048507/EU XXVIII. GP
Eingelangt am 03/12/25

Council of the
European Union

Brussels, 3 December 2025
(OR. en)

16389/25

POLCOM 368
FDI 58
COMER 182
RECH 543
TELECOM 457
COMPET 1297
DUAL USE 58
RELEX 1623
ENER 647
ENV 1330
IND 580
INDEF 179
CYBER 364
PROCIV 176

COVER NOTE

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
date of receipt:	3 December 2025
To:	Ms Thérèse BLANCHET, Secretary-General of the Council of the European Union
Subject:	JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Strengthening EU economic security

Delegations will find attached document JOIN(2025) 977 final.

Encl.: JOIN(2025) 977 final

www.parlament.gv.at

EUROPEAN COMMISSION

HIGH REPRESENTATIVE OF THE UNION FOR FOREIGN AFFAIRS AND SECURITY POLICY

Brussels, 3.12.2025
JOIN(2025) 977 final

JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

Strengthening EU economic security

www.parlament.gv.at

1. Introduction

The increasingly frequent and targeted use of **economic tools to advance strategic objectives** has become a defining feature of today's geopolitical landscape. From disruptive tariffs and the weaponisation of dependencies to the arbitrary deployment of trade defence measures, major players are using economic levers to pursue their strategic and geopolitical objectives, putting the EU's security, public order, competitiveness and economy at risk.

The risks to the EU's economic security are not new but have recently intensified: vulnerabilities are now more visible, more pressing, and more difficult to overlook. These risks include:

- a growing **instability in the global trade and investment environment**, marked by the rise of disruptive trade measures and export restrictions to weaponise dependencies;
- a proliferation of **predatory practices** targeting critical supply chains and technologies, undermining our industrial base, some of which (such as State-funded overcapacities) creating new dependencies;
- the continued deterioration of the security landscape, including in the context of Russia's continuing **war of aggression against Ukraine** and the rise in hybrid attacks.

The 2023 **European Economic Security Strategy** set out the EU's initial response to these challenges.[1] It outlined a series of actions – grounded in risk assessments – to strengthen the EU's economic security by **promoting** competitiveness, **protecting** against risks and **partnering** with those who share our concerns. These three pillars remain at the core of our economic security approach and the Commission together with Member States work to integrate them into any policy considerations and actions. Moreover, economic security is essential for the EU to maintain its values, its principles and the wellbeing of its citizens, as well as to reinforce our economic independence.

However, since the adoption of the 2023 strategy, the need for the EU to act with greater boldness, speed and unity has become even stronger. This Communication outlines a more strategic and assertive use of the Union's tools – complementing their original policy objectives - to support Europe's economic security, which concerns the Union's ability to ensure security, alongside other objectives, through a strong, dynamic and resilient economy by anticipating, deterring and responding to potential or actual threats, linked to the EU's economic relationships with the wider world. The EU can do this, in particular, by ensuring it stays ahead in terms of critical technologies, industries and services. It reflects a **paradigm shift**, moving from a reactive posture towards a more proactive and systematic deployment of our toolbox. Moreover, in certain cases, the EU, its Member States and industry will increasingly need to be ready to accept economic costs for the benefit of reduced vulnerabilities and enhanced overall security.

This call to action includes **improving** information gathering, monitoring and analysis, as well as the capacity to anticipate emerging threats; **deterring** third countries from

[1] JOIN(2023) 20 final.

www.parlament.gv.at

weaponising the Union's dependencies; **reducing** our exposure to third countries that may weaponise such dependencies; and **preventing** efforts to undermine our derisking actions.

Importantly, this call to action also recognises the need to **play to the EU's strengths** in terms of, among others, the unparalleled weight of the EU's single market, our technological and industrial capabilities as well as access to EU funding and programmes. This includes identifying, the EU's economic opportunities as well as those areas where others are dependent on the EU. Therefore, this communication makes the case for **an integrated, whole-of-government and business approach, improved governance** as well as **even closer cooperation with like-minded partners and, where appropriate, joint action.** It is complementary to the comprehensive EU Preparedness Union Strategy. The EU's economic security is underpinned by that of its Member States. It is also intrinsically linked with its broader relations with the world and therefore the Common Foreign and Security Policy, which will be used more systematically to support the stated objectives.

On this basis, anchored in a risk-based analysis, this Communication focuses on six high-risk areas outlined in Section 3, applies the tools at our disposal and outlines how they can be further improved.

2. A proactive approach to economic security

The EU has a wide range of tools that contribute to its economic security. It must now deploy them **more strategically, efficiently and proactively** to strengthen its economic security. While most of these tools were not originally developed with economic security in mind, they are nevertheless highly relevant to advance the Union's economic security objectives.

