



Council of the
European Union

Brussels, 6 October 2023
(OR. en)

13892/23

LIMITE

**DUAL USE 11
POLCOM 225
COMPET 961
TELECOM 291
RELEX 1151
CFSP/PESC 1357**

COVER NOTE

From:	General Secretariat of the Council
To:	Delegations
No. Cion doc.:	C(2023) 6689 final
Subject:	COMMISSION RECOMMENDATION of 3.10.2023 on critical technology areas for the EU's economic security for further risk assessment with Member States

Delegations will find attached document C(2023) 6689 final.

Encl.: C(2023) 6689 final



EUROPEAN
COMMISSION

Strasbourg, 3.10.2023
C(2023) 6689 final

COMMISSION RECOMMENDATION

of 3.10.2023

**on critical technology areas for the EU's economic security for further risk assessment
with Member States**

COMMISSION RECOMMENDATION

of 3.10.2023

on critical technology areas for the EU's economic security for further risk assessment with Member States

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 292 thereof,

Whereas:

- (1) The Commission and the High Representative have recognised that with rising geopolitical tensions, deeper economic integration and the acceleration of technological development, certain economic flows and activities can present a risk to our economic security and adopted a Joint Communication on European Economic Security Strategy¹ to put in place a comprehensive strategic approach to economic security.
- (2) The European Economic Security Strategy is based on a three-pillar approach: promotion of the EU's economic base and competitiveness; protection against risks; and partnership with the broadest possible range of countries to address shared concerns and interests.
- (3) As part of this framework and in light of the risks that certain economic dependencies and technical evolutions can present, the EU needs a clear-eyed view of the risks to its economic security and their evolution over time.
- (4) These risks should be identified and assessed together with EU Member States, with inputs from private stakeholders in a dynamic and continuous process.
- (5) The European Economic Security Strategy identified the following four broad and non-exhaustive categories of risks for further assessment: resilience of supply chains, including energy security; physical and cyber-security of critical infrastructure; technology security and leakage; weaponisation of economic dependencies and economic coercion.
- (6) The Commission committed in the Joint Communication to assess the risks of technology security and leakage on the basis of a list of strategic technologies critical for economic security and, as regards the most sensitive risks, to propose a list of critical technologies in view of a risk assessment to be pursued collectively with Member States by the end of 2023.
- (7) The Joint Communication identified the following three narrowly defined and forward-looking criteria for the selection of technologies presenting the most sensitive risks, for further assessment: the enabling and transformative nature of the technology; the risk of civil and military fusion; and the risk of misuse of the technology for human rights violations.

¹ JOIN(2023)20 final

- (8) The enabling and transformative nature of the technology criterion looks at the technology's potential and relevance for driving significant increases of performance and efficiency and/or radical changes for sectors, capabilities, etc.
- (9) The risk of civil and military fusion criterion looks at the technology's relevance for both the civil and military sectors and its potential to advance both domains, as well as risk of uses of certain technologies to undermine peace and security.
- (10) The risk of misuse of the technology for human rights violation criterion looks at the technology's potential misuse in violation of human rights, including restricting fundamental freedoms.
- (11) Following a first internal analysis, the Commission has identified a list of 10 critical technology areas for the EU's economic security. This list of technology areas takes into account work done pursuant to the Action Plan on synergies between civil, defence and space industries². It is a living document and could be subject to further amendments reflecting technological developments as part of an ongoing exercise.
- (12) On the basis of the three narrowly defined and forward-looking criteria for the selection of technologies for further assessment, out of this list, the present Recommendation identifies 4 technology areas, which it considers highly likely to present the most sensitive and immediate risks related to technology security and technology leakage, namely Advanced Semiconductors, Artificial Intelligence, Quantum Technologies and Biotechnologies. These technology areas should, as a matter of highest priority, be subject to a collective risk assessment with Member States by the end of the year. Subject to scoping work with Member States, this collective assessment may focus on subsets of technologies within these four technology areas.
- (13) The structuring of the list reflects the Commission's assessment of which technology areas, among these, are more likely to present the most sensitive and immediate risks related to technology security and technology leakage. This can serve as an aid to decision-making on further steps. The Commission will engage in an open dialogue with Member States on the appropriate calendar and scope of further risk assessments, having regard inter alia to the contribution of the time factor to the evolution of risks. The Commission would welcome a timely exchange on this aspect of the Economic Security Strategy in Council, in the context of its overall political deliberations and orientations in response to the Joint Communication. The Commission may present further initiatives in this respect by Spring 2024, in light of such dialogue and of the first experience with the initial collective assessments, as well as of further inputs that may be received on the listed technology areas. In deciding on proposals for further collective risk assessments with Member States on one or more of the listed additional technology areas, or subsets thereof, the Commission will take into account ongoing or planned actions to promote or partner in the technology area under consideration. More generally, the Commission will bear in mind that measures taken to enhance the competitiveness of the EU in the relevant areas can contribute to reducing certain technology risks.
- (14) The objective of the risk assessment should be to identify and analyse vulnerabilities of a systemic nature according to their potential impact on the EU's economic security and the degree of likelihood that the negative impact materialises. To structure the

² COM(2021) 70 final.

upcoming risk assessment exercise with Member States, the Commission has identified some guiding principles.

