



ANALYSIS

De-risky business

EU risk assessments
for economic security

September 2026

Executive summary

In recent years, economic security has become a central policy priority for the European Union (EU). Geopolitical tensions, supply-chain disruptions and concerns over technology leakage and economic coercion have prompted the EU to develop new methods for assessing risks arising from international trade, investment and technological interdependence. This analysis examines the EU's emerging framework and policies for economic security risk assessments. It finds that the EU has made progress in identifying vulnerabilities related to supply chains, critical technologies and strategic dependencies. New methodologies and monitoring initiatives have strengthened the EU's understanding of these risks and increasingly underpin policies aimed at enhancing resilience and reducing vulnerabilities.

At the same time, important challenges remain. While existing approaches have improved the mapping of structural dependencies, they are less suited to anticipating future risks arising from geopolitical developments, technological change and the behaviour of foreign actors. The next phase of the EU's economic security agenda should therefore focus on strengthening governance mechanisms, intelligence-sharing and strategic foresight. In particular, the EU should move from periodic assessments towards more continuous risk intelligence, improve coordination between the Commission, member states and national authorities, strengthen cooperation with the private sector, and promote greater coherence across risk-assessment frameworks and policy instruments. Closer cooperation with trusted partners and through international fora such as the OECD could further strengthen methodologies and support a shared understanding of economic security risks.

Table of contents

Executive summary	2
1 Introduction	4
2 The EU's policy framework for economic security risk assessments	5
2.1 Supply chain resilience.....	6
2.2 Weaponisation of economic dependencies or economic coercion.....	8
2.3 Technology security and technology leakage	9
2.4 Systematic risk intelligence and foresight.....	10
3 Risk assessments in the EU's risk-mitigating policies	12
4 Discussion.....	15
5 Conclusion and policy recommendations.....	18
6 References	20
Sammanfattning på svenska <i>Summary in Swedish</i>	23

This analysis was written by Hannes Berggren, with valuable contributions and comments from Edvin Johannessen and Kristina Olofsson.

1 Introduction

Recent geopolitical tensions, supply chain disruptions and the increasing strategic use of economic measures have drawn attention to vulnerabilities arising from international trade and investment relationships. While interdependence remains an important source of productivity, lower costs and wider access to goods and services, recent developments have shown that dependencies can also create risks. This has prompted governments worldwide to focus more closely on economic security and resilience, including the identification and management of vulnerabilities linked to international trade and investments.

Within the European Union, these concerns have created a growing policy agenda on economic security, de-risking and crisis preparedness. Since 2023, the European Commission has developed a range of initiatives to identify, assess and mitigate risks associated with dependencies. Risk assessments have become an increasingly important tool in this process. They are used not only to improve the understanding of potential vulnerabilities, but also to inform policy interventions designed to reduce or manage those risks. Given their growing influence on policymaking, such assessments must be proportionate, effective, high-quality, evidence-based and conducted systematically and coherently across the EU.

This analysis maps the EU's approach to risk assessments related to economic security and evaluates their effectiveness, proportionality and precision. It draws on publicly available information and input from public- and private-sector stakeholders. The analysis begins by outlining the EU's methodologies and initiatives for risk assessments. The next section maps selected risk-mitigating policies that include risk assessment mechanisms and criteria. This is followed by a discussion evaluating the EU's approach and, finally, a conclusion with policy recommendations.

2 The EU's policy framework for economic security risk assessments

In response to growing economic security, resilience and geopolitical imperatives, the EU has launched several initiatives for assessing risks to supply chains, resources, infrastructure and technologies. The Economic Security Strategy of 2023 stated that the Commission and EU member states would deepen their analysis of critical supply chains, including through stress tests, to establish the level of risk (European Commission, 2023a).

Four broad categories of risks to economic security were identified:

1) resilience of supply chains, 2) physical and cyber security of critical infrastructure, 3) technology security and technology leakage; and 4) weaponisation of economic dependencies or economic coercion.

These risks, it was established, could materialise along the entire value chain, from knowledge creation and basic research to commercialisation and manufacturing at scale. Accordingly, and of relevance to this analysis, the European Commission and the High Representative were expected to:

- Develop a framework for assessing risks affecting the EU's economic security together with member states. This included establishing a list of technologies critical to economic security and assessing their risks with a view to devising appropriate mitigating measures.
- Engage in structured dialogue with the private sector to develop a collective understanding of economic security and encourage due diligence and risk management in light of economic security concerns.
- Instruct the EU Single Intelligence Analysis Capacity (SIAC) to work specifically on detecting possible threats to EU economic security.

The European Commission's (2025a) Communication on Economic Security further underlined that access to reliable information and analysis is a prerequisite for EU economic security policy. The risk assessment framework introduced by the 2023 Economic Security Strategy would be developed through updated and new assessments of critical technologies, supply chains and infrastructure. The Commission also stated that it would strengthen its capacity to identify strategic dependencies, monitor third-country actions and anticipate vulnerabilities affecting the Union's economy.

The Communication further stressed the need for closer coordination between the Commission and member states, including through an Economic Security Network (ESN) and an Economic Security Information Hub.¹ These mechanisms, it stated, were intended to support common threat assessments, scenario planning and the

¹ The Economic Security Network is a coordination mechanism that brings together the European Commission and member states to support information sharing, joint risk assessments and coordinated responses on economic security. The Economic Security Information Hub is a platform intended to collect, integrate and analyse information on economic security risks to support evidence-based policymaking.

implementation of mitigation measures. The Commission also proposed stronger engagement with industry, including regular calls for evidence, a trusted adviser group and a Trade Resilience Information Portal to improve information flows on supply-chain risks and third-country restrictions.

