Centrum für Europäische Politik
FREIBURG | BERLIN

cepInput

No. 3 | 2025 28 January 2025

An Economic Security Doctrine For Europe

Managing External Economic Threats in Times of Fragmentation

André Wolf

The ever more visible decay of a rules-based global trade order has forced the EU to recalibrate its external economic policies. The new Commission has identified economic security as a key issue on its agenda for the new legislative period. It will initiate the development of an overarching risk management framework aimed at reducing the vulnerability of the EU economy to hostile third country policies. This will require policymakers to centrally organize and strategically deploy the existing arsenal of economic defense instruments, while remaining consistent with the principles of an open economy. This cepInput analyzes the EU's current economic risk profile and provides recommendations for the formulation of an EU Economic Security Doctrine.

- Current EU risk profiles are highly specific to technologies and value chain segments. The EU should follow a value chain-centered approach in economic risk management, identifying and monitoring weak spots in the value chains of technologies most critical for the green and digital transformation.
- When implementing own countermeasures to hostile third country policies, the EU must pay specific attention to unintended negative side effects on the economy of partner countries. This requires detailed impact assessments of cross-sectoral effects and in-depth consultation with foreign governments.
- Strategic partnerships with third countries are an integral part of any EU long-term strategy to mitigate external policy risks. The EU should speed up their implementation by intensifying bilateral talks and improve the involvement of the private sector. Moreover, to address the risk of long-term instability in partnerships, the EU should work on creating partnership-specific assets. The prospect of joint technological leadership through R&D collaboration and market integration can be particularly attractive for potential partners.
- The EU should seek to merge individual partnership initiatives into plurilateral economic security clubs. Their purpose is to institutionalize economic security cooperation, offering reduced exposure to external risks through value chain diversification and a common defense strategy against external shocks.

Table of Contents

List of Figures

1 Background

With a protectionist US president in office and a number of international trade disputes still unresolved, the EU must be prepared for further attacks on its established supply chains. In an increasingly fragile and politicized world trade order, these risks go well beyond traditional trade policy, affecting areas such as knowledge sharing and the security of physical infrastructure. The surge in external risks comes at a time when Europe's business models are particularly vulnerable due to declining cost competitiveness and high financing needs for green and digital transformation. To reduce risks ex ante and increase resilience to crises, the EU needs to develop a balanced risk management framework, including room for unilateral action where necessary.

In recent years, the EU has significantly expanded its arsenal of unilateral trade defence instruments, responding to the widespread use of subsidy practices by competitors and an eroding multilateral trade order. Simultaneously, the range of objectives has expanded as well, going beyond the protection of domestic producers from market distortions and encompassing economy-wide goals like the prevention of knowledge outflow and a reduced susceptibility to economic blackmailing by third countries. With the European Economic Security Strategy[1], the EU intended to sharpen existing instruments against these long-term risks like foreign investment screening and export controls for critical technologies. However, strategic guidelines for a targeted use of the different economic security instruments are still missing.

Against this background, it is not surprising that in the new legislative term Commission President Ursula von der Leyen defined the position of a commissioner both responsible for trade policies and economic security. The mission letter to the corresponding commissioner Maroš Šefčovič includes several initiatives to strengthen economic security, including the preparation of an Economic Security Doctrine.[2] Based on the existing Economic Security Strategy, it shall establish a framework for making strategic use of the existing set of EU policy instruments to enhance economic security. Specifically, this shall involve the development of economic security standards for key supply chains together with partners from the G7 and other like-minded actors, stressing the fact that economic security cannot be achieved through unilateral means only.

This cepInput contributes some thoughts on the development of such a policy framework. It disentangles the sources and impact channels of risks, indicating the variety and complexity of challenges involved. It presents an overview on the current strategic and legislative approach of the EU on economic security. For the set of technologies currently considered critical by the EU, it examines the risk profile in merchandise trade and technology cooperation, comparing the partner portfolios to a set of benchmark countries. Finally, it develops guidelines for the future formulation of an Economic Security Doctrine, stressing the need for a pragmatic yet consistent approach, which remains true to the EU's vision of restoring a rules-based global economic order.

---

1 European Commission / High Representative of the Union for Foreign Affairs and Security Policy (2023). Joint Communication to the European Parliament, the European Council and the Council on "European Economic Security Strategy". JOIN(2023) 20 final.

