Council of the
European Union

Brussels, 25 January 2024
(OR. en)

5832/24

POLCOM 29
COMER 19
RELEX 109
DUAL USE 12
RECH 30
ENER 39
ENV 91

COVER NOTE

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
To:	Ms Thérèse BLANCHET, Secretary-General of the Council of the European Union
No. Cion doc.:	COM(2024) 22 final
Subject:	COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Advancing European economic security: an introduction to five new initiatives

Delegations will find attached document COM(2024) 22 final.

Encl.: COM(2024) 22 final

EUROPEAN
COMMISSION

Brussels, 24.1.2024
COM(2024) 22 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

Advancing European economic security: an introduction to five new initiatives

1. Introduction

Context

On 20 June 2023 the European Commission and the High Representative for Foreign and Security Policy adopted a Joint Communication on a European Economic Security Strategy[1]. Premised on the notion that the EU thrives in an open and rules-based world, the strategy highlighted that new economic security risks are emerging as a result of increasing geopolitical tensions, geo-economic fragmentation and profound technological shifts.

The strategy set out a comprehensive approach to European economic security. In particular, it provides a framework for assessing and addressing - in a proportionate, precise and targeted way - risks to EU economic security, while ensuring that the EU remains one of the most open and attractive destinations for business and investment. In full respect of Member States' prerogatives, the strategy underlined the need to develop a more cohesive and impactful common EU approach.

Recognising that risks to our economic security challenges change over time, linked to the broader geopolitical and geo-economic context, the strategy identified four risk categories to be addressed as a matter of priority, i.e. risks to the resilience of supply chains; risks to the physical and cyber-security of critical infrastructure; risk for technology security and of technology leakage; and risk of weaponisation of economic dependencies or economic coercion.

To address these risks, the Strategy is structured around three pillars:

- *Promoting* the EU's competitiveness and growth, strengthening the Single Market, supporting a strong and resilient economy, and strengthening the EU's scientific, technological and industrial bases.
- *Protecting* the EU's economic security through a range of policies and tools, including targeted new instruments where needed.
- *Partnering* and further strengthening cooperation with countries worldwide who share our concerns and those with which we have common economic security interests.

As part of the rollout of the European Economic Security Strategy, this Communication presents five initiatives to enhance the EU's economic security, while taking stock of the progress made on other work strands.

2. The package

The initiatives proposed today aim at:

(1) improving existing legislation (proposal for a revision of the Regulation on the screening of Foreign Direct Investment);

(2) fostering further discussions within the EU on export controls of dual-use technologies that impact our security (White Paper on Export Controls);

[1] Joint Communication by the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy: European Economic Security Strategy, 26.06.2023, JOIN (2023) 20 final

(3) consulting Member States and stakeholders on potential risks stemming from outbound investments, focusing at this stage on actions needed to enable a better identification of such risks (White Paper on Outbound Investment);

(4) promoting further discussions within the EU on how to better promote research and development involving technologies with dual-use potential (White Paper on options for enhancing support for research and development involving technologies with dual-use potential);

(5) proposing that the Council recommends measures aimed at strengthening research security at national and sector level (Proposal for a Council Recommendation on enhancing Research Security).

Future EU actions will continue to be informed by the on-going risk assessments and by continuous strategic coordination with Member States to reach a common understanding of the risks that Europe faces and of the appropriate actions - under the three pillars of promote, protect and partner - to tackle them.

a. New initiatives related to investment and trade

Proposal for a new regulation on the screening of foreign investments

Regulation 2019/452 establishing a framework for the screening of foreign direct investments into the EU ("FDI Screening Regulation") is in place for just over three years. The Regulation established a cooperation mechanism which has enabled the Member States and the Commission to exchange information on more than 1.200 transactions and flag concerns on foreign direct investments (FDIs) in the single market that present potential risks to their security and public order. It has allowed the Commission and Member States to identify, assess and act on threats resulting from certain investors and cross-border vulnerabilities. As any restrictions are based on a limited and targeted exception justified by security or public order concerns, the regulation has confirmed the EU's overall openness to FDI.