The approach assigned responsibility to both public authorities and businesses. Companies were expected to strengthen resilience by diversifying critical supply chains and reducing dependence on high-risk suppliers, while public authorities were advised to use industry input to improve risk assessments and policy responses. The Commission also planned to assess whether further measures were needed to collect company-level supply-chain information, expand the Observatory on Critical Technologies² to cover emerging technologies and defence- and space-related supply chains, and encouraged member states to appoint National Economic Security Advisers.

Of the four risk categories, assessments have been carried out for 1) resilience of supply chains and 4) weaponisation of economic dependencies or economic coercion. For 3) technology security and technology leakage, assessments have been partially completed, while for 2) physical and cyber security of critical infrastructure, information on progress remains more limited. Accordingly, this section outlines the approaches used for categories 1, 4 and 3, in that order. It then maps EU initiatives to monitor risks more systematically and continuously.

2.1 Supply chain resilience

The first of the four areas assessed under the 2023 Strategy was supply chain resilience. This built on an approach the EU had initiated after the Covid-19 pandemic to quantitatively assess supply-chain vulnerabilities using trade data. The European Commission (2021; 2022a) developed a method for evaluating strategic dependencies, starting with a bottom-up mapping of extra-EU imports of more than 5,000 products³. That methodology consists of two steps. First, a quantitative screening exercise identifies import dependencies on non-EU countries. Product groups are classified as dependencies when imports are highly concentrated among a small number of suppliers, when a large share of imports originates outside the EU, and when imports exceed the EU's own export capacity, indicating limited ability to replace foreign supply with domestic production. Applying these criteria identifies 390 product categories as import dependencies. The second step assesses whether these dependencies are strategic. This qualitative evaluation focuses on products within sensitive ecosystems and considers their relevance to EU strategic interests, including security, public health, and the green and digital transitions. The analysis identifies 137 strategic dependencies, representing just over 6 per cent of the EU's imports from non-EU countries in 2018. These are concentrated in raw materials, chemicals,

² The Observatory on Critical Technologies (OCT), co-led by DG DEFIS and the JRC, monitors critical technologies and related supply chains, providing analysis and risk assessments to support EU policymaking, initially in the space and defence sectors with a longer-term ambition to expand to civil technologies.

³ At the six-digit level using the international nomenclature of the Harmonized System (HS6)

pharmaceuticals and technology components, and are sourced primarily from China, Vietnam and Brazil. A subset of 34 product categories is considered particularly vulnerable because diversification or substitution opportunities are limited.

Arjona et al. (2023) have refined the European Commission's original methodology while retaining its two-step structure. Their updated approach uses trade data that more accurately identify the true country of production rather than transit locations. They also apply the methodology across multiple years to distinguish structural dependencies from temporary fluctuations, and supplement fixed thresholds, above which products are deemed dependencies, with a ranking method to better identify the most significant dependencies and reduce the influence of arbitrary cut-off values. These refinements aim to improve the accuracy of dependency assessments and reduce the risk of over- or underestimating vulnerabilities. Applying the updated methodology identifies 204 strategic dependencies at the HS6 level, accounting for approximately 9 per cent of the EU's total imports from non-EU countries. More than 70 per cent of these product categories also appear in the European Commission's original list of strategic dependencies.

Bonnet et al (2026) have further refined the methodology by including production data instead of using export data as a proxy for EU production. They also calibrate thresholds using a data-driven method rather than relying on more arbitrary cut-off values. This produces a larger number of foreign-dependent products: 835 instead of the 390 products originally identified in 2021. Of these, 378 goods are deemed to belong to strategic ecosystems such as energy-intensive industries, digital, aerospace & defence, health and renewables.

In a similar vein, the National Board of Trade (2026a) has developed and applied a quantitative method for identifying strategic dependencies in Swedish imports from third countries. Using a four-step screening process, the method identifies 818 import dependencies, of which 323 are classified as strategic, 97 as vulnerable, and 47 as particularly vulnerable. The results show that Sweden's most vulnerable dependencies are concentrated in intermediate goods used in industrial production, particularly advanced technologies, chemical products and critical raw materials, and become increasingly concentrated on China and the United States when diversification opportunities and supply-related risks are considered. Based on these findings, the report recommends a systematic approach to mapping strategic dependencies, including enhanced methodological coordination within the EU, improved trade and supply-chain statistics, more coherent national approaches to identifying strategic sectors and products, and better tools for capturing indirect dependencies in global value chains. It also emphasises the need to complement quantitative analysis with qualitative assessments and close cooperation between public authorities, businesses and other stakeholders.

Several other initiatives also track supply-chain risks. The External Vulnerability Index (EXVI) is a composite indicator developed by DG GROW to measure external vulnerability across products, sectors, supply chains and entire economies. The index combines two dimensions of vulnerability: exposure arising from foreign dependencies, measured through the concentration of trade flows and reliance on

external suppliers and markets; and vulnerability stemming from a weak position in global markets, assessed through indicators such as price competitiveness and comparative advantage. The resulting index ranges from 0 to 1, with higher values indicating greater vulnerability to external shocks. Since its development, the EXVI has been adopted as a key performance indicator in the Annual Single Market and Competitiveness Report and the Clean Industrial Deal (Arjona et al, 2025).

The Joint DG GROW-EIB Supply Chain Survey is an annual survey of approximately 850 EU importers and exporters designed to provide firm-level insights into supply-chain management, sourcing strategies, diversification efforts, exposure to disruptions and adjustment measures. By collecting information on trade obstacles, supply-chain tensions and business expectations, the survey complements quantitative monitoring tools with direct evidence from a sample of firms. Recent findings indicate that supply-chain disruptions remained significant in 2024, although less severe than in 2023, with particular challenges related to raw materials, semiconductors and logistics. The survey also highlights the role of intra-EU trade in mitigating external shocks and shows that firms exposed to imports from China are more likely to report supply difficulties. It further provides insights into business responses, including supplier diversification and investments in supply-chain monitoring tools (Arjona et al, 2025).