A non-exhaustive list of key tools is set out in *Figure 1*, and their coordinated application further articulated in *section 3*.

www.parlament.gv.at

Figure 1: List of tools which support economic security, non-exhaustive

To advance the EU's economic security, the Commission will deploy these tools, in coordination with Member States, as follows:

- **Trade and competition tools** will be used to gradually reduce the EU's exposure to risks and to prevent the EU's derisking objectives from being undermined. This includes expanding diversification opportunities and thus our broader security under EU trade agreements, making strategic use of customs toolbox and addressing distortions caused by foreign subsidies, both within the Single Market and through subsidies or dumped imports.
- **Resilience and cybersecurity** tools will focus on preparing for and managing emergency situations, as well as on reducing exposure to external threats, such as cyberthreats.
- **Security and public order tools** will be used to reduce the EU's excessive exposure to risks to, inter alia, ensure the normal functioning of society, while supporting actions aimed at developing its position in critical technologies and industries, as well as preventing its derisking objectives from being undermined.
- **Anti-coercion and restrictive measures** will aim at deterrence and dealing with situations where third countries attempt to coerce the EU as well as shielding the EU's businesses from extraterritorial measures imposed by third countries and, where relevant, triggering a change in behaviour of the country concerned.
- **Funding and restrictions** through EU tools like the NDICI (Global Gateway), Horizon Europe, NextGenerationEU, InvestEU, Digital Europe Programme, Connecting Europe Facility, Instruments for Pre-Accession Assistance (IPAs), Growth Plans for the Western

www.parlament.gv.at

Balkans and Moldova, as well as the Ukraine Facility, EU4Health and the future European Competitiveness Fund should strengthen the EU's economic security or, as a minimum, not weaken it, in line with the programmes' rules.

- **Sectoral initiatives** – will be used to build up the EU's own capacity and strategic capabilities in the high-risk areas identified in the risk assessment process.

Close cooperation and coordination with countries that assign similar importance to economic security and a rules-based global order, is more important than ever. The EU will work to strengthen **international cooperation on economic security issues**, particularly with **trusted partners**, including through **focused economic security dialogues conducted both bilaterally and in plurilateral settings.** Such cooperation will support joint action on shared economic security interests or concerns. It will also deepen the collective understanding of risks, help anticipate threats, enable the design of mitigation measures that **minimise negative externalities**, contribute to building and maintaining reliable and resilient supply chains in key strategic sectors, and help to avoid negative impacts on our like-minded international partners.

The Commission will seek cooperation with third countries, bilaterally, through the G7, and in frameworks such as the Comprehensive and Progressive Trans-Pacific Partnership and other relevant fora. It will work with partners on the development and deployment of economic security standards for resilient supply chains. Closer cooperation may include **coordinated deployment of tools** and coalition building with partners who share similar economic security objectives or face similar challenges.

Deploying economic security standards

Building on work in the G7 on standards-based trade, the Commission will encourage the development and use of economic security standards. They will be:

→ focused on action to diversify critical supply chains by creating the conditions for new suppliers to enter the market or limiting access of dominant suppliers;

→ guided by the principles of transparency, interoperability and compliance with international rules;

→ targeted and tailor-made, factoring in the specific risks, economic impacts and business realities of each supply chain.

This work will focus as a matter of priority on critical raw materials and semiconductor supply chains, while exploring further collaboration in other areas.

The relevance of, and impact on, the EU's **neighbourhood and enlargement policy** must also be adequately factored in. Risks and opportunities for the EU's economic security will be integrated in the Commission's implementation of policies and programmes with these regions. Candidate countries are on a path to become future EU Member States; their alignment on economic security policy as well as gradual integration into the Single Market, is essential to ensure their successful accession, while enhancing the EU's ability to address both existing and new risks. It is therefore important that candidate countries reflect the EU's economic security approach and, where appropriate, gradually align with EU legislation of relevance to economic security objectives.

3. Advancing Europe's economic security: high-risk areas

www.parlament.gv.at

The 2023 Strategy launched risk assessments covering supply chain resilience and energy security, critical infrastructure, weaponisation of economic dependencies, and technology security and technology leakage. Four critical technologies – AI, quantum technologies, semiconductors, and biotechnology - have already been assessed. Building on this work, the Commission has identified **six high-risk areas** where it will concentrate its efforts in immediate to short term, in close cooperation with Member States, industry and trusted partners. At the same time, the Commission will continue to monitor developments and, where needed, assess and act on newly emerging high-risk areas.

Overview of six high-risk areas

3.1. Strengthening supply chain resilience and counteracting high-risk dependencies in critical goods and services

Non-cumulative indicators of a high-risk dependency:
- 60% or more of EU supply is controlled by a single third country or operators;
- input/service has systemic value for the EU's economy due to their role in multiple sectors, e.g. critical raw materials, semiconductors;
- input/service is critical to the EU's defence industry/strategic capacities or specific critical technology supply chains, such as clean energy technologies;
- the third country has already weaponised economic dependencies or threated to do so, e.g. through export restrictions;
- there is already non-market overcapacity or it is being created.