2 Von der Leyen, U. (2024). Mission letter to Maroš Šefčovič - Commissioner-designate for Trade and Economic Security.

2 Risk mapping

2.1 Risk sources and impact channels

The analysis of economic security requires the identification of sources of risk and their channels of impact. Sources of risk can be broadly categorized into the following areas: Markets, Economic Policy, Military and Terrorist Actions. Markets spread risk in the form of unexpected disruptions to supply or demand. These can arise, for example, from a sudden shortage of resources or changes in the expectations of market participants. The threat to the economic security of EU actors depends on their degree of interdependence with other actors through market interactions. Changes in the economic policies of other countries or economic blocs are also a source of various forms of risk. They can affect the availability of products in international supply chains, the size of markets and the organization of international trade as a whole. Military and terrorist actions pose economic risks to the security of a country's capital stock, particularly its public infrastructure. These spheres cannot be considered in isolation, but overlap. For instance, market developments are often the direct result of policy adjustments and vice versa.

International trade is an important channel of influence. The risks associated with trade fall into several categories. One category is the supply risks associated with imported goods. These can affect both the availability of quantities (risk of shortages) and the evolution of prices (risk of price increases). The extent of these risks depends on the degree of trade concentration (market dominance of the main exporting countries) and the technological relevance (degree of technical substitutability) of the imported products. At present, the EU's external dependence is in some cases very high, especially for resources and technology goods considered critical for a future digital and climate-neutral economy.[3] This poses real risks to the stability of international supply chains. Examples include the escalating chip war between the US and China[4] and China's discretionary export policy on scarce materials like rare earths, driven by strategic interests.[5]

Another risk relates to the competitive situation on international markets. Unfair competition resulting from third country policies that directly or indirectly favor their exports threatens the functioning of the internal market and the competitiveness of EU companies. One example is China's policy of massive subsidies for key technologies such as photovoltaics or electric mobility.[6] In addition to export subsidies, this can also take the form of exploiting differences in national tax policies.[7] An opposite case is the targeted use or threat of trade restrictive measures to achieve geopolitical objectives. A recent example of this form of political blackmail is China's coercive economic campaign against Lithuania, which followed a change in the country's foreign policy stance towards Taiwan.[8] In addition to diplomatic pressure, the campaign included temporary restrictions on Lithuanian products on the Chinese market and warnings to companies trading with China to buy Lithuanian inputs. The risk of

[3] Wolf, A. (2022). Europe's position on raw materials of the future. cepInput No.11/2022.
[4] The Guardian (2024). Chip war ramps up with new US semiconductor restrictions on China.
[5] Mancheri, N. A. (2015). World trade in rare earths, Chinese export restrictions, and implications. Resources Policy, 46, 262-271.
[6] Bickenbach, F., Dohse, D., Langhammer, R. J., & Liu, W. H. (2024). Foul play? On the scale and scope of industrial subsidies in China (No. 173). Kiel Policy Brief.
[7] Harta, L., Kullas, M., Vöpel, H, Wolf, A. (2024). Digital Services - European Solutions for Fair Taxation of Multinational Digital Service Providers. cepStudy.
[8] Andrijauskas, K. (2022). An analysis of China's economic coercion against Lithuania. Council on Foreign Relations, 7.

political blackmail depends to a large extent on the degree of integration of the supply chain with individual third countries.

Finally, foreign trade can also be associated with the risk of technology leakage. Learning-by-importing is a well-established concept in the economic growth literature. There is strong empirical evidence that technology laggards are indeed able to reduce the technology gap and increase their productivity through reverse engineering of imported knowledge-intensive products.[9] In some cases, this may even extend to exports, if the provision of highly specialized inputs requires some knowledge exchange with trade partners in international supply chains.[10] For EU companies, this may entail the risk of a loss of competitive advantage due to knowledge leakage, especially in areas with a high degree of specialization and a strong dependence on export opportunities. Examples of this are certain green-tech areas such as wind turbines and heat pumps, where European producers still have significant global market shares but are facing increasingly fierce competition by Chinese firms.[11] In areas where products can be used for military purposes, this risk also has a military security dimension.

Another important channel is **cross-border capital flows**. The most important of these is foreign direct investment (FDI), i.e. investment that allows foreign entities to exert strategic influence over domestic companies. In the case of inward FDI, this entails the risk of foreign control of companies of critical economic importance, which increases the vulnerability towards blackmailing by foreign investors as well as by their home governments. This is particularly true where foreign investors are closely linked to, or under the direct economic control of, the public sector. A related risk is that of technology leakage. Even more than in the case of trade relations, foreign ownership carries the risk of exclusive knowledge flowing back to the investor's home country.[12] A prominent example is the "Made in China 2025" strategy, where the targeted acquisition of foreign high-tech firms is an integral part of the envisaged catching-up process.[13] In the case of some restrictive FDI policies, this may also apply to outward FDI. If EU investors are forced to cooperate with domestic firms in the target countries, e.g. through arrangements such as joint ventures, the establishment of a foreign presence can also lead to an outflow of critical knowledge. Again, Chinese policies towards foreign investors are a prime example.[14]