2.2 Weaponisation of economic dependencies or economic coercion

This category focuses on how economic dependencies may create vulnerabilities that third countries could exploit for strategic purposes. The EU's assessment framework seeks to identify dependencies that are both economically significant and difficult to replace, while also considering the broader implications disruptions could have for the EU's economy, security interests and societal functioning. The analysis extends beyond trade in goods to encompass a wider range of economic relationships and enabling systems that are important for economic activity and resilience.

The assessment combines quantitative and qualitative analysis to identify potential vulnerabilities, evaluate the circumstances under which dependencies could create risks, and assess the possible consequences of disruption. It draws on a range of economic, technological and geopolitical information, as well as lessons from previous cases in which economic relationships have been used for strategic purposes. The approach recognises that dependencies do not automatically constitute risks and therefore considers both the nature of the dependency and the broader context in which it exists. Overall, the analysis appears to suggest that vulnerabilities are often linked to concentrated dependencies on certain partners and limited diversification options rather than to economic openness as such, which is in line with previous research (see, e.g., National Board of Trade 2025a).

Accordingly, the Communication from 2025 proposes several indicators. These include that a dependency may be considered high-risk if a single third country or operator controls 60 per cent or more of EU supply, if the relevant good or service has systemic importance for the EU economy, if it is critical to defence, strategic capabilities

or key technology supply chains, if the supplying country has previously weaponised economic dependencies or threatened to do so, or if the market is characterised by existing or emerging non-market overcapacity. These indicators are non-cumulative, meaning that the presence of any one may be sufficient to warrant further attention from an economic security perspective (European Commission, 2025a).

2.3 Technology security and technology leakage

In addition to the Strategy, the European Commission (2023b; 2023c) adopted a Recommendation on critical technology areas for the EU's economic security to guide further risk assessments carried out jointly with member states. The Commission Recommendation identified ten critical technology areas for the EU's economic security: (1) advanced semiconductors technologies, (2) artificial intelligence technologies, (3) quantum technologies, (4) biotechnologies, (5) advanced connectivity, navigation and digital technologies, (6) advanced sensing technologies, (7) space and propulsion technologies, (8) energy technologies, (9) robotics and autonomous systems, and (10) advanced materials, manufacturing and recycling technologies. These areas were selected for their strategic importance, potential dual-use applications, and relevance to the EU's long-term competitiveness, resilience and security.

The Commission's Recommendation stated that risk assessments should identify and analyse vulnerabilities based on both their potential impact on EU economic security and their likelihood of occurrence. To this end, they should consider factors such as threat actors, geopolitical developments, technology value chains, supply-chain chokepoints, the EU's competitive position, and the global interconnectedness of technology ecosystems. The assessment was recommended to focus on risks with EU-wide implications, build on existing analyses at both EU and national levels, incorporate input from the private sector, and avoid country-specific assessments.

Thus far, risk assessments have been conducted for four critical technologies: advanced semiconductors, artificial intelligence technologies, quantum technologies and biotechnologies (European Commission 2023b; 2023c; 2025a). According to stakeholders consulted for this analysis, the first round of technology risk assessments highlighted some challenges associated with conducting complex assessments across multiple technologies, institutions and member states. They pointed in particular to the importance of clear methodologies, effective coordination and access to relevant information. These experiences appear to have informed ongoing efforts to refine the assessment process and further develop the EU's approach to technology risk assessments.

In addition, assessments for the other six technologies⁴ remain to be completed. The next phase of technology risk assessments appears to focus first on selected segments within these technologies, after which the European Commission will likely continue to scope risks in the remaining technology areas and progressively launch additional

4 Advanced connectivity, navigation and digital technologies, advanced sensing technologies, space and propulsion technologies, energy technologies, robotics and autonomous systems, and advanced materials, manufacturing and recycling technologies.

assessments. Compared with the first round, the approach is therefore more targeted, concentrating on specific technological domains rather than broad categories. The Commission also seems to be seeking to identify potential mitigation measures earlier in the assessment process, rather than treating risk identification and policy responses as entirely separate stages (see e.g. European Commission, 2025a).

2.4 Systematic risk intelligence and foresight

Several noteworthy initiatives have been developed in recent years to strengthen the EU's ability to monitor risks continuously. One is the European Commission Strategic Foresight Reports (see, e.g., European Commission, 2025b). Launched in 2020, these annual publications explore possible future developments, emerging risks and strategic opportunities facing the European Union. Their purpose is to assess how policy can remain robust across different scenarios and support long-term strategic planning. In addition, the Economic Security Strategy established that the EU will enhance its Single Intelligence Analysis Capability (SIAC) to improve its ability to detect threats to EU economic security (European Commission, 2023a). SIAC, which is located at the External Action Service (EEAS), consists of both the civilian EU Intelligence and Situation Centre (EU INTCEN) and EU Military Staff Intelligence (EUMS INT).

The Supply Chain Alert Notification (SCAN) method is an early-warning system developed by DG GROW to identify signs of supply-chain disruptions using high-frequency customs data. It monitors changes in import prices and quantities in near real time to detect potential mismatches between supply and demand. The method uses two indicators to detect supply-chain anomalies: prices rising while import volumes fall, indicating possible supply bottlenecks; and prices increasing faster than import volumes, suggesting that supply is not adjusting sufficiently to meet demand. SCAN is complemented by information on strategic dependencies to assess whether emerging disruptions affect products already identified as vulnerable. The methodology has been applied to monitor critical raw materials used in green technologies and semiconductor supply chains, and has informed other Commission monitoring initiatives, including the implementation of the Chips Act and efforts to track trade-diversion risks (Amaral et al, 2022; Arjona et al, 2025).