The risk. Modern economies are deeply interconnected and rely on a wide range of inputs, intermediate goods and essential services from partners globally. In some cases, supply is highly concentrated – often in countries that do not share the same strategic interests and that have the capability and willingness to increase and weaponise such dependencies. These risks to the EU's supply chains are particularly visible in our reliance on certain **critical raw, processed and advanced materials, clean tech components,** and **mainstream semiconductors**, as well as in **financial services, pharmaceuticals, aeronautics, digital and space technologies**. They are also

www.parlament.gv.at

visible in the **agri-food sector**, where the Vision for Agriculture and Food[2] sets out the need to reduce strategic dependencies, notably where the EU relies on a handful of partners for imports of feed and feed additives as well as fertilisers.

High-risk dependencies can: (i) be **weaponised** for coercion purposes (e.g. critical raw materials, mainstream semiconductors, advanced materials, energy products, threats of disabling certain services); (ii) create **systemic economic vulnerability** or systemic risk to public order and public health protection in crises (e.g. personal protective equipment, critical medicines supply, food supplies); (iii) create the risk of large-scale, cross-sector disruption (e.g. by penetrating telecom networks, reliance on a single cloud provider, kill switches of digital services); (iv) **affect the EU´s competitiveness, slowing down the green and digital transitions** if supply is disrupted (e.g. batteries, permanent magnets, clean tech products and components, advanced materials); (v) affect Member States's autonomy to develop and operate **military capabilities**; or (vi) threaten EU's food sovereignty.

Application example: mainstream semiconductors

Risk: structural reliance on a single third country supplier for the manufacturing of essential low margin chips puts several European industries at risk. Such semiconductors form a critical part of multiple supply chains.

Use of tools: the Commission will work with trusted partners to diversify sources of supply and will seek to encourage the ramping up of production within the EU. The upcoming revision of the Chips Act will set out effective mitigation measures. The cyber security of imported mainstream semiconductors used in security-related applications should be further assessed under the Cyber Resilience Act.

Objective. The Commission and Member States will seek to **minimise the potential for short-term disruption** while putting in motion measures to **progressively reduce current high-risk dependencies in the single market and counter efforts to create new ones**. It will use its tools to monitor the supply chain, create a framework to support supply diversification and prevent the undermining of EU action by addressing distortions of competition in the single market. Actions in the context of advancing towards the Circular Economy will also play an important role.

The Commission will take the necessary action to ensure its alternative supply chains are not being undermined by dumping and price manipulation.

The Commission will assist Member States in deploying fully and effectively existing tools, notably the resilience criteria that will have to be applied as of January 2026 by Member States in public procurement, auctions and public support schemes under the Net Zero Industry Act.

The Commission will also take measures to both develop the **EU's internal capacity and capability** and to diversify supply **through cooperation with partners, including by building on its extensive network of trade agreements and other forms of bilateral and**

[2] COM/2024/75 of 19 February 2025.

www.parlament.gv.at

plurilateral forms of cooperation. This will include considering the production of certain critical products in our candidate countries and our partner countries more broadly, including with regions, such as the Middle East and North Africa. This will reinforce the resilience of the EU's diversified supply chains and open further opportunities for EU businesses. The Commission will continue to identify and continuously monitor supply chain vulnerabilities and **high-risk dependencies** through its risk assessment process and engagement with Member States and industry. .

3.2. Attracting value-added inbound investment that reinforces the EU's economic security

The risk. Inbound investments boost EU resilience and competitiveness by creating jobs, developing industrial capabilities, tapping into financing and scale, supporting innovation and technology transfer. However, certain forms of inbound investments may pose risks. The risks include: (i) risks to **security and public order**, including access to sensitive data (e.g. geo-localisation, biometric data, trade secrets), access to critical infrastructure, access to dual-use and other critical technologies; and (ii) **economic resilience risks**, such as deeper dependencies or a single point of failure in critical supply chains controlled by high-risk entities or third countries which undermine our economic security interests (e.g. batteries, CRM, software and components), which render the EU vulnerable to economic disruptions or weaponisation; and (iii) **low competitiveness challenges,** such as lack of technological transfer, limited added value creation (e.g. assembly lines only), hiring workers from the investing country and thereby impacting, among others, the local labour market.

Objective. The Commission's focus will be on ensuring that the EU remains open and attractive to foreign investments. It will seek to balance this openness, where necessary for the EU's economic security, against the need to avoid deepening dependencies or creating new ones. Moreover, it is crucial to preserve the ability of EU companies to innovate, including through foreign acquisition of key intellectual property from emerging champions, and ensuring security of supply and continuity of service. The Commission will use its tools and initiatives to set out and implement targeted measures such as inbound investment conditioning that encourage technology transfer for entities in countries that purposefully undermine our economic security.