The legislative proposal presented by the Commission today aims at revising this framework, based on an evaluation of the regulation[2]. It builds on the experience of the first three years of operation, as well as an assessment made by OECD experts in November 2022[3], and the findings and recommendations of a special report issued by the European Court of Auditors on 6 December 2023[4].

The proposed regulation will improve the effectiveness of the FDI Screening Regulation by addressing the shortcomings of the current mechanism. It aims to ensure that all Member States have a screening system in place so as to avoid loopholes in the screening of risky transactions, to focus on the cases which present the highest risks and ensure there is greater accountability within the system in respect of the security or public order concerns expressed by Member States and/or the Commission.

The Commission aims to promote greater efficiency in the cooperation mechanism by facilitating convergence of national systems. The proposed regulation also extends the cooperation mechanism to intra-EU transactions where the investor is controlled by a foreign

[2] See the Staff Working Document as part of the package adopted with this Communication.
[3] https://www.oecd.org/daf/inv/investment-policy/oecd-eu-fdi-screening-assessment.pdf
[4] https://www.eca.europa.eu/en/publications/SR-2023-27

company. It would therefore close gaps that may undermine the EU's ability to protect its security or public order.

White Paper on Export Controls

Multilateral Export Control Regimes remain at the heart of the control of dual-use technologies in the EU. As the Economic Security Strategy anticipated, geopolitical tensions and the pace of technological change mean there is a need for more coordinated action at EU level. The EU therefore must make full use of the possibilities under the Dual-Use Regulation. A multiplication of national controls by Member States would risk undermining the effectiveness of the EU export controls framework, of Member States' controls themselves, and the integrity of the Single Market. This risk is more pronounced in the current environment, where divergent approaches of Member States to specific technologies could weaken the security of the EU as a whole.

Improved coordination of export controls at EU level would increase the ability of the EU and Member States to act effectively in a geo-political context, for example by taking the lead in defining a shared agenda with partners. It would also reinforce the EU ability to confront possible unilateral actions by third countries seeking to impose new export controls, including on emerging technologies, or to manage cases of pressure (on the EU or specific Member States) from third countries in response to such controls.

Since the adoption of the Dual-Use Regulation in 2021, the global context for export controls has changed. Russia's war of aggression against Ukraine has been met with rapid deployment of sanctions, including in the form of export restrictions on dual-use and sensitive items. At the same time, the ability of the multilateral export control regimes to take decisions on new items to be subject to controls and to keep pace with technological developments has been hampered as some of their members are blocking the decision-making processes. Furthermore, a united EU voice in the development of future controls on specific technologies has not yet been sufficiently articulated. For these reasons, there is a need to reinforce the EU's ability to act internationally in an effective manner.

The White Paper on Export Controls proposes both short and medium-term actions to address these concerns. In the short term, also to safeguard the important technical work carried out in multilateral regimes, the Commission will make a proposal to introduce uniform EU controls for those items that would have been adopted in the multilateral regimes had it not been for the blockage of the decision-making process within these regimes. The Commission also proposes to create a forum for political coordination, which would allow discussions between the Commission and Member States at an appropriate senior level to foster common EU positions on export controls.

By summer 2024, the Commission will adopt a Recommendation to improve coordination between Member States and the Commission on any new National Control List envisaged by a Member State before adoption, to allow for comments on potential effects beyond that Member State's borders. This would improve the EU capacity to identify risks linked to items which are not yet controlled at the multilateral level.

In the medium term, the Commission will advance the evaluation of the Dual-Use Regulation to the first quarter of 2025 to assess and, subsequently, potentially make proposals to remedy any shortcomings in its effectiveness and efficiency. This evaluation will be supported by a comprehensive study in 2024 and will also draw on the results of the risk assessments of critical technology areas outlined above.

The White Paper should also trigger a broader debate about the type of export controls needed and how to best cooperate internationally to respond to current and future challenges.