The Preparedness Union Strategy proposes a comprehensive EU risks and threats assessment, a crisis dashboard for decision-makers and a stronger Emergency Response Coordination Centre. The strategy also emphasises crisis monitoring, coordination between EU and national authorities, and improved anticipation of cross-border and cascading risks. Relevant assessment factors include interactions between risks, effects on vital societal functions, civil-military coordination, and the ability of authorities to respond to crises. Its role is therefore to support risk identification, situational awareness and coordination, rather than to impose specific obligations or quantitative thresholds (European Commission, 2025c).

The Observatory of Critical Technologies (OCT) and the Raw Materials Information System (RMIS) are two other EU initiatives that support supply chain resilience, risk assessment and strategic foresight. The OCT focuses on identifying, monitoring and assessing critical technologies and their associated supply chains, particularly in the

defence, security and space sectors, providing analyses and risk assessments that help identify technological vulnerabilities and emerging strategic risks. RMIS performs a similar function for raw materials and associated value chains, offering data, analysis and foresight on issues such as supply risks, resilience, circularity and sustainability across the full material life cycle. Together, these initiatives strengthen the EU's capacity to understand strategic dependencies, anticipate future vulnerabilities, monitor developments in critical supply chains, and provide the evidence base needed to support economic security, industrial policy and long-term resilience planning (European Commission, 2026b; 2026c).

On the governance of risk assessments, the Communication of 2025 mentions several initiatives at various stages of development (European Commission, 2025a). The Economic Security Network (ESN) is a coordination mechanism between the European Commission and member states intended to strengthen cooperation on economic security matters. According to the Communication, the Network will support the development of common threat assessments, scenario planning, information exchange and the implementation of mitigation measures, particularly in areas where member states have primary responsibility. It is also intended to facilitate the secure exchange of classified information on risk assessments, high-risk entities and transactions of concern, thereby helping to build a shared understanding of economic security risks and supporting more coordinated EU and national responses.

The Economic Security Information Hub is envisaged as a central platform for collecting, consolidating and analysing information relevant to EU economic security. Supported by the EEAS, EU INTCEN, the EU Delegation network, member states and existing monitoring tools such as SCAN, the Hub will bring together information from public and private sources and coordinate the collection of additional data where needed. Its functions will include monitoring developments in high-risk sectors, tracking trade flows in areas subject to diversification efforts, consolidating information on high-risk entities, and supporting assessments related to EU funding, investment and procurement decisions. The Hub is also intended to improve situational awareness and strengthen the analytical basis for economic security policymaking across the EU.

The Communication also proposes that member states appoint senior-level National Economic Security Advisers responsible for coordinating economic security risk assessments and mitigation measures across government. The Commission intends to bring these advisers together regularly to strengthen policy coordination, facilitate information exchange and support joint action on economic security issues across the EU. In parallel, the Commission plans to establish a trusted adviser group composed of representatives from European businesses to provide expertise on specific risks, possible policy responses and de-risking strategies. Industry representatives will also be invited to participate in sector-specific discussions within the ESN, reflecting the Commission's objective of creating more structured cooperation between public authorities and the private sector in identifying, assessing and managing economic security risks.

3 Risk assessments in the EU's risk-mitigating policies

Building resilient supply chains has become a key EU policy objective (National Board of Trade, 2025b). Accordingly, several policy instruments have been developed in recent years to mitigate risks to the EU's economic security. Several of those instruments include mechanisms to track, monitor or assess risks, and are therefore outlined in this section.

The Critical Raw Materials Act (CRMA) establishes a framework for monitoring and assessing risks related to the supply of critical and strategic raw materials. The Act requires the Commission to monitor supply chains and assess supply risks, taking into account factors such as the concentration of supply, import dependencies, production capacities and the availability of alternative suppliers. It also provides for stress tests of strategic raw material supply chains and requires certain large companies manufacturing strategic technologies to assess vulnerabilities in their supply chains. To evaluate and strengthen resilience, the Act sets several benchmarks for 2030: at least 10 per cent of the EU's annual consumption of strategic raw materials should be extracted within the Union, at least 40 per cent should be processed within the Union, and at least 25 per cent should come from recycling. In addition, the EU should not source more than 65 per cent of its annual consumption of any strategic raw material from a single third country at any relevant stage of processing (European Commission, 2024b). Under the RESourceEU Action Plan, the proposed European Critical Raw Materials Centre is intended to develop systemic intelligence on critical raw material value chains and markets, monitor strategic projects, and support EU and national actions on investment, stockpiling and joint purchasing (European Commission, 2025d).

The European Chips Act establishes mechanisms for monitoring risks and disruptions in semiconductor supply chains. The Act requires the Commission, member states and the European Semiconductor Board⁵ to monitor the semiconductor ecosystem, including supply and demand conditions, production capacities, dependencies, bottlenecks and potential shortages. The information collected should be used to identify vulnerabilities and assess risks to the security of semiconductor supply. The Act also creates an early-warning and crisis-response system that can be activated when significant disruptions are identified (European Commission, 2023d). Unlike the CRMA, the Chips Act does not establish quantitative thresholds for acceptable levels of dependency. Instead, it defines criteria for assessing risks, including the severity of supply disruptions, their expected duration, the strategic importance of affected semiconductor products, and the likely economic effects on critical sectors and value chains within the Union.

The proposed Chips Act 2.0 would develop the EU's approach to mapping and monitoring risks in semiconductor value chains from a primarily crisis-oriented system into a more permanent framework for information gathering and market

⁵ The European Semiconductor Board is a Commission-chaired coordination body composed of representatives of the member states that supports the implementation of the EU Chips Act, including semiconductor supply-chain monitoring.

monitoring. A central element of the proposal is an industry-led information-sharing platform through which companies operating along the semiconductor value chain, as well as semiconductor users, would be expected to contribute data and, in return, gain access to aggregated market insights. At the same time, the Commission would receive expanded powers to use the platform and collect information for strategic mapping, monitoring, pre-crisis assessment and crisis management, including before a crisis has emerged (European Commission, 2026c).