Example: battery electric vehicles (BEVs)

Risk. The dominant position of certain suppliers of BEVs and strict controls on the technologies needed for BEV production risk undermining the key role of the automotive sector in the EU economy, while benefiting from the EU market. There are also inherent cybersecurity risks associated with connected vehicles.

Use of tools: The Commission is exploring ways in which value-added investments can be encouraged, including through the use of trade and competition policy initiatives. It will continue monitoring trade flows and deploy its risk mitigating toolbox to de-risk connectivity elements, support investment in the next generation of BEV technologies to ensure Europe remains resilient and competitive and where necessary limit exposure to high-risk entities in relevant connected components of BEVs. The Commission will also incentivise the sharing of technology and related know-how that can strengthen the EU's economic security objectives.

www.parlament.gv.at

3.3. Supporting a vibrant defence and space industrial base and other high-risk industrial sectors

The risk. Russia's war of aggression against Ukraine, rising geopolitical tensions and policy-driven action to weaponise trade dependencies highlight the importance of investing in a vibrant domestic industrial base, notably in the defence and space sectors as well as strategic dual-use sectors, such as transport (e.g. aviation, aeronautics, shipbuilding and ports), that fuels the EU's economy and supports its strategic autonomy. Risks in this area include: (i) insufficient (internal) investment; (ii) low production volumes combined with insufficient procurement of domestic technology for institutional infrastructure; (iii) third-country non-market policies and practices that lead to distortions in global and regional markets; (iv) unjustified or disproportionate export controls from third-countries imposed on European products and technologies (extraterritoriality of third-country export regimes); (v) loss of ownership and control due to foreign acquisitions, including in certain cases through portfolio acquisitions; (vi) rigid regulatory framework and fragmented capital markets that neither facilitate flow of funds nor promote the start-up and scale-up of high-risk / high-reward technologies with dual-use capabilities.

Application example: Key components for drones and counter drones systems

Risk: Dependence on third-countries suppliers for key components of drones, batteries and counter drones systems; extremely short innovation cycle to keep drone solution operationally effective, based on real battlefield experience (counted in months sometimes in weeks).

Use of tools: the Commission will use its tools under the European defence industrial programmes to secure EU-made production capacity and the shortening of innovation cycles for drone technologies based on real operational experience. It will continue to strengthen cooperation and information exchange on a voluntary basis between relevant bodies (e.g. national procurement agencies, international procurement organisations - OCCAR, EDA, NATO) and within European defence industrial programmes instruments/actions. In order to ensure supply chain resilience, it will establish targeted mapping of supply chains for specific products and equipment, including dual-use items, and support production through co-investment.

Certain components in critical sectors such as defence are sourced from high-risk entities, which could prevent the access to and use of **defence equipment, dual use technologies and military mobility assets** if a situation of geopolitical tension arises. Moreover, it is crucial that the EU maintains a highly skilled workforce and does not fall behind the innovation curve in the technologies underpinning strategic sectors. Effectively mitigating these risks by swiftly mobilising targeted and effective tools is essential for defence and military capabilities in the EU.

Objective. The Commission will use its tools to maintain and develop strategic manufacturing capacity and capabilities in the EU, notably by: (i) promoting and, where relevant, derisking public and private **investment**; (ii) **supporting demand** (incentives) also through aggregation or joint purchasing; (iii) **preventing the relocation** of strategic capabilities and sectors; (iv) **phasing out potentially hostile actors** from defence and other critical supply chains including limiting the procurement of restricted critical defence and space technologies from outside the EU; (v) mitigating **threats posed by foreign direct investments** into companies supplying critical

www.parlament.gv.at

products or technologies, (vi) **support the development of critical technologies, components and materials** in the EU following long term objectives as well as their domestic procurement for institutional infrastructures; (vii) ensuring that EU **start-ups and businesses** have the conditions needed to scale up, for example, through adequate financing and via a temporary favourable tariff treatment for certain inputs as well as a favourable capital markets ecosystem.

The priority will be to support the **defence and space industrial base**. While the immediate focus will be on the specific high-risk situations identified in the risk assessment process, the Commission will closely monitor from an economic security perspective all key industries such as clean tech, energy and energy-intensive and circular industries, agri-food, digital and electronics, aviation (incl. aeronautics), shipbuilding, automotive and health.

3.4. Developing and maintaining leadership across critical technologies

The risk. Certain third countries and businesses have demonstrated their interest in acquiring control of nascent or advanced EU technology and know-how. In some instances, such actions have been aimed at compromising the Union's ability to compete in the technology. They are pursuing this aim by, for instance, acquisitions, R&D cooperation, reverse engineering, or industrial espionage. It is also done by artificially taking market share away from more innovative companies, which in turn results in less revenue for them to invest in cutting-edge R&D. In the long term, the EU's economic performance, security and geopolitical standing will depend on maintaining and developing our technological capabilities. Therefore, preserving EU capabilities across these technologies, by enhancing dedicated EU funding tools and addressing technology security and leakage, is of strategic importance. At the same time, a close attention must be paid to the increasingly fragmentated implementation and enforcement of dual-use export controls.