Finally, intensified FDI flows also carry the risk of a loss of human capital. International evidence suggests that FDI flows and labor migration may play a complementary role.[15] This includes scenarios where foreign investors seek to attract highly skilled workers from affiliates to their foreign headquarters, for example by offering higher wages or a more attractive working environment. At least in the short term, this is associated with a loss of embodied knowledge at the location of the affiliate. In the

9 Keller, W. (2021). Knowledge Spillovers, Trade, and FDI (No. 28739). National Bureau of Economic Research.
10 Freixanet, J., & Federo, R. (2023). Learning by exporting: A system-based review and research agenda. International Journal of Management Reviews, 25(4), 768-792.
11 European Commission (2023a). Investment needs assessment and funding availabilities to strengthen EU's Net-Zero technology manufacturing capacity. Commission Staff Working Document. SWD(2023) 68.
12 Smeets, R. (2008). Collecting the pieces of the FDI knowledge spillovers puzzle. The World Bank Research Observer, 23(2), 107-138.
13 Levine, D. A. (2020). Made in China 2025. Journal of Strategic Security, 13(3), 1-16.
14 Pinsent Masons (2024). Foreign direct investment in China.
15 Candau, F. (2013). Trade, FDI and migration. International Economic Journal, 27(3), 441-461.

long run, however, this could be compensated by a positive incentive effect for higher education at the location of the affiliate.[16]

Another impact channel is **international cooperation in research and development** (R&D). While cooperation between non-profit research institutions such as universities is a long-established phenomenon around the world and generally serves to improve mutual efficiency, the situation for private companies is more complex. Important questions are what rules are established for the use of pre-existing and jointly created knowledge and how these can be enforced. From a societal perspective, research partnerships promise a (partial) solution to the problem of socially insufficient R&D activities by private firms due to the presence of positive externalities (knowledge spillovers). However, this has to be weighed against the risk that joint product innovation could become the starting point for a production joint venture or collusion, which could lead to monopoly situations in future markets.[17] Moreover, from a national perspective, cross-border knowledge spillovers from research cooperation may be harmful if they significantly enhance the competitiveness of foreign firms. This is particularly the case when these firms compete in specialization areas of the domestic economy. Any targeted policy to support cooperation must therefore be carefully conditioned and complemented by firm rules on knowledge appropriation and the prevention of collusion. In addition, like FDI, R&D cooperation can encourage the creation of personal networks that may encourage the emigration of scarce local talent.[18]

Concerns about economic security also extend to the **security of physical infrastructure**. In the Western world, critical infrastructure components such as energy and ICT networks are increasingly subject to hostile attacks.[19] These include both physical attacks - the destruction of undersea cables and pipeline links - and attempts to disrupt the digital control of infrastructure systems.[20] By directly affecting production that relies on the continuous supply of infrastructure - such as digital service providers or industrial consumers of bulk electricity - even short-term disruptions of critical infrastructure services can have potentially devastating economic cascading effects. For most critical infrastructure components, risk prevention is made particularly difficult by the fact that they are widely dispersed in space, resulting in high monitoring costs and the need for close cooperation between public and private stakeholders.

2.2 Policy instruments

A broad catalogue of policy instruments is necessary to counter the variety of economic security risks. With regard to external trade risks, measures include the list of traditional tariff-based trade defense instruments. Based on the nomenclature in WTO law, these can be divided into three types of measures, depending on the occasion. **Anti-dumping measures** are aimed at eliminating dumping of imports through temporary tariff increases.[21] Dumping occurs when producers from a third country sell goods in the EU below the selling price in their home market or below the cost of production. Such

[16] Docquier, F., & Rapoport, H. (2012). Globalization, brain drain, and development. Journal of economic literature, 50(3), 681-730.
[17] Katz, M. L. (1986). An analysis of cooperative research and development. The RAND Journal of Economics, 527-543.
[18] Scellato, G., Franzoni, C., & Stephan, P. (2015). Migrant scientists and international networks. Research Policy, 44(1), 108-120.
[19] Slakaityte, V., & Surwillo, I. (2024). Protecting EU's critical infrastructure - The fight intensifies in the cyber realm. DIIS Policy Brief.
[20] EnergiCERT (2022). Cyber-attacks against European energy & utility companies. Report September 2022.
[21] European Commission (2022a). Introduction to trade defence policy.

tariff increases can be imposed temporarily for a maximum of six months and permanently for a maximum of five years. A practical difficulty in many cases is the lack of reliable price and cost information to identify the occurrence and extent of dumping.