Beyond sector-specific initiatives such as the CRMA and the Chips Act, the EU has developed broader policies to identify and manage risks related to security, resilience and strategic dependencies.

The Internal Market Emergency and Resilience Act (IMERA) establishes procedures for identifying and responding to disruptions that may affect the functioning of the internal market and its supply chains. The Act provides for contingency planning, risk monitoring and information exchange between the Commission and member states. When a serious threat to the internal market is identified, a vigilance mode may be activated, enabling closer monitoring of supply chains for goods and services considered important in the circumstances. The Commission may also request information from economic operators concerning production capacities, stock levels, shortages and supply constraints to assess risks and support coordinated responses. Rather than defining resilience through quantitative thresholds or indicators, such as a dependency above 60 per cent constituting a vulnerability, IMERA sets out the procedural conditions under which different levels of EU coordination and emergency response may be activated where an internal market emergency exists or is imminent. These include the existence of a serious threat or disruption with the potential to affect the free movement of goods, services or persons, create shortages of crisis-relevant goods or services, or significantly impair the functioning of the internal market (European Commission, 2024a).

Several other policies are also noteworthy. The FDI Screening Regulation enables member states and the Commission to assess foreign investments against criteria such as their effects on critical infrastructure, critical technologies, critical inputs and sensitive information (European Commission, 2019; European Commission, 2026d). Following risk assessments for the first four technologies, the European Commission has also issued a recommendation for member states to screen outbound investments in semiconductors, artificial intelligence and quantum technologies (European Commission, 2025e). The Dual-Use Regulation requires authorities to assess security, non-proliferation, human rights and diversion risks when authorising exports of sensitive technologies. The European Commission's 2024 package of new initiatives for economic security suggested discussions on enhancing cooperation and coordination among member states on export controls (European Commission, 2024c). In the digital domain, the Cyber Resilience Act requires manufacturers to assess and mitigate cybersecurity risks throughout the lifecycle of products with digital elements, while the NIS2 Directive requires essential and important entities to conduct cybersecurity risk management, including assessments of supply-chain vulnerabilities (European Commission, 2022b; 2024d). The EU 5G Toolbox complements these instruments by providing a framework for assessing risks

associated with 5G suppliers and technologies, including risks related to third-country interference and excessive dependence on individual vendors (European Commission, 2020). Moreover, for future policies, the European Commission is currently exploring the development of a diversification instrument (European Commission, 2026e).

Together, these measures illustrate how the EU's policy toolbox increasingly incorporates risk assessment and monitoring mechanisms related to economic security across a range of domains. In addition, the EU's risk assessments underpin a growing set of industrial policies that, beyond the already mentioned policies for chips and critical raw materials, include proposals for an Industrial Accelerator Act, ResourceEU and Quantum Strategy (European Commission, 2025a). Ensuring that the various risk assessments and criteria are effective, proportionate and precise is therefore a high priority. The next chapter discusses whether and how the EU's risk assessment approaches could be improved in that regard.

4 Discussion

The EU has made progress in assessing risks stemming from its **supply-chain dependencies** and risks related to the **weaponisation of economic dependencies or economic coercion**. The EU's methodology for identifying strategic dependencies has been refined several times since it was first introduced after the Covid-19 pandemic. The results of these assessments point to risks in particular inputs such as critical raw materials and chemicals, rather than in consumer goods, and to dependencies on specific trading partners. Methodological improvements from Bonnet et al (2026) and the National Board of Trade (2026a) could further improve the accuracy of existing methods, for example by including production data. The same applies to implementing the National Board of Trade's (2026a) policy recommendations, especially on improved and harmonised approaches to methodology and statistics across member states.

In addition, the European Commission and member states could further strengthen understanding of reverse dependencies – which may give rise to so-called strategic indispensability – by integrating them more fully into risk assessments. Another logical next step would be to ensure more continuous monitoring and intelligence, so that emerging risks related to new products and growing trade dependencies can be understood before they materialise.

Regarding **technology security and technology leakage**, four risk assessments have been undertaken, with six more underway. The assessment process thus far appears to have contributed to a shared understanding of economic security risks within the EU and encouraged earlier and more systematic discussions of potential vulnerabilities and mitigation measures. Going forward, more emphasis will likely be placed on improving the qualitative side of risk assessments. This would probably entail a more granular understanding of the risks associated with specific technologies, infrastructures and identified critical inputs, including services. It would also entail a better understanding of reverse dependencies that can create strategic indispensability. As such, moving forward with the remaining risk assessments on technology security and technology leakage, as well as physical and cyber security of critical infrastructure, will be important.

While the EU has made considerable progress in developing methodologies, cooperation fora and policy instruments for economic security risk assessments, important **governance challenges** remain. The EU's approach combines a Commission-led policy process with assessments that depend heavily on information, expertise and implementation by member states. This reflects the division of competences in economic security, where trade policy falls largely within EU competence, while national security remains primarily the responsibility of member states (Jarlebring, 2026). As a result, the quality and usefulness of risk assessments depend not only on analytical frameworks, but also on effective coordination between EU institutions, member-state authorities and private actors. The approach therefore needs further development, supported by clear rules on the collection, sharing and use of information, while ensuring proportionality, confidentiality and trust among participants. The establishment of an Economic Security Network (ESN) and an Economic Security Information Hub, together with national economic security

advisers and structured engagement with industry, may help support more consistent risk assessments, better situational awareness and a more coordinated approach to economic security across the Union (European Commission, 2025a).