Application example: quantum

Risk: Foreign state-backed or high-risk entities seek access to EU quantum computing, communication, and sensing know-how and infrastructures via investments, acquisitions or R&D partnerships, accelerating sensitive military/intelligence uses abroad and eroding EU technological sovereignty.

Use of tools: the Commission will continue to map key EU quantum actors/infrastructures and track foreign investments, partnerships and IP flows to feed FDI screening, export control and research-security risk assessments. It will use its tools to investigate investments that pose risks and to work with Member States to coordinate rapid responses to attempted hostile takeovers or leakage cases. In order to support economic security objectives, it will prioritise EU/like-minded funding and suppliers for critical quantum components and services, and limit reliance on high-risk quantum/cloud providers in sensitive sectors. It will further seek to ensure that entities under undue foreign influence cannot access sensitive quantum projects.

Objective. The Commission will use its tools to support a positive framework environment to for the development of critical technologies in the EU and prevent action that undermines the EU's efforts by addressing distortions. It will monitor market developments and provide further support for research and innovation in the EU by start-ups and scale-ups, established businesses, research and

www.parlament.gv.at

innovation organisations and academia. It will focus on ensuring the industrial deployment and valorisation of RDI achievements in the single market's industrial base. The 28th regime, providing businesses with a single, harmonised set of EU-wide rules for company formation, governance, mobility and access to finance, will strengthen the EU's economic resilience by enabling more secure cross-border operations and more robust, diversified supply chains.

The Commission will advance research and innovation security and take the flanking measures needed to mitigate the risk of leakage of technology or know-how, for example through predatory acquisitions, R&D cooperation and investment in strategic and emerging EU markets in sensitive destinations or sectors while continuing to promote trusted international research and innovation partnerships that are crucial for the Union's economic security objectives. It will explore how to ensure that businesses and research and innovation organisations in the EU can scale up and avoid acquisitions/ownership transfers exclusively driven by insufficient financing opportunities from trusted sources. At the same time, the Commission will seek to prevent access by high-risk entities to Union supported actions in the critical technology sphere, which can potentially be weaponised against the EU.

3.5. Prevent access to sensitive information and data that could undermine the EU's economic security

The risk. Third countries gain access to sensitive information/data of the EU or its Member States, either as a result of industrial espionage, their supply of hardware or software used in certain products (e.g. connected vehicles, 5G/other telecommunication systems, electricity grid infrastructure, DNA sequencing platforms) or due to their ownership and control of certain businesses possessing sensitive information/data (e.g. port, airport and traffic operators, financial networks, AI models, data portals, telecom, personal data or sensitive market information). There are clear implications on security and public order, further compounded by potential economic impacts, for example linked to the fragmentation of supply chains. In the energy sector, for example, this risk extends to the acquisition by non-EU investors of EU companies that hold advanced technologies for monitoring and processing operational data from critical energy infrastructure.

Objective. Lower and where possible eliminate the risk of access by high-risk entities and related entities to sensitive information/data of

Example: detection equipment at EU borders (ports, airports, land borders etc.)

Risk: lack of common practice across the EU, dependency on a single or limited number of suppliers, unauthorised access (including through authorized channels, e.g. maintenance) that impacts the performance of the detection equipment and the integrity and/or confidentiality of related sensitive information, vulnerability to malware that could compromise or distort the related information/systems/networks through the equipment

Use of tools: based on the cybersecurity risk assessment under the NIS2 Directive, the Commission will seek to mitigate identified risks through the identification of high-risk suppliers, use cybersecurity certification schemes, strengthening cybersecurity standards and embedding security requirements in procurement calls for tenders. The Commission will assess the potential role of foreign subsidies in giving competitive advantage to certain suppliers.

www.parlament.gv.at

the EU or its Member States and thereby limit the potential negative impacts on the EU economy and security. Attention will also be given to the risk potentially posed by foreign workers in strategic sectors and foreign students at higher education, including in Science, Technology, Engineering, and Mathematics (STEM) in line with relevant procedures.

3.6. Prevent and mitigate disruptions to EU critical infrastructure affecting the EU economy

The risk. The EU's critical infrastructure - including critical transport, space systems, energy and communications infrastructure, in particular those that are identified as strategic to military mobility - being disrupted by foreign actors, which could lead to cascade effects on the European economy. The focus will be on ensuring the stability of services provided. Disruptions could occur through physical-, cyber- or hybrid-attacks, including the sabotage of entire facilities or their parts/subcomponents. They could also be linked to ICT supply chains, which underly critical components or services to critical infrastructures. There is also a risk of pre-positioning of high-risk third countries and operators in the EU's critical infrastructure with a view to gaining the capacity to disrupt them (when and if needed). In addition, there is a reputational and credibility risk if certain infrastructure is threatened or actually impacted. Finally, there is a risk linked to third countries taking a leading role in setting international standards, which may affect critical infrastructure.