In contrast, the decisive criterion for **anti-subsidy measures** is the subsidization of products imported into the EU from third countries. The subsidy need not be specifically limited to exports. In this case, temporary tariff increases are intended to offset the level of subsidization and thus restore a level playing field in the internal market. Such tariff increases can be decided on a temporary basis for a maximum of four months and on a permanent basis for a maximum of five years. The sensible use of this instrument also requires a high level of information, both on the amount of subsidies paid to companies and on their appropriate distribution among individual products. Moreover, even if applied accurately, they make imported products more expensive for domestic consumers and, in the case of intermediate products, for industry.

A third category of trade defense measures is **safeguard measures**. They do not require evidence of unfair trade policies by third countries, but are simply linked to the condition that imports of a particular product into the EU suddenly have increased sharply. Their purpose is to give domestic industry time to adjust to the unexpected increase in foreign competition. Provisional safeguard measures can last up to 200 days and definitive measures up to 4 years.[22]

Besides these conventional anti-distortive measures, the era of ambitious climate policies has brought up a fourth category of tariffs trying to compensate for differences in CO_2 pricing embedded in imports and domestically produced products. In this case, the purpose of import tariffs is to eradicate the competitive advantage of producers from less ambitious third countries on the internal market.[23]

In addition to making imports more expensive through higher tariffs, unfair competition can also be tackled through quantitative restrictions on imports. Unlike tariffs, import quotas make it possible to directly control the market share of imported goods - and thus to reduce the political room for maneuver of foreign countries. Alternatively, a similar effect can be achieved by excluding products from hostile countries from domestic public procurement procedures.

A common limitation of all these trade defense measures is that there is no guarantee that they will actually improve the overall competitive situation of domestic industries. Apart from the likely negative direct impact of higher import prices on domestic consumers and downstream industries, the wider impact on international trade as a whole is difficult to predict, as trade diversion and other market linkage effects may arise. Even if measures are undoubtedly WTO-compliant, the risk of retaliation by adversely affected third countries cannot be ignored, potentially reinforcing geo-economic fragmentation tendencies and triggering a downward spiral for trade freedom. This also leads to potential conflicts with the objective of supply chain security.

Instruments targeting **FDI flows** start with screening mechanisms that analyze the impact of acquisitions or greenfield investments on the competitive situation for products and technologies. FDI transactions are assessed based on their riskiness for domestic economic sovereignty and technological

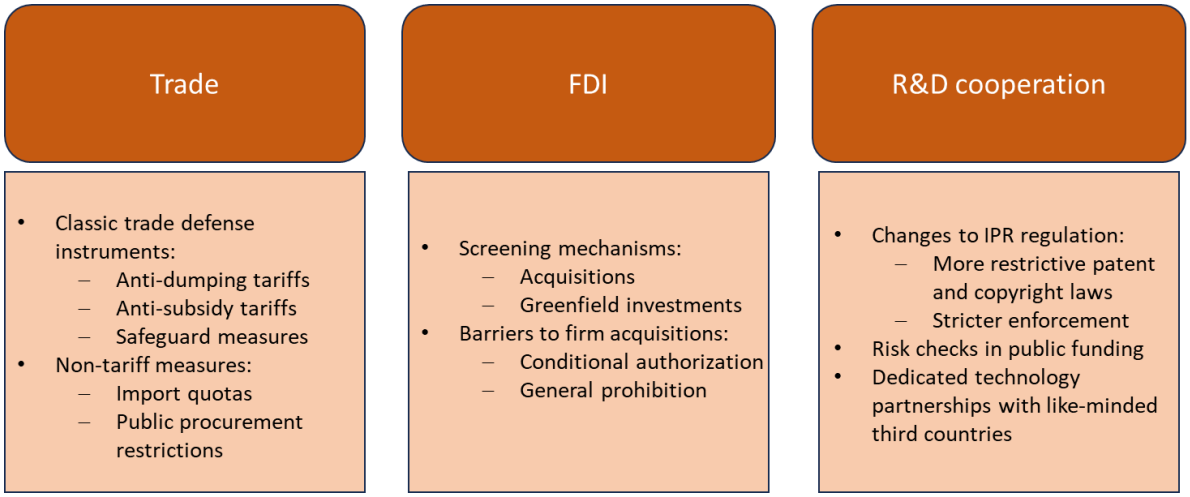
[22] See European Commission (2022a).