A particular governance challenge concerns **access to intelligence** (National Board of Trade, 2025b). Many of the risks that economic security policies seek to address are linked to geopolitical developments, foreign state behaviour and national security considerations. The Nexperia case, where the acquisition of a strategic semiconductor producer raised national security concerns only after the transaction had taken place, caught EU member states and the European Commission unprepared and led to supply chain disruptions (García-Herrero, 2025). This illustrates the difficulty of identifying security risks before they materialise and raises questions about whether existing assessment frameworks are sufficiently forward-looking. While economic dependency mapping can identify structural vulnerabilities and thereby guide de-risking efforts, it is less suited to anticipating strategic behaviour by foreign actors. This points to a continued need for contributions from national security and intelligence authorities, as well as stronger mechanisms for information sharing between member states and EU institutions. The Economic Security Network and Economic Security Information Hub may represent steps in this direction, but such platforms should also support more systematic scenario planning, stress testing and foresight exercises. In addition, EU member states may wish to consider whether pooling more resources to strengthen SIAC, or exploring mechanisms to improve intelligence-sharing between national security agencies while respecting member-state competences, could further improve the EU's joint capacity to anticipate economic security risks. The ESN and member states' single points of contact could help facilitate such exchange and overcome the underlying competences challenge.

Another challenge relates to **the role of the private sector**. Firms make sourcing, investment and technology decisions daily and often possess information unavailable to public authorities, for example on the complexity of supply chains. Effective risk assessments therefore require structured cooperation between governments and industry, in addition to robust quantitative analyses and intelligence. At the same time, policymakers must recognise the limits of supply chain knowledge and avoid assuming that vulnerabilities can be fully understood and mitigated by the public sector.

Private-sector participation appears to have been hampered in the first batch of risk assessments because firms found it difficult to provide requested information without compromising trade secrets and other valuable information. For the second batch of assessments, the European Commission seems to have moved from broad questionnaires towards more targeted information collection through engagement with selected companies and experts. This shift may improve the quality of information gathered. However, it also raises questions about representativeness, sample bias and the potential influence of vested interests. From a political economy perspective, less competitive firms may have a greater incentive to engage in risk assessment exercises as a way to seek protection from foreign competition. Going forward, a key issue will be how to **improve private-sector participation while ensuring that input is representative** and does not create a biased sample based on vested interests.

In this regard, it will be important to carefully analyse any potential incentive schemes for private -sector participation, whether financial⁶ or in the form of influence.

The EU should also be **careful that new regulation mandating** companies to hand over information does not hamper their competitiveness by increasing the administrative burdens. A parallel can be drawn with the regulatory burden of overlapping reporting requirements for cybersecurity, which was described ahead of the Omnibus simplification drive (see Digital Europe, 2024). The EU should learn from these experiences and avoid creating overlapping reporting burdens in the evolving field of economic security. In that regard, it will be important to harmonise the information-collection approaches of various risk assessments. Moreover, the different mechanisms and criteria for assessing risks in policies such as the Chips Act, IMERA and CRMA could benefit from a collective overview aimed at improving harmonisation across policies. One opportunity to do so is the upcoming diversification instrument currently being developed (European Commission, 2026e).

While there is a recognised need to swiftly understand and mitigate risks to the EU's economic security, the process **must remain evidence-based**. The EU should avoid adopting new policies to mitigate risks that have not yet been mapped using an evidence-based approach. In addition, new policies should rely not only on economic security risk assessments, but also on economic analyses and wider impact assessments.

Finally, while a more in-depth comparison with other countries' approaches to risk assessment is outside the scope of this analysis, the focus of EU risk assessments overlaps in several instances with that of partner countries such as Japan, the UK, Canada and Australia. While the priority is to strengthen the EU's own capacity to assess risks, deepening **cooperation with key economic security partners** is a natural next step. For example, Japan has worked in this field for longer than the EU and would therefore be a useful partner for closer cooperation on developing risk assessment frameworks and methods, undertaking joint scenario exercises and stress-testing. Likewise, international fora with key partners, such as the OECD, could help develop more sophisticated and harmonised methodologies for assessing risks (National Board of Trade, 2026b).

6 As suggested by Arcesati & Gehrke (2024)

5 Conclusion and policy recommendations

The EU has made progress in developing tools, methodologies and institutions for assessing risks related to economic security. Compared with a few years ago, the Union now has a better understanding of strategic dependencies, supply-chain vulnerabilities and technology-related risks. At the same time, economic security remains an evolving field. New technologies, geopolitical developments and forms of economic coercion continue to create potential vulnerabilities. Developing the EU's risk assessment framework should therefore be understood as a continuous process rather than a one-off exercise.

Move from periodic assessments to continuous risk intelligence. The next stage of the EU's economic security agenda should focus on strengthening its ability to forecast and monitor emerging risks as close to real time as possible. Existing tools for dependency-mapping provide valuable insights into structural vulnerabilities but are less effective at identifying future risks. The EU should therefore invest further in strategic foresight, scenario planning, stress testing and early-warning capabilities, while strengthening bodies such as SIAC, the Economic Security Information Hub and sector-specific monitoring systems.

Strengthen governance and information-sharing across the EU. Effective risk assessments depend on close cooperation between the European Commission, member states and relevant intelligence authorities. The Economic Security Network (ESN) and national economic security advisers provide an opportunity to develop a more coherent governance framework. Particular attention should be given to improving the exchange of information and intelligence relevant to economic security while respecting confidentiality and national competences.

Develop structured partnerships with the private sector. Businesses often possess information about supply chains, technologies and market developments that is unavailable to public authorities. The EU should therefore continue developing mechanisms for structured engagement with industry while minimising administrative burdens and protecting commercially sensitive information. The objective should be to improve the quality of risk assessments with as few additional reporting requirements as possible. It is also essential to ensure that the sample of private-sector views is representative and does not merely reflect the views of particular vested interests.