White Paper on Outbound Investment

The June Joint Communication on the European Economic Security Strategy recognises the importance of open global markets for the success and economic security of the European Union. It also acknowledges the growing concerns regarding outbound investments in a narrow set of advanced technologies that could enhance military and intelligence capacities of actors who may use these capabilities to threaten international peace and security. While the EU and its Member States already screen foreign direct investments into the EU and control the exports of dual-use technologies outside the EU, there is currently no scrutiny of investments that flow out of the EU to third countries.

In July 2023, the Commission set up an Expert Group on outbound investments with Member States to advance the discussion in these issues. Its preliminary assessment is that more work and analysis are needed for the Commission and the Member States to determine any necessary policy response to these growing concerns.

The Commission now seeks to broaden and structure this discussion on the basis of a White Paper to better understand outbound investments in certain strategic sectors and any potential related risks. The Commission envisages to recommend that this is supported by Member State monitoring and assessment of the current situation. On the basis of this monitoring over a 12 months' period, the Commission, together with Member States, could undertake an assessment of risks to EU security, based on a common methodology, to establish whether and what mitigating measures might be required.

b. New initiatives related to research and innovation

Proposal for a Council Recommendation on Research Security

The proposed Council Recommendation aims at better supporting and empowering Member States as well as higher education institutions and other public and private research performing organisations across Europe to identify and address research security risks. This will help to ensure that research and innovation actions are not misused in ways that affect the EU's security or infringe ethical norms.

While national governments are best placed to support the R&I sector, EU-level cooperation and coordination is needed to ensure a proper functioning of the European Research Area.

Building on the work already done and in line with the principle of academic freedom, the proposed Recommendation aims to mobilise all Member States to create awareness and strengthen resilience in the research and innovation sector. Member States would be recommended to establish a policy framework for research security based on a whole-of-government approach, creating support structures, introducing safeguards through funding organisations, incentivising universities and other public and private research performing organisations to appoint research security advisers and introducing due diligence and risk management processes.

The measures taken by Member States should be proportionate, with emphasis on self-governance by the sector in line with academic freedom and institutional autonomy. The overall approach should be risk based and avoid all forms of discrimination and stigmatisation.

To complement these efforts, the EU would support policy learning, coordination and consistency among Member States, through existing European Research Area governance structures and establishment a European Centre of Expertise on Research Security.

The Commission would monitor the progress in the implementation of this Recommendation as part of the biennial reporting on the Global Approach to Research and Innovation and may, taking into account the evolution of the geopolitical situation, propose further actions.

White Paper for enhancing support for research and development involving technologies with dual-use potential

Many technologies that are critical for the EU's economic security have a dual-use potential: these technologies are relevant for many fields in both civil and defence domains and could benefit European industry and the wider economy. In the face of geopolitical challenges, support for R&D involving technologies with dual-use potential is increasingly relevant.

The White Paper adopted today reviews the support offered under current EU funding programmes and identifies potential options for their enhancement. For example, programmes like the EU Defence Innovation Scheme (EUDIS) under the European Defence Fund (EDF) aim at identifying promising technologies in the civil domain and promote their uptake in the defence domain.

It puts forward three possible options for the future: (1) going further based on the current set-up and strengthening it, (2) removing the exclusive focus on civil applications in selected parts of the successor programme to Horizon Europe, and (3) creating a dedicated instrument with a specific focus on dual-use R&D. With the White Paper, the Commission launches a broad consultation with public authorities, civil society, industry and academia on options for strategic support to dual-use technology development. This consultation will allow a comprehensive dialogue with all parties concerned that will inform the Commission's next steps.

3. Progress on other Economic Security-related work

Since the adoption of the Economic Security Strategy last June, intensive work has continued on the main dimensions of EU economic security.

Risk assessments

On 3 October 2023, the Commission adopted a Recommendation to the Member States **identifying ten technology areas as critical for the EU's economic security.** Four of these technologies were recommended for an urgent joint risk assessment by Commission and Member States[5]: Advanced Semiconductor Technologies, Artificial Intelligence Technologies, Quantum Technologies and Biotechnologies.