[23] Jousseaume, M., Menner, M., & Reichert, G. (2021). CBAM: Damaging to Climate Protection and EU Export Industries. cepStudy.

leadership in critical areas. If an acquisition is found to pose a significant risk, restrictive measures could be imposed. In the strictest case, this could take the form of an outright prohibition of the transaction. Alternatively, authorization could be made subject to certain conditions, such as the unbundling (legal or purely economic) of firm assets within the corporate structure.[24] Such restrictive measures are not necessarily limited to inward FDI, but could also be applied to acquisitions by EU investors in third countries, with a focus on the risk of knowledge leakage. However, such restrictive measures cannot discriminate between knowledge outflows and inflows and thus also exclude domestic firms from mutually beneficial knowledge exchange.

In the field of **research cooperation**, the basis for risk mitigation is again the implementation of a screening mechanism, identifying potentially sensitive research areas and critical partners in terms of intellectual property rights (IPR) policies. A short-term approach of reducing identified risks is to strengthen own IPR laws or their enforcement, thus ensuring a more effective sanctioning of the foreign exploitation of own knowledge exchanged in the cooperation process. However, even with strict patent and copyright laws in place, knowledge spillovers can in many cases not be fully avoided, as any protection of intellectual property is limited in time, restricted to codifiable knowledge and subject to enforcement costs.[25] Another approach is to apply consistent conditions for the choice of research partners in public research grant applications. Finally, a long-term risk reduction approach is to change the geographical nature of research cooperation by creating institutionalized R&D partnerships with likeminded third countries. To stabilize such partnerships, cooperation could be steered towards areas where joint efforts are promising strong scale economies. This concerns, for instance, the enforcement of IPR protection in international research cooperation and common work on standardization as a way to guide the future technology development.[26]

Figure 1: Overview of policy instruments to combat external economic risks



Source: own illustration

[24] Tingvall, P., & Hallberg, J. (2023). Economic Perspectives on FDI and Investment Screening. In Weaponising Investments: Volume I (pp. 117-139). Cham: Springer International Publishing.

[25] See Katz (1986).

[26] Caloghirou, Y., Hondroyiannis, G., & Vonortas, N. S. (2003). The performance of research partnerships. Managerial and Decision economics, 24(2-3), 85-99.

3 EU economic security policies

3.1 The leading concept of open strategic autonomy

External trade policy is the exclusive competence of the EU. The increase in trade disputes and supply chain disruptions in recent years, even before the outbreak of the war in Ukraine, has led to a noticeable reorientation in this area. In its Trade Policy Review 2021, the European Commission introduced the concept of 'open strategic autonomy' as a new guiding principle for EU trade policy. On the one hand, it emphasizes that it will continue to work for open and rules-based global trade based on multilateral cooperation. But it also makes clear that the EU must be able to defend its strategic interests and values independently and confidently in the global trade order. This includes measures to increase the resilience and sustainability of its supply chains and the ability to tackle unfair trade practices by third countries. The Commission summarizes this reorientation in three medium-term trade policy objectives: 1) supporting the EU economy in the upcoming transformation towards decarbonization and digitalization, 2) influencing global trade rules towards a more sustainable and fairer form of globalization, 3) enhancing the EU's ability to pursue its objectives through autonomous action.[27]

This reorientation reflects the EU's attempt to reconcile the principles of free trade and multilateralism, which are central to its self-image, with the radically changing internal (primacy of climate and sustainability goals) and external (global fragmentation processes) environment. This inevitably leads to points of friction. For example, it needs to address the extent to which past trade liberalization has contributed to the current fragility of supply routes by fostering the geographical fragmentation of supply chains. The future viability of multilateralism as an organizing principle is also being severely challenged by geopolitical confrontation. Key institutions, such as the WTO dispute settlement mechanism, still lack a long-term vision of how global coordination and enforcement should work in an era of polarization. The war in Ukraine and its trade-distorting side-effects have made these issues even more acute.

3.2 The Economic Security Strategy

On June 20th 2023, the Commission and the High representative published a joint Communication sketching the pillars and priorities of a future "**European Economic Security Strategy**".[28] It represents the first attempt of the EU to put the notion of economic security at the center of strategic action. It is motivated by the EU's perceived increase of economic vulnerability, which was demonstrated by recent shock events like the COVID-19 pandemic and the Ukraine war, and perpetuated by ongoing geopolitical tensions and a fierce international technology competition. Against this background, economic linkages with third countries are no longer viewed as a pure blessing, but under some circumstances also as a source of risk for European supply chains and competitiveness.

The central objective of the strategy is to provide guidelines for a better balancing of benefits and risks in the economic cooperation with third countries. The leitmotif is a both competitive and resilient

[27] European Commission (2021). Communication to the European Parliament, the European Council and the Council on the European economic and financial system: Fostering openness, strength and resilience. COM(2021) 32 final.

[28] European Commission / High Representative of the Union for Foreign Affairs and Security Policy (2023). Joint Communication to the European Parliament, the European Council and the Council on "European Economic Security Strategy". JOIN(2023) 20 final.