Promote coherence across risk assessments and policy instruments. Economic security considerations are increasingly embedded in a wide range of EU policies, including critical raw materials, semiconductors, investment screening, export controls and cybersecurity. As these frameworks continue to expand, greater effort should be devoted to harmonising methodologies, definitions and risk criteria. A more coherent approach could improve comparability across assessments, reduce reporting burdens and strengthen the effectiveness of de-risking policies. It could also facilitate a better understanding of the stage of a supply chain, value chain or development process at which risks can most effectively be mitigated.

Deepen cooperation with trusted international partners. Countries such as Japan, the United Kingdom, Canada and Australia have developed related approaches to economic security and resilience. Closer cooperation – bilaterally and in fora such as the OECD – on methodologies, scenario exercises, stress-testing and information exchange could help improve the quality of risk assessments and contribute to a more consistent understanding of economic security risks among like-minded partners.

6 References

- Amaral, A., Connell, W., Di-Comite, F. and Herghelegiu, C. (2022) ‘SCAN’ (*Supply Chain Alert Notification*) monitoring system. Single Market Economics Papers. https://single-market-economy.ec.europa.eu/publications/scan-supply-chain-alert-notification-monitoring-system_en
- Arcesati, R. and Gehrke, T. (2024) *Europe’s economic security agenda needs far better techno-industrial intelligence*. MERICS. <https://merics.org/en/comment/europes-economic-security-agenda-needs-far-better-techno-industrial-intelligence>
- Arjona, R., Connell, W. and Herghelegiu, C. (2023) *An enhanced methodology to monitor the EU’s strategic dependencies and vulnerabilities*. Single Market Economics Papers. https://single-market-economy.ec.europa.eu/publications/enhanced-methodology-monitor-eus-strategic-dependencies-and-vulnerabilities_en
- Arjona, R., Connell, W., Herghelegiu, C., Ho, V. and Varela-Irimia, X.-L. (2025) *DG GROW’s Supply Chain Analytics Hub*. Single Market Economics Briefs. <https://webgate.ec.europa.eu/circabc-ewpp/d/d/workspace/SpacesStore/475d6e99-55ba-41bf-920d-1da2b44fdeb3/download>
- Bonnet, P., Di Girolamo, E.F., Pagano, A., Velazquez, B. and Zaurino, E. (2026) *EU foreign dependencies: Assessment of trade and geopolitical vulnerabilities*. DG Trade Chief Economist Note, Issue 2. <https://circabc.europa.eu/ui/group/50a0487d-086a-4a75-a1ff-92bdd2ec2c4b/library/a2e01f42-cfac-4669-bb18-fe287788bd1d/details?open=true> (accessed via the Economic analysis portal).
- Digital Europe (2024) *The Download, Issue 6: Taming the cyber storm whilst empowering European businesses to thrive*. https://cdn.digitaleurope.org/uploads/2024/11/DIGITALEUROPE-THE-DOWNLOAD-ISSUE-6-FINAL_WEB.pdf
- European Commission (2019) *Regulation (EU) 2019/452 establishing a framework for the screening of foreign direct investments into the Union*. <https://eur-lex.europa.eu/eli/reg/2019/452/oj>
- European Commission (2020) *Cybersecurity of 5G networks: EU toolbox of risk mitigating measures*. <https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures>
- European Commission (2021) *Strategic dependencies and capacities*. Commission Staff Working Document, SWD(2021) 352 final. https://commission.europa.eu/system/files/2021-05/swd-strategic-dependencies-capacities_en.pdf
- European Commission (2022a) *EU strategic dependencies and capacities: Second stage of in-depth reviews*. Commission Staff Working Document, SWD(2022) 41 final. <https://ec.europa.eu/docsroom/documents/48878>
- European Commission (2022b) *Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive)*. <https://eur-lex.europa.eu/eli/dir/2022/2555>
- European Commission (2023a) *European Economic Security Strategy*. Joint Communication, JOIN(2023) 20 final. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52023JC0020>

- European Commission (2023b) *Commission Recommendation on critical technology areas for the EU's economic security for further risk assessment with member states*. C(2023) 6689 final. https://defence-industry-space.ec.europa.eu/commission-recommendation-03-october-2023-critical-technology-areas-eus-economic-security-further_en
- European Commission (2023c) *List of 10 critical technology areas for the EU's economic security*. Annex to Commission Recommendation C(2023) 6689 final. https://defence-industry-space.ec.europa.eu/document/download/d2649f7e-44c4-49a9-a59d-bffd298f8fa7_en?filename=C_2023_6689_1_EN_annexe_acte_autonome_part1_v9.pdf
- European Commission (2023d) *Regulation (EU) 2023/1781 establishing a framework of measures for strengthening Europe's semiconductor ecosystem (Chips Act)*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2023.229.01.0001.01.ENG
- European Commission (2024a) *Regulation (EU) 2024/2747 establishing a framework of measures related to an internal market emergency and to the resilience of the internal market (Internal Market Emergency and Resilience Act)*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202402747
- European Commission (2024b) *Regulation (EU) 2024/1252 establishing a framework for ensuring a secure and sustainable supply of critical raw materials*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202401252
- European Commission (2024c) *Commission proposes new initiatives to strengthen economic security*. https://ec.europa.eu/commission/presscorner/detail/en/ip_24_363
- European Commission (2024d) *Regulation (EU) 2024/2847 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act)*. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R2847>
- European Commission (2025a) *Strengthening EU economic security*. Joint Communication, JOIN(2025) 977 final. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52025JC0977>
- European Commission (2025b) *2025 Strategic Foresight Report: Resilience 2.0 – Empowering the EU to thrive amid turbulence and uncertainty*. COM(2025) 484 final. https://commission.europa.eu/strategy-and-policy/strategic-foresight/2025-strategic-foresight-report_en
- European Commission (2025c) *European Preparedness Union Strategy*. Joint Communication, JOIN(2025) 130 final. https://commission.europa.eu/topics/preparedness_en
- European Commission (2025d) *RESourceEU Action Plan: Accelerating our critical raw materials strategy to adapt to a new reality*. COM(2025) 945 final. https://single-market-economy.ec.europa.eu/document/download/01c448d6-dc93-40d7-9afe-4c2af448d00c_en
- European Commission (2025e) *Commission calls on member states to review outbound investments and assess risks to economic security*. https://ec.europa.eu/commission/presscorner/detail/en/ip_25_261