- (15) This Recommendation does not prejudice the outcome of the risk assessment. Only the outcome of the detailed collective assessment of the level and nature of the risks presented can serve as the basis for a further discussion on the need for any precise and proportionate measures to promote, partner or protect on any of these technology areas, or any subset thereof. Member States and the Commission may use this information in designing future policy actions, including promotion, partnership or protection measures at national, EU or international level, which should be proportional to the level of risk addressed and precise in terms of scope. No conclusion can therefore be drawn at this pre-assessment stage on recourse to any particular instrument in the EU's or the Member States' toolboxes of measures to promote, partner or protect with others in view of enhanced economic security.
- (16) Any measures that may be taken will be proportionate and precisely targeted to the assessed risks of each critical technology area, or of a relevant technology. Any implemented measures will aim at reinforcing the Union's strength in these areas and be designed to minimise any negative spill-over effects on the market and the economy. In particular, these assessments will contribute to the development of Union policies in support of innovation and industrial development for the identified technologies, including through international initiatives.

HAS ADOPTED THIS RECOMMENDATION:

- 1. Out of the list of 10 critical technology areas identified in the Annex, it is recommended, as an initial step, that Member States together with the Commission assess, by the end of 2023, the following 4 technology areas with the highest likelihood of presenting the most sensitive and immediate risks related to technology security and technology leakage:

- (a) Advanced semiconductors technologies

Semiconductors, microelectronics and photonics are essential components of electronic devices in critical areas such as communications, computing, energy, health, transportation and defence and space systems and applications. Due to their huge enabling and transformative nature and their use for civil and military purposes, remaining at the forefront of building and further developing these technologies is crucial for economic security.

- (b) Artificial intelligence technologies

AI (software), high-performance computing, cloud and edge computing, and data analytics have a wide range of dual-use applications and are crucial in particular for processing large amounts of data and making decisions or predictions based on this data-driven analysis. These technologies have huge transformative potential in this regard.

- (c) Quantum technologies

Quantum technologies have a vast potential to transform multiple sectors, civil and military, by enabling new technologies and systems that make use of the properties of the quantum mechanics. The full impact of quantum technologies that are being/will be developed cannot yet be fully qualified.

- (d) Biotechnologies

Biotechnologies have a major enabling and transformative nature in areas such as agriculture, environment, healthcare, life science, food chains or biomanufacturing. Some biotechnologies, such as genetic engineering applied to pathogens or harmful compounds produced by genetic modification of microorganisms, can have a security/military dimension, in particular when being misused.

2. The Commission invites the Member States to engage in an open dialogue on an appropriate calendar and scope for collective risk assessment of other technology areas listed in the Annex, or subsets thereof, having regard to the fast-moving geopolitical environment and to the differing degrees of likelihood that the listed technologies present the most sensitive and immediate risks related to technology security and technology leakage.
3. To structure the collective risk assessment exercise, the following guiding principles have been identified:
 - (a) Identify and analyse vulnerabilities according to their potential impact on the EU's economic security and the degree of likelihood that the negative impact materialises. The analysis should identify the main types of threats and threat actors, and should take into account geopolitical factors where relevant to assess the likelihood of negative impacts. It should also take into account, inter alia, the value chain of the technologies, the evolution of risks as well as relevant technological developments, including any chokepoints and expected future chokepoints, a mapping of the EU's relative position in each technology, including key players and elements of the EU's comparative lead; the global interconnectivity of the ecosystem of the technology, including in research and the supply chain for the technology.
 - (b) At the scoping phase of the collective assessment, regard should be had to whether the detailed assessment will focus on certain, most relevant subsets of technologies.
 - (c) The risk assessment will not be country-specific.
 - (d) Prioritise risks having potential effects on the entire EU.
 - (e) Ensure synergies and complementarities with existing analyses at the EU level and Member State level, to feed into the risk assessment process.
 - (f) Take into account private sector input.
4. The collective risk assessment will ensure the confidentiality, upon request, of inputs received from Member States or private sector. The final outcome document of the collective risk assessment will be classified appropriately.
5. The assessment should be conducted by the Member States and the Commission making use of existing fora, or where necessary new ones, to include relevant experts, as required for each of the critical technologies.

6. The Commission will continue monitoring the technological developments and, if necessary, complement the present Recommendation by proposing additional technologies for further assessment.

Done at Strasbourg, 3.10.2023

For the Commission
Thierry BRETON
Member of the Commission