European economy, which does not shy away from global competition, but addresses specific security gaps while using its weight to enforce a rules-based global trade order.

The first analytical step is to identify and monitor the types of risks the European economy is facing. The Communication distinguishes between four types:

- Threats to **supply chains**: Price and supply risks for critical inputs (e.g. raw materials and energy)
- Threat to **tangible infrastructure**: Physical and digital attacks on critical infrastructure (e.g. sabotage of undersea cables)
- Threats to **technological supremacy and security**: Protection against technology leakages (e.g. knowledge transfers through FDI, espionage)
- Risk of **weaponization of economic dependencies**: Blackmailing by third countries through policy measures targeting European economic vulnerabilities (e.g. export ban on critical inputs, blocking of EU investments)

The broad spectrum of risks covered is thus not limited to criminal practices and malicious attacks, but also encompasses policy measures by third countries and further disruptive market developments which are not policy-induced.

As priorities for risk prevention and management, the Communication proposes a three-pillar approach. The EU should i) **promote** its domestic competitiveness, ii) **protect** itself against identified security risks and iii) **partner** with third countries to reinforce economic security. While pillars i) and iii) are basically summaries of pre-existing strategic approaches, pillar ii) adds a genuine element to the Economic Security Strategy. The horizon of protective measures envisaged by the Communication addresses all four risk types and involves both physical protection of critical components and an arsenal of trade and technology policy measures. At the same time, the Communication propagates the principles of **proportionality** and **precision** for all measures seized, stressing that the danger of overreactions and conflict escalations are supposed to be kept in check.

3.3 Legislation

3.3.1 Existing legislation

Even before the publication of the Economic Security Strategy, the EU implemented a set of policy tools specifically targeted at complementing and restructuring the existing arsenal of trade defense instruments. In 2020, a **Regulation establishing a framework for the EU-wide screening of inward FDI** went into force.[29] It created a cooperation mechanism among Member States and between Member States and the Commission to better supervise potentially risky FDI activities within the EU. Its intention was to link and (in the long-run) harmonize existing national FDI screening mechanisms that were already applied by many (but not all) Member States. To that end, Member States are asked to notify cases of national screening and to provide further information (e.g. identity of investor, economic sector, investment value) on single cases upon request by the Commission or other Member States. Based on the provided information, Commission and other Member States have the right to make comments (Member States) and issue opinions (Commission) on a case, which the affected Member State is

[29] European Union (2019). Regulation (EU) 2019/452 of the European Parliament and of the Council of 19 March 2019 establishing a framework for the screening of foreign direct investments into the Union.

supposed to consider in its decision on authorizing or prohibiting the investment. However, the control over the process and the exclusive right to make the decision remains in the hands of the Member State. The Regulation also does not force all Member States to implement FDI screening mechanisms. This limited its effectiveness as a coordination device.

On July 12th 2023, the **Foreign Subsidies Regulation** went into force.[30] It seeks to promote a level playing field on the internal market by giving the Commission the right to investigate and remedy the consequences of distortive foreign subsidies paid to companies operating in the EU. In this way, it complements the existing instrument of anti-subsidy tariffs imposed upon subsidized imports (see Section 2.2) with investment-focused measures. The Commission may issue requests for information to companies, conduct own market investigations and carry out inspections. It does so within three predefined procedures. The first procedure comprises the monitoring of foreign subsidies paid to firms involved in transactions in the form of firm acquisitions, mergers and joint ventures. The second procedure investigates bids in public procurement procedures that involve a significant foreign financial contribution. For both of these procedures, specific monetary thresholds are defined above which the parties involved are obliged to notify the Commission of any financial contributions received from non-EU public authorities in advance. Notified transactions may not be implemented without the approval of the Commission. The third procedure grants the Commission the right to collect similar information in all other market situations based on its own initiative. In its analysis, the Commission shall balance the distortive effect of foreign subsidies against potential positive effects (e.g. lower procurement prices, strengthened competition position of domestic firms through mergers). If the distortive effect is found to dominate, remedial action can be taken. These can take the form of commitment offers by the affected parties (e.g. repayment of subsidy, provision of certain assets) or by remedies imposed by the Commission itself. In all, this Regulation assigns much more significant monitoring and control rights to the Commission than the FDI screening framework.

