strategy deal with?

According to the June 2023 European Economic Security Package, the key economic security risks Europe faces include supply chain resilience concerns, energy security, and product scarcity – especially related to the green transition, and pharmaceuticals.

Physical and cyber-security risks are also cited, including disruption/sabotage to critical infrastructure and data in the EU. Technology security and “leakage risks” are also considered

threats. This could include espionage or illicit leaking of critical knowledge, and ties into the need for tighter military/intelligence capabilities requiring “specific mitigation measures”, especially for dual-use technologies like quantum, semiconductors, and artificial intelligence.

Further, the “weaponisation of economic dependencies” is explained in the Strategy as the risk of third countries targeting the EU, its Member States, and businesses through trade/investment-related measures directed at influencing policy.

The updated measures unveiled in January 2024 address new, emerging or evolving concerns and include:

- Enhancing EU security and public order by advocating for enhanced screening of foreign investments within the EU.
- Encouraging dialogue and coordinated action among European nations regarding export controls, while respecting existing multilateral frameworks and Member States’ sovereignty.
- Engaging with Member States and stakeholders to identify potential risks associated with outbound investments in specific high-tech sectors.
- Facilitating discussions on how to better support research and development involving dual-use technologies.
- Proposing Council recommendations aimed at bolstering research security at both national and sectoral levels.

Some clarity on dual-use technology

Broadly defined, dual use can refer to an item or technology that serves more than one purpose, but in foreign affairs and the [trade-policy domain](#) dual-use items usually refer to goods, software and technology that can be used for both civilian and military applications. This means they can be subject to export controls which apply to “any natural or legal person, including researchers or partnerships, physically sending, electronically transmitting or personally carrying dual-use items”, according to [EU regulations](#), and affect “brokering, technical assistance, transit and transfer of dual-use items”.

Various types of authorisation are required for a range of items deemed dual-use, including but not limited to nuclear materials, facilities and equipment; special materials and related equipment; materials processing; electronics; computers; telecommunications and information security; sensors and lasers; navigation and avionics; marine; aerospace and propulsion systems.

Other dual-use items intended entirely or partly for chemical, biological or nuclear weapons; military use in countries subject to an arms embargo; and components of military items already exported from an EU Member State without the necessary authorisation. What’s more, authorisation is required for the export of cyber-surveillance items likely to be used for internal repression or serious violations of human rights and international humanitarian law; the transfer of dual-use items listed in the annex of the [consolidated original 2021 list \(Regulation \(EU\)2021/821\)](#), such as stealth technology and strategic control, from one Member State to another.

The 2023 Strategy notes that the Commission was tasked with proposing a updated list of dual-use technologies for risk assessment based on “narrowly defined and forward-looking criteria”. These should factor in the “enabling and transformative nature of a technology, the risk of civil military fusion, and the risk of their misuse for human rights violations”.

The Strategy calls for tighter export controls for certain dual-use items to protect the economy and integrity of European R&D. Decisions on such items, it notes, primarily lie with Member States within the framework of multilateral and EU regulations.

Better aligning economic, security and R&I interests

The historical approach under EU trade policy has aligned security objectives with efforts to foster an “environment conducive to research, innovation, and non-proliferation efforts”. But recent challenges and global tensions have seen heightened military application of strategic fields, notes the Commission, prompting some EU Member States and third countries to intensify national controls on critical technology exports. Often leveraging or supplementing existing multilateral frameworks, these controls target emerging risks associated with advanced semiconductor chip manufacturing and quantum computing equipment.

Recognising the need for greater flexibility to adapt to rapidly changing events, in September last year the EU revisited its [Regulation on Dual-Use Export Controls](#). This and prior revisions seek to further mitigate risks in the “evolving security, technology, and trade landscape, particularly concerning sensitive emerging technologies”.

In October last year, the Commission responded by publishing a [compilation of EU Member States’ national export control lists](#), effectively allowing Member States to “impose authorisation requirements” on items already included on other Member States’ control lists. This helps to streamline efforts and, according to a statement on the announcements, this “first list” includes Dutch controls on machines to make semiconductors, as well as Spanish measures on quantum computing, additive manufacturing, and other emerging technologies. “The publication opens the door for other Member States to coordinate their actions on export controls at a time of increased awareness of essential security concerns,” it notes.