Example: solar inverters

Risk: increasing reliance on a single supplier; cyber risks - manipulating electricity production parameters, preventing electricity production, access to operational data, infiltrating supply chain actors.

Use of tools: the Commission will continue to assess cyber risks through a coordinated assessment under the framework of the NIS2 Directive (to be concluded in 2026). On this basis it will deploy mitigation measures focused both on strengthening preparedness (e.g. Electricity Risk Preparedness Regulation, Critical Entities Directive) and to address identified vulnerabilities through for example: certification and standardisation under the Cyber Resilience Act and non-price criteria under the Net-Zero Industry Act. The Commission will monitor market developments and seek to prevent or mitigate high-risk investments. The Commission will continue to assess the role of foreign subsidies that may distort the level playing field in solar energy markets, notably through subsidised imports.

Objective. In line with relevant EU strategies for defence, internal security and preparedness, to enforce existing rules to lower the risk of data leakage/espionage and of physical and cyber-disruption, notably by: (i) **limiting ownership/control/operation by high-risk entities** of European critical infrastructure; (ii) increasing **physical protection** measures; (iii) **limiting cyber-vulnerabilities**; and (iv) **limiting dependencies on single suppliers or high-risk suppliers**, as well as concealed vulnerabilities, backdoors or potential systemic ICT supply disruptions, particularly in cases of technological lock-in or supplier dependency; (v) **reserving critical EU manufacturing capacities** with the potential to scale up in times of global supply chain disruptions or health crises; (vi) the Commission will **prevent access by high-risk entities to Union supported actions**, including those actions supported by public financial institutions and instruments; ; (vii) support the **development of trusted suppliers of**

www.parlament.gv.at

critical subcomponents in the EU and in trusted third countries so that there are viable alternatives; (viii) supporting **flagship initiatives** in defence and related domains (Eastern Flank Watch, European Drone Defence Initiative).

4. Actions to strengthen EU economic security

Access to quality information and its thorough analysis is the starting point for an effective and well-informed EU economic security policy and decision-making. The risk assessment system launched by the 2023 Strategy will remain at the heart of these efforts. The existing assessments will be updated, deepened, and complemented by new ones across critical technologies and supply chains.

The Commission will further develop its economic security information gathering capability. It will speed up the **mapping of strategic dependencies along value chains that lead to vulnerabilities for the Union's economy** and strengthen **monitoring and anticipation of third country actions** to create new dependencies or sustain existing ones.

Furthermore, the success of the EU's economic security policy will depend on **greater coordination both at EU level and with Member States**. This includes building a common understanding of the economic security threats, identifying concrete risks, and developing mitigation measures. This should be underpinned by better information flows, a full understanding of the costs and benefits of EU action, and a willingness to act jointly when needed, putting the EU in a position of strength. The Commission has taken the necessary internal organisational steps. But this also requires a new way of working with Member States, and increasingly among and within the Member States themselves, especially with regards to policy areas that are increasingly strategic but have been traditionally decentralised such as research and innovation.

The EU will continue to engage closely with **industry,** by ensuring secure information exchange and a more structured engagement. Industry is in the front line of the EU's economic security. Businesses must become more resilient and diversify their critical supply chains, notably by eliminating a complete reliance on a single high-risk supplier. It is also crucial to integrate in their business models the costs that come with greater diversification recognising the benefit that resilience to geopolitical risks brings. This must be a **two-way process** and **a responsibility that must be shared between the public and private sector,** allowing policymakers to improve the EU's threat assessment and business intelligence capacity and equip it for action, while helping industry to pursue company-level mitigation measures.

The Commission, supported by the High Representative, will:

→ Improve its information **gathering and analysis capacity** by advancing risk assessments more rapidly on specific critical supply chains, critical infrastructure and critical technologies, and launching regular **calls for evidence** to obtain industry and stakeholder input into supply chain vulnerabilities and exposure to external pressure.

→ Promote greater **coordination and information exchange through its Economic Security Network with Member States.** The Commission will use the Network to

www.parlament.gv.at

promote scenario development, align understanding of threats, risks and scope for mitigation, facilitate information exchange and support implementation, particularly in the use of the tools that are in the remit of Member State responsibilities. In this context, the Commission will ensure that there are suitable information systems available to support the **rapid and secure exchange of classified information among and with Member States** on economic security issues – including on risk assessments, critical and high-risk entities, and transactions of potential concern. This will complement the work of the EU stockpiling network, which focuses on ensuring the supply of essential goods in crisis situations.