The Commission and Member States are currently working on these risk assessments, drawing on inputs from stakeholders, including through the Industrial Forum, with a view to reporting in February. The work on the risk assessments, which focuses particularly on risks to technology security and technology leakage, is complementary to the work of the Commission-run **Observatory of Critical Technologies**, which provides regular monitoring and analysis of critical technologies of the EU defence, space and related civil value chains.

[5] C(2023) 6689 final

The Commission is also continuing work on the three other risk assessments that were identified in the Strategy (i.e. resilience of supply chains; physical and cyber-security of critical infrastructure and weaponization of economic dependencies or economic coercion).

For example, **supply chain risks** are monitored via the Supply Chain Alert Notification "SCAN" analysis to assess strategic dependences and supply chain distress[6]. This risk assessment is based on data-driven methodologies to identify EU strategic dependencies across sensitive industrial ecosystems (i.e. relating to areas like security and safety, the health of Europeans, the green and digital transitions), as well as those dependencies which may represent vulnerabilities to the EU's economic security. The data-driven approach is complemented with an intelligence-based qualitative assessment in order to understand the supply chain implications of disruptive effects affecting particular goods and ecosystems.

As regards the **physical and digital security of critical infrastructure**, the Critical Entities Resilience Directive which entered into force on 16 January 2023 provides for Member States to carry out risk assessments by 17 January 2026 on essential services. The **NIS 2 Directive**[7] provides the framework for coordinated risk assessment on the cybersecurity of critical infrastructure. These risk assessments will also guide the actions set out under the proposed by the Commission in April 2023, and in particular the coordinated preparedness testing.**Cyber Solidarity Act,**

Several assessments have been performed already and some are ongoing: for example, the assessment on 5G[8] and on cybersecurity implications of Open Radio Access Networks (OpenRAN)[9] that will in the coming years provide an alternative way of deploying the radio access part of 5G networks based on open interfaces. As regards critical infrastructures, effective measures to strengthen the security and resilience of submarine cable infrastructures are also key.

The Commission is also working with Member States to assess risk levels and areas of potential **weaponisation of economic dependencies** or **economic coercion**. This assessment looks at potential impacts and likelihood of such practices directed against the EU. It considers various actions that could seek to interfere with the legitimate sovereign choices of the EU and its Member States or otherwise weaponise economic dependencies in relations with the EU.

Risk assessments Where **will contribute to informing decisions on whether further action is warranted.** this is considered necessary, the Commission will, when appropriate in coordination with the High Representative, propose additional actions to be taken to mitigate risks through promoting, protecting or partnering measures.

Research security in current EU funding programmes

As the EU is one of Europe's biggest research funders the Commission has taken action to **boost research security**, by shoring up the application of the existing safeguards to ensure

6 For more details, see SWD(2021) 352 final and Arjona et al. (2023)
[7] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union
[8] Report on EU coordinated risk assessment of 5G (europa.eu)

[9] Cybersecurity of Open Radio Access Networks | Shaping Europe's digital future (europa.eu)

research security, based on a strict risk-based approach. These safeguards aim at protecting the Union's strategic assets, interests, autonomy or security under the Horizon Europe and Euratom Regulations[10]. The EU has also adopted guidelines for research involving dual-use items, to ensure that risks are effectively identified, managed and mitigated by authorities and research organisations[11].

The implementation of these safeguards is being further enhanced in the framework of the Horizon Europe Regulation. Concretely, 31 actions under the 2023-2024 work programme (3.5% of total) have restricted eligibility under Article 22.5 of the Regulation, meaning entities based in, owned or controlled from certain third countries may not participate in such actions. In addition, cooperation with entities based in China has been excluded for innovation actions, under Article 22.6 of the Regulation. The participation of legal entities from Russia and Belarus in all topics under Horizon Europe has been excluded in line with EU sanctions regime[12].

The Commission reinforced its monitoring system for cases of transfer of ownership of results of EU-funded research projects to non-associated third countries. It is also working together with national authorities to determine whether Horizon Europe and Euratom projects comply with applicable security rules, in particular regarding the sensitivity of information.