- European Commission (2026a) *The EU Observatory of Critical Technologies*. https://defence-industry-space.ec.europa.eu/eu-space/eu-observatory-critical-technologies_en
- European Commission (2026b) *Raw Materials Information System (RMIS): About RMIS*. <https://rmis.jrc.ec.europa.eu/about>
- European Commission (2026c) *Proposal for the Chips Act 2.0*. <https://digital-strategy.ec.europa.eu/en/library/proposal-chips-act-20>
- European Commission (2026d) *Investment screening*. https://policy.trade.ec.europa.eu/enforcement-and-protection/investment-screening_en
- European Commission (2026e) *Statement by President von der Leyen at the joint press conference with President Costa following the meeting of the European Council of June 2026*. https://ec.europa.eu/commission/presscorner/detail/en/statement_26_1401
- García-Herrero, A. (2025) *The Nexperia crisis: A wake-up call for Europe's approach to Chinese investment*. Bruegel. <https://www.bruegel.org/newsletter/nexperia-crisis-wake-call-europes-approach-chinese-investment>
- Jarlebring, J. (2026) *Governing economic security*. Europapolitisk analys 2026:5epa. Swedish Institute for European Policy Studies. <https://sieps.se/publikationer/2026/governing-economic-security/>
- National Board of Trade (2025a) *Tools for resilient supply chains: An overview of EU policy*. <https://www.kommerskollegium.se/globalassets/publikationer/rapporter/2025/tools-for-resilient-supply-chains-an-overview-of-eu-policy.pdf>
- National Board of Trade (2025b) *Ten priorities for the EU's economic security agenda*. <https://www.kommerskollegium.se/globalassets/publikationer/rapporter/2025/ten-priorities-for-the-eus-economic-security-agenda.pdf>
- National Board of Trade (2026a) *Strategic dependencies in Swedish imports: A methodological framework and analysis*. <https://www.kommerskollegium.se/globalassets/publikationer/rapporter/2026/strategic-dependencies-swedish-imports.pdf>
- National Board of Trade (2026b) *Recommendations to strengthen the EU's economic security cooperation*. <https://www.kommerskollegium.se/globalassets/publikationer/rapporter/2026/recommendations-to-strengthen-the-eus-economic-security-cooperation.pdf>

Sammanfattning på svenska

Summary in Swedish

Under senare år har ekonomisk säkerhet blivit en politisk prioritering för Europeiska unionen. Geopolitiska spänningar, störningar i leveranskedjor samt oro för teknikläckage och ekonomiskt tvång har fått EU att utveckla nya metoder för att bedöma risker som följer av internationell handel, investeringar och tekniskt ömsesidigt beroende. Den här analysen utvärderar EU:s framväxande ramverk och politik för riskbedömningar inom ekonomisk säkerhet. Analysen visar att EU har gjort framsteg när det gäller att identifiera sårbarheter kopplade till leveranskedjor, kritisk teknik och strategiska beroenden. Nya metoder och övervakningsinitiativ har förbättrat EU:s förståelse av risker och utgör i allt högre grad underlag för åtgärder som syftar till att stärka motståndskraften och minska sårbarheterna.

Samtidigt kvarstår betydande utmaningar. Befintliga metoder har förbättrat kartläggningen av strukturella beroenden, men är mindre lämpade för att förutse framtida risker som följer av geopolitisk utveckling, teknisk förändring och utländska aktörers agerande. Nästa fas i EU:s agenda för ekonomisk säkerhet bör därför inriktas på att stärka styrningsmekanismer, informationsdelning och strategiskt förutseende. EU bör gå från periodiska bedömningar till en mer kontinuerlig riskanalys, förbättra samordningen mellan kommissionen, medlemsstaterna och nationella myndigheter, stärka samarbetet med näringslivet samt främja större samstämmighet mellan olika ramverk och policyinstrument för riskbedömning. Ett närmare samarbete med betrodda partner och inom internationella forum som OECD skulle ytterligare kunna stärka metoderna och bidra till en gemensam förståelse av risker för EU:s ekonomiska säkerhet.

The National Board of Trade Sweden is the government agency for international trade, the EU internal market and trade policy. Our mission is to facilitate free and open trade with transparent rules as well as free movement in the EU internal market.

Our goal is a well-functioning internal market, an external EU trade policy based on free trade and an open and strong multilateral trading system.

We provide the Swedish Government with analyses, reports and policy recommendations. We also participate in international meetings and negotiations.

The National Board of Trade, via SOLVIT, helps businesses and citizens encountering obstacles to free movement. We also host several networks with business organisations and authorities which aim to facilitate trade.

As an expert agency in trade policy issues, we also provide assistance to developing countries through trade-related development cooperation. One example is Open Trade Gate Sweden, a one-stop information centre assisting exporters from developing countries in their trade with Sweden and the EU.

Our analyses and reports aim to increase the knowledge on the importance of trade for the international economy and for the global sustainable development. Publications issued by the National Board of Trade only reflect the views of the Board.

The National Board of Trade Sweden, September 2026, ISBN: 978-91-89742-94-9