→ Create an **Economic Security Information Hub** where with the support of EEAS, INTCEN/SIAC[3], the EU's Delegation network and Member States, as well as existing Single Market economic monitoring tools like the Supply Chain Alert Notification (SCAN); it will map and consolidate available information under existing public and private mechanisms and coordinate the collection of additional information relevant for economic security. This will include a **market monitoring mechanism** to collect information on developments in high-risk areas, including rapid information on trade flows in sectors subject to diversification to ensure that EU action isn't undermined. It will also consolidate information **on high-risk entities** to support the process of assessing eligibility for EU funding and participation in an EU investment or procurement process. In addition, the European Customs Authority and the EU Customs Data Hub would allow to efficiently **support and enforce the implementation of the related EU economic security initiatives** facilitating also the exchange of relevant information.

→ Intensify **structured engagement by EU Delegations**, liaising with Member State Missions, other EU bodies and the EU business community present in third countries; to ensure effective contributions to risk assessments, monitoring and mitigation with regard to economic security, including by facilitating business-to-business and business-to-government exchanges.

→ Assess by Q3 2026 the extent to which the Internal Market Emergency and Resilience Act (IMERA) allows to gather company level supply chain information from businesses in high-risk sectors. In light of this analysis, the Commission will assess the necessity for further measures.

→ Recommend that Member States nominate senior-level **National Economic Security Advisers** responsible for cross-government coordination of economic security risk assessment and mitigation. The Commission will promote greater policy coordination and joint actions by **regularly bringing these advisers together**. It also invites the Council of the EU to consider regularly convening the relevant Council formations for political-level

[3] The EU Intelligence and Situation Centre (EU INTCEN) at the European External Action Service is part of the EU's Single Intelligence Analysis Capacity (SIAC), and is the civilian intelligence centre of the EU, providing in-depth analysis for decision makers in all EU Institutions.

www.parlament.gv.at

discussions.

→ Create a **trusted adviser group drawn from EU business representatives** to, among others, advise on specific risks and potential responses as well as discuss de-risking strategies. The Commission will regularly invite industry representatives to participate in sector-specific discussions of the Economic Security Network and, where relevant, debrief European Commissioners.

→ Set up a **Trade Resilience Information Portal** to provide EU businesses with up-to-date information, as part of the Access to Markets (A2M) portal, on export restrictions and other restrictive measures imposed by third countries, as well as on the potential risks linked to the need to build EU resilience.

→ Expand the **Observatory on Critical Technologies** to identify, monitor and analyse the defence and space industry and related supply chains, and to cover emerging technologies and to support implementation at EU and national level of the resulting EU technology roadmaps.

→ Use the future **Centre of Expertise on Research Security** to promote research security and increase the research community's resilience, including by developing a due diligence platform to support universities in choosing their international partners.

→ Explore ways to align and **integrate candidate countries with our economic security approach**, especially in those areas where their economic security vulnerabilities can pose a security risk to the EU.

Building on a strengthened analysis and governance, the EU can better pursue its economic security objectives by (i) clarifying and improving the deployment of existing tools and (ii) developing new tools where needed.

First, the **Commission will adapt how it uses some of its tools** to make them more effective in managing economic security risks and will seek to improve coordination between these tools.

The Commission will take the following steps to improve the use of tools:

→ EU funding:

- Going forward, the Commission will **incentivise in its funding activities projects that support the EU's economic security.**
- In particular it should mobilise a sufficient level of funding for reducing dependencies of critical technologies, components and materials especially in strategic sectors as space and defence, including to fully implement the Observatory for Critical Technologies' (OCT) technology roadmaps.
- The Commission, Member States and implementing partners should seek to prevent access by high-risk entities to sensitive Union supported actions. Article 136 of the Financial Regulation provides a horizontal legal base to protect the EU's security and public order when the Commission and implementing partners

www.parlament.gv.at

implement the EU budget. This allows preventing high-risk entities from benefitting from EU funds as well as restricting access to EU funds in the strategic sectors and areas of critical technology and infrastructure by entities coming from third countries which undermine the EU economic security interests. For the avoidance of doubt implementing partners should refrain from supporting projects that contradict the above, including in operations at own risk. To that end and to ensure better policy alignment between EU programmes and economic security aims guidance will be made available in Q1 2026, thereby supporting the development of a more cohesive and effective approach. Furthermore, the Commission will encourage the Member States, the **EIB group and other IFIs/national promotional banks and institutions that are implementing national or EU budgets** to prioritise support to EU businesses that reduce foreign dependencies in critical sectors, especially for specific projects, critical technologies and critical infrastructure identified as high-risk. Similarly, third-country high-risk suppliers should be prevented from accessing EU and national funding where those third countries, based on specific criteria, are identified as undermining EU economic security interests.