In addition, the Commission has introduced investment safeguards under the European Innovation Council, to be included in investments in small and medium-sized enterprises (SMEs) and start-ups developing technologies and innovations that may pose risks to economic security, if acquired by non-associated third countries. All of this experience has fed into the preparation of the abovementioned proposal for a Council Recommendation, presented today.

Promoting and partnering

As part of the "promote" pillar of the Strategy and in the broader context of the EU competitiveness agenda, the Commission has strengthened the Single Market and the Union's economic base. Several important steps have been taken to strengthen the resilience of the EU economy and the competitiveness of Europe's economy and industry, including by improving access to finance, implementing important social initiatives of the European Pillar of Social Rights Action Plan and boosting investments and reforms through the roll-out of NextGeneration EU and the Cohesion Funds. Some of these steps that contribute to the EU's economic security are outlined in the (non-exhaustive) examples below.

The **Single Market Emergency Instrument**, once adopted by the co-legislators, will put the EU in a better position to monitor essential goods and services in the context of a crisis and ensure a governance framework for fast collective reactions. The **Critical Raw Materials Act** will ensure the EU's access to a secure, diversified, affordable and sustainable supply of critical raw materials. The **Net-Zero Industry Act** will foster the competitiveness of our industry and facilitate the transition to a net-zero economy. **AggregateEU** will help to diversify energy import sources, whilst the **EU's electricity market design reform** will accelerate the surge in renewables, thus diversifying energy supplies and limiting dependencies.

[10] Regulation (EU) 2021/695 of the European Parliament and of the Council of 28 April 2021 establishing Horizon Europe – the Framework Programme for Research and Innovation, laying down its rules for participation and dissemination, and repealing Regulations (EU) No 1290/2013 and (EU) No 1291/2013.
11 Commission Recommendation (EU) 2021/1700 of 15 September 2021 on internal compliance programmes for controls of research involving dual-use items under Regulation (EU) 2021/821 of the European Parliament and of the Council setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items.
12 Council Regulation (EU) No 833/2014 of 31 July 2014 and Council Regulation (EU) 2021/1986 of 15 November 2021

The upcoming **Advanced Materials for Industrial Leadership Initiative** will foster the production and use of innovative and sustainable materials in the EU. The upcoming **EU Biotech and Biomanufacturing** initiative will promote competitiveness in this critical technology. It will, inter alia, take into account the results of the abovementioned joint risk assessment. The reform of the ,**EU Customs Union** proposed in May 2023, will ensure that customs authorities have tools and resources to properly assess exports and stop imports which are illegal or pose real security risks to the EU, its citizens and its economy.

Progress is also being made on promoting critical technology areas. The Policy Programme**Digital Decade**13 has set the framework for fostering the development and deployment of European strategic digital technologies and services. The **EU Cyber Resilience Act** will ensure that hardware and software products, such as wireless and wired devices, are more cyber-secure for business users and consumers across the Union and will better position EU industry through leadership on related standards.

Political negotiations are ongoing on the **Strategic Technologies for Europe Platform (STEP).** , thisOnce adopted will leverage and steer existing EU instruments to support the development of manufacturing of critical technologies in the Union. The **Chips Joint Undertaking**, inaugurated end November 2023, bridges the gap between research, innovation and deployment, notably through EUR 1.67 billion funding from the EU for four pilot lines.

The EU's **Artificial Intelligence Act**, which was politically agreed in December 2023 will boost investment and innovation across the EU by providing businesses with legal certainty and creating trust for consumers and businesses using AI. It will shortly be complemented by a Commission initiative to enhance the cooperation between AI start-ups and the EU's growing supercomputer capacity and to develop the EU's AI innovation ecosystem. Furthermore, EUR 1.2 bn of state aid by seven Member States has been approved for an **Important Project of Common European Interest** to support research, development and first industrial deployment of advanced cloud and edge computing technologies in Europe. The **Smart Networks and Services Joint Undertaking**, which became operational in 2022, fosters alignment with Member States on 6G Research and Innovation, and the deployment of advanced 5G networks.