Bolstering national and sectoral research

Developing and keeping pace with new technologies is crucial for EU economic security, reducing dependencies and maintaining/bolstering technological advantages. The original Strategy is clear on the need to prevent technology and valuable innovation being leaked to economic competitors. As such, the Commission is given powers to exclude certain third country entities from participating in research and innovation projects, and limit the transfer of sensitive Horizon Europe results to non-associated third countries.

For critical technologies, it can propose measures to improve research security while attempting to preserve its commitments to openness in R&I, underpinned by the Global Approach. EURAXESS Worldwide tackled this subject in a story last year, called ‘Safeguarding European R&I, a delicate balancing act’, which pointed out that Europe is threading that needle by progressing in its efforts to promote international cooperation in R&I “while at the same time strengthening its leadership and safeguarding its strategic interests in the world” – the conclusion of a timely [Global Approach Implementation Report](#).

To support its research security efforts at the national and sectoral level, in 2022 the EU came up with a [Toolkit on Tackling Foreign R&I Interference](#). Upon its release, Mariya Gabriel, Commissioner for Innovation, Research, Culture, Education and Youth, said that the toolkit was designed to “help us protect our fundamental values, key research findings and intellectual assets”. She added: “Raising awareness and implementing preventive measures is key to tackle threats of foreign intrusion that target critical vulnerabilities and extend across all research activities, scientific domains, research outputs, researchers and innovators.”

Two years on, this is clearly playing out in the latest update to the Strategy, and in particular the new initiative proposing Council recommendations to enhance research security at national and sectoral levels. The presumption here is that strengthened research security is likely to further impact EU R&I as well as related international cooperation under Horizon Europe and especially third country participation in EU research projects and initiatives.

The resulting implications on international research cooperation will likely be revealed once the new initiatives are fleshed out and the Council makes its recommendations.

Unity for economic security

Ultimately, the goal of the Strategy and, no doubt, a key reason behind the recent update is to project greater unity and enhance understanding of the need for secure international trade and cooperation.

Here, the original Strategy clearly signals the sentiment behind Europe’s changing stance on economic security, saying that today’s “interconnected world” demands a greater resolve to ensure the proper functioning of the internal market, integrity of EU trade policy, and safeguarding of its wider security interests.

“Member States’ economic and national security interests, vulnerabilities and responses can rarely be seen or identified in isolation from those of other Member States or those of the Union as a whole,” the authors note.

Again drawing parallels with the Global Approach, they continue that an unwanted alternative to this “EU approach to economic security” is that partners end up picking and choosing alliances, “while less well-intentioned players will seek to divide and conquer”.

Joint EU action across policies and through cooperation between the EU and Member States, is “essential for the Union’s economic security [and the] key to success will be to act in unity”, the Strategy concludes.

How all this ultimately affects and is affected by the global R&I landscape is of course a major talking point, and EURAXESS Worldwide will keep abreast of these developments.

Economic Security Strategy backstory...

On 20 June 2023, the European Commission and the High Representative released a Joint Communication outlining the European Economic Security Strategy. This document set out to mitigate risks amid rising geopolitical tensions and rapid technological changes while maintaining economic openness and vitality in key areas including research and technological development. The Strategy establishes a working framework to both assess and then address identified risks to EU economic security, ensuring the EU remains attractive to business, investment and, from EURAXESS Worldwide’s perspective, for international research mobility as well.

The original Strategy prioritised four risk categories: supply chains, critical infrastructure security (both physical and cyber), technology security and leakage, and economic coercion or dependencies. To tackle these risks, three pillars were raised:

1) Boost EU competitiveness and growth by strengthening the Single Market, supporting a resilient economy, and enhancing scientific, technological, and industrial capacities.

2) Safeguard EU economic security through various policies and tools, including the implementation of new instruments as necessary.

3) Enhance partnerships and cooperation with like-minded countries to address shared concerns and advance common economic security interests.