In December 27th 2023, another Regulation implementing an **Anti-Coercion Instrument** entered into force.[31] Resulting from the experience of previous cases of attempted economic blackmailing of Member States (see Section 2.1), it intends to create an EU-wide scheme for deterring and responding to coercive measures by third countries. It is based on the official recognition of an economic coercion incident through an Implementing Act by the Commission. This is defined as fulfilled if a third country imposes – or threatens to impose - a measure affecting trade or investment with the goal of forcing the EU or Member States to make certain policy decisions. It conducts examinations of potential cases both on its own initiative or as a response to a duly substantiated request by Union businesses and other private stakeholders. If economic coercion is diagnosed, the Regulation spells out a series of concrete counteractions. This starts with creating the opportunity for joint consultations with the accused third country, exploring options like direct negotiations or the submission to international adjudication to settle the matter. If this proves unable to stop the coercion, the Union shall take own unilateral response measures from a list of measures spelled out in the Annex. These comprise a broad range of instruments from classic tariff-based countermeasures over exclusion from public procurement up to restrictions on IPR protection – even if this implies the non-performance of existing international obligations. Moreover, the instrument also departs from the existing defense tools in that it

[30] European Union (2022). Regulation (EU) 2022/2560 of the European Parliament and of the Council of 14 December 2022 on foreign subsidies distorting the internal market.

[31] European Union (2023). Regulation (EU) 2023/2675 of the European Parliament and of the Council of 22 November 2023 on the protection of the Union and its Member States from economic coercion by third countries

is already applicable in stages where hostile measures are not yet implemented, but only brought up as a threat.

3.3.2 Economic Security Package

In addition, to implement the new priorities of the Economic Security Strategy, several new legislative proposals and other policy initiatives were announced. Foremost, this includes an **Economic Security Package** proposed on January 24th 2024[32] comprising five initiatives: i) a Proposal for a new Regulation on FDI screening, ii) a Proposal for a Council Recommendation on enhancing Research Security as well as three white papers on the topics of iii) export controls for dual-use goods, iv) R&D support in the dual-use segment and v) security of outbound investments.

The proposed new **Regulation on the screening of inward FDI[33]** aims to streamline the existing cooperation mechanism between Member States and to improve its overall effectiveness by closing loopholes. It foresees an obligation for all Member States to implement a screening mechanism. This involves the imposition of an authorization requirement for all foreign investments in either "projects or programs of Union interest" or "activities of particular importance for the security or public order interests of the Union", both groups defined by lists in the proposal's Annex. The latter group includes all items on the EU list of critical technologies (see next Subsection), the list of dual-use items subject to export controls, the military list of the European Union, the Union list for critical medicines as well as a list of critical institutions for the European financial system. Hence, the scope of risk monitoring clearly exceeds the areas of military or terrorist threats and comprises a range of purely civil technologies.

Moreover, if, as a result of a risk screening, a Member State concludes that a foreign investment is likely to negatively affect security or public order, it shall either prohibit the investment or at least demand mitigating measures (e.g. unbundling of certain assets). In determining whether this is the case, a negative impact on the availability of critical technologies is one risk to be checked. Hence, while not banning or restricting inward FDI in sensitive, knowledge-intensive fields in general, the proposed Regulation aims to spread a cautious, risk-oriented view among European regulators on these forms of international cooperation. This might give rise to more restrictive measures in the future, also in areas where no military issues are at stake.

The Proposal for a **Council Recommendation on enhancing Research Security[34]** aims to create awareness for security risks in the research sector and strengthen the resilience towards these risks. It has been adopted by the Council on May 23rd 2024.[35] In the recommendation, research security refers to the management of three types of risks: i) undesirable transfer of critical knowledge to third countries, ii) malign foreign influence on the research discourse and iii) ethical or integrity violations. In the explanation of category i), military purposes are mentioned, but only in the form of an example. Hence, unintended knowledge transfers in civil technologies are potentially addressed as well. The proposed

[32] European Commission (2024a). Commission proposes new initiatives to strengthen economic security. Press Release, 24 January 2024.

[33] European Commission (2024b). Proposal for a Regulation of the European Parliament and of the Council on the screening of foreign investments in the Union and repealing Regulation (EU) 2019/452 of the European Parliament and of the Council. COM(2024) 23 final.

[34] European Commission (2024c). Proposal for a Council Recommendation on enhancing research security. COM(2024) 26 final.

[35] European Council (2024). Council Recommendation of 23 May 2024 on enhancing research security (C/2024/3510).

recommendations to Member States include the development of national action plans with targeted measures to boost research security. These shall include safeguarding measures in the form of risk appraisals of applicants in national research funding programs and the provision of resources to higher education investments for the build-up of internal risk management schemes. Again, special attention shall be paid to cooperation in research fields covered by the EU's list of critical technologies. Moreover, the Council recommends to the Commission to develop a Union one-stop-shop platform that collects, manages and presents EU-wide data on foreign R&D interference (European Centre of Expertise on Research Security).