→ FDI screening:

- Develop **guidelines** drawing on the experience of implementing the current FDI Screening Regulation to ensure national screening authorities approach screening consistently, including in strategic sectors. The guidelines would also set out how to take account of the potential cumulative risk of multiple investments. This will be complemented by guidance on the interplay between any EU level requirements and the application of national screening mechanisms in the financial sector.

→ Export Controls of Dual-Use items:

- Carry out an **overall evaluation** of the Dual-Use Export Control Regulation. As part of this evaluation, the Commission will assess whether the Regulation achieves its objectives in the context of the new geopolitical and geoeconomic realities, including the impacts of increasing recourse to unilateral controls that may also impact the Single Market. It will continue exploring with Member States how to efficiently adopt European controls in emerging technology areas in this new context. During the evaluation process, the Commission will ensure active outreach to stakeholders from the Member States, industry, research institutes and academia.

→ Trade defence instruments:

- When a case of relevance for the EU's economic security is initiated, **the EU's economic security will be reflected in the conduct of the investigation and in the design of possible measures**.

→ Internal Market, Customs and Competition tools:

- Make full use of the **Foreign Subsidies Regulation** to maintain fair competition in

www.parlament.gv.at

areas where foreign subsidies lead to distortions that pose economic security risks.

- Encourage Member States to make full use of existing State aid possibilities, such as the Clean Industrial State Aid Framework, the Regional Aid Guidelines, the Research Development and Innovation framework, the General Block Exemption Regulation and important projects of common European interest as instruments to build greater resilience.
- **Review the use of strategic customs instruments (tariff suspensions, autonomous quotas) for key inputs** with the view to support the competitiveness of Union enterprises.

Second, the Commission will **develop new measures** to advance the EU's economic security.

The Commission will:

→ Explore putting in place on a pilot basis an **EU-level start-up monitoring mechanism aimed at identifying startups in critical technology areas that are vulnerable to the risk of hostile foreign acquisitions**, redirecting them to EU investment alternatives and other forms of support (e.g., advisory, capacity-building, matchmaking with investors). The mechanism would work in lockstep with existing initiatives, such as the EU Startup and Scaleup Strategy.

→ Work with supervisory authorities to monitor **portfolio investments,** (that fall outside the scope of the FDI coordination mechanism), in areas identified as high-risk for economic security purposes.

→ Include an economic security component for key strategic sectors in the upcoming **Competitiveness Coordination Tool.**

→ Strengthen the EU's industrial base and supply chains resilience through the **Industrial Accelerator Act**.

→ As outlined in ResourceEU, further develop **secondary markets** for critical raw materials, including through the Circular Economy Act, to make it easier to finance strategic CRM projects in areas identified as high-risk for economic security purposes.

→ Assess by Q3 2026 ways of **strengthening the protection of the industry from unfair trade policies and negative global market developments, such as overcapacity**. Here, the Commission will evaluate the effectiveness and adequacy of the existing tools and consider the necessity of possible new measures.

→ Review the **Blocking Statute** to simplify its application and reduce compliance costs for EU persons and businesses and create a credible deterrent against the extra-territorial application of third-country sanctions. This will strengthen European economic security by better protecting EU operators from conflicting third-country measures and by ensuring a more predictable, effective and assertive framework.

→ Explore the modalities of encouraging companies in specific high-risk sectors to ensure that **supplies are sourced from at least two different suppliers** and limit exposure to a

www.parlament.gv.at

single dominant supplier.

→ Explore the scope to provide **financial support to companies subject to FDI screening decisions** in situations where their financial viability may be at risk absent an investment, without prejudice to State aid rules.

→ As part of the review of the Public Procurement Directives, **propose European preference criteria in specific strategic sectors** in which our public procurement stimulates demand for European industrial leadership, increases our resilience and mitigates risks for security.

→ Incentivise companies to **reduce dependencies in emerging technology areas** as part of the upcoming Chips Act 2.0, Quantum Act, Cloud and AI Development Act and Commission Strategy on Open Source.

→ Use the upcoming review of the **Cybersecurity Act** to enact at EU level restrictions on access of high-risk suppliers to critical infrastructure.

5. Conclusion

The EU remains firmly committed to open and rules-based trade, investment relations and international cooperation. It will therefore continue to support and benefit from open trade and investment with partners around the world. At the same time, in today's geopolitical environment, safeguarding the EU's economic security is imperative. Addressing the risks that come with openness is key to preserving it, as well as our broader security and the competitiveness of our industry.

The EU already has many tools at its disposal to pursue this goal. These instruments must now be used strategically and, where needed, further improved, both to credibly deter threats to the EU's economic security before they arise and respond effectively when they do. Achieving this requires the Commission, European Parliament and Member States to work in lockstep and to cooperate closely with industry, towards an efficient and informed decision-making.

The EU is determined to make a more proactive, strategic and coordinated use of all available tools to build a strong, secure and resilient economy for the long term, and to operate effectively in the new geopolitical and geoeconomic conditions shaping global trade.

www.parlament.gv.at