As part of the "**partner**" pillar, **the EU has continued to strengthen its engagement with international partners to advance common economic security interests**. This cooperation ranges from ensuring access to raw materials, to understanding critical supply chains, establishing cooperation on emerging technologies in key areas, and reform of the World Trade Organisation.

In 2023 the EU signed **free trade agreements** with New Zealand, Chile and Kenya, as well as the first ever Sustainable Investment Facilitation Agreement (SIFA) with Angola, and finalised negotiations on an agreement with Japan on cross-border data flows.

Work has continued within the **G7 Coordination Platform on Economic Coercion** to share information and better coordinate actions against weaponization of trade and economic coercion. The **G7 Security and Integrity of the Global Research Ecosystem** Working-Group has published best-practices in November 2023 and set up a Virtual Academy to inspire further activities. The G7-initiated Partnership for **Resilient and Inclusive Supply-chain Enhancement** (RISE) aims at supporting low- and middle-income countries in playing bigger roles in the mineral and global clean energy manufacturing industries.

13 Decision (EU) 2022/2481 establishing the Digital Decade Policy Programme 2030

The outcome of the October 2023 **EU-US Summit** underlines the shared interest in reducing excessive dependencies, tackling non-market practices, responding to economic coercion, addressing risks stemming from inbound and outbound investments and strengthening supply chain resilience, to be taken forward under the Trade and Technology Council. The EU and **Canada** have also agreed at their November 2023 Summit to hold regular dialogues on economic security. Likewise, the EU and the **Republic of Korea** agreed in May 2023 to strengthen dialogue economic security. Close cooperation on economic security is also maintained with **Japan** and **India**.

Reflections on how to improve the economic security and resilience of the EU and of its partners have also been integrated in the roll-out of the **Global Gateway**, which is mobilising up to EUR 300 billion in mutually beneficial investment for sustainable development in emerging markets and developing economies. Sustainable critical **raw materials partnerships** with seven countries across three continents, including Chile, the Democratic Republic of Congo and Kazakhstan and **digital economy packages** with Colombia, Nigeria, Kenya, and the Philippines are examples of partnerships the EU has already completed in the context of Global Gateway. These contribute to the partners' economic security while also advancing the EU's strategic interests.

The EU continues to be a strong supporter of a **broad reform of the World Customs Organization**to address more effectively developments in international trade.

The EU is also partnering with a broad range of countries on **research and innovation**, notably by facilitating a multilateral dialogue on values and principles for international science cooperation, on which it will host an international ministerial conference in February 2024. The Commission will also enhance dialogues on economic security concerns with third countries associated with Horizon Europe[14], such as the UK, Canada or New Zealand.

4. Conclusion

The package of proposals and initiatives set out in this Communication represent a further step in implementing the European Economic Security Strategy.

The package presents a comprehensive approach to strengthen the EU toolbox to mitigate risks linked to foreign investments in the EU, to outbound investments, to dual-use goods and to bolsters research security. This strengthening is essential to enable the EU and Member States to address systematically the risks identified in the ongoing risk assessments related to supply chains, technologies, infrastructures and economic coercion.

The Commission invites the Member States, the European Parliament and the Council, in line with their respective competences, to consider these proposals and initiatives, and to give them the appropriate follow up, in close cooperation with the Commission. Given the geopolitical environment, and the opportunities and risks it engenders, it will be necessary to proceed at a steady pace.

Implementing the European Economic Security Strategy is an ongoing process, based on thorough risk analysis, leading to the adoption of targeted measures to address risks, taking into account the evolving nature of the risk environment. Therefore, the Commission will

[14] Currently 19 third countries are associated to Horizon Europe, with the UK, New Zealand, and Canada as the most recent partners. These associations provide, as far as possible, the same rights and obligations to these countries' research and innovation entities as those accorded to entities of EU Member States.

propose in due time and, when appropriate, in coordination with the High Representative, further initiatives to implement the Strategy.