The **White Paper on outbound investments**[36] argues for the need of introducing a monitoring scheme for outward FDI comparable to the monitoring of inward FDI. It sets the stage for a Commission Recommendation to Member States on implementing such a scheme. Its main arguments for this extension are first the danger of a circumvention of the export ban on dual-use goods through outward investments. Second, the attempt to prevent technology access through a ban on inward FDI could be circumvented by outward investments as well. Again, while pointing to foreign military activities as a prominent danger, the concrete steps sketched in the White Paper is to monitor a wide field of investment transactions including primarily civil technology fields. Alternatively, the recommendation is to at least cover investments in the four technology areas currently classified by the EU as most sensitive (see next Subsection).

3.4 The list of critical technologies

The background of the recent proposals is a specific list of critical technologies published as part of a Recommendation by the Commission on October 3rd 2023.[37] According to the Commission, these are technology areas whose strategic importance for the overall economic security of the EU require a profound assessment of the risks of technology security and technology leakage. The list found in Annex I of the Recommendation[38] is presented in Table 1. In selecting these technology areas, the Commission applied three criteria. The first is the enabling and transformative nature of the technology. This relates to its potential of causing drastic changes in production conditions and thus stimulating long-term productivity improvements. This is the immediate economic aspect of the definition. The second criterion is the risk of military and civil fusion, i.e. the dual use potential of the technology. It reflects the risk that unintended knowledge outflows could enhance military threat for the EU. The third criterion is the potential of misusing the technology for the violation of human rights in third countries, e.g. the surveillance of the population and the suppression of free speech.

The Commission stresses the fact that the publication of the list does not involve any definitive statement on the severity of risks. It only represents a prioritization of technology areas for such a later assessment. The assessments shall be carried out by Member States and involve private stakeholders from the industries. In this process, four of the ten technology areas are recommended to have highest priority, due to their high likelihood of causing severe and immediate risks: Advanced Semiconductors, Artificial Intelligence, Quantum Technologies and Biotechnologies. For these areas, the Commission proposed collective risk assessments to be carried out already by the end of 2023. The investigations

[36] European Commission (2024d). White Paper on outbound investments. COM(2024) 24 final.

[37] European Commission (2023b). Commission Recommendation of 3.10.2023 on critical technology areas for the EU's economic security for further risk assessment with Member States.

[38] European Commission (2023c). Annex to the Commission Recommendation on critical technology areas for the EU's economic security for further risk assessment with Member States. C(2023) 6689 final.

conducted so far entered the Economic Security Package, in particular the extended monitoring of FDI (see previous Subsection).

Table 1: List of 10 critical technology areas for the EU's economic security

No.	Technology area	Examples specific technologies
1	**Advanced semiconductor technology**	Microelectronics; Photonics; High frequency chips; Manufacturing equipment at very advanced node sizes
2	**Artifical intelligence technologies**	High performance computing; Cloud and edge computing; Data analytics technologies
3	**Quantum technologies**	Quantum computing; Quantum cryptography; Quantum communications; Quantum sensing and radar
4	**Biotechnologies**	Techniques of genetic modification; New genomic techniques; Gene-drive; Synthetic biology
5	Advanced connectivity, navigation and digital technologies	Secure digital communications and connectivity; Cybersecurity technologies; Internet-of-Things and Virtual Reality; Distributed ledger and digital identity technologies; Navigation and control technologies
6	Advanced sensing technologies	Electro-optical, radar, chemical, biological, radiation and distributed sensing; Magnetometers; Underwater electric field sensors; Gravity meters and gradiometers
7	Space and propulsion technologies	Dedicated space-focused technologies; Space surveillance and earth observation technologies; Space positioning, navigation and timing; Secure communications; Propulsion technologies
8	Energy technologies	Nuclear fusion technologies; Hydrogen and new fuels; Photovoltaics; Smart grids and energy storage
9	Robotics and autonomous systems	Drones and vehicles; Robots and robot-controlled precision systems; Exoskeletons; AI-enabled systems
10	Advanced materials, manufacturing and recycling technologies	Technologies for nanomaterials; Additive manufacturing; Digital controlled micro-precision manufacturing; Technologies for extracting, processing and recycling critical raw materials

Source: European Commission (2023b). Bold: high priority fields.

The list intends to fill a gap in the EU's overall strategy of regaining control over international supply chains in critical technology areas. While previous EU initiatives were focused on managing supply risks for tangible resources like energy (RePowerEU)[39] and raw materials (Critical Raw Materials Act)[40], or promoting domestic production capacities for technologies (Net Zero Industry Act, STEP), this initiative focuses on knowledge as a critical intangible resource. It reflects the insight that having influence on the organization of future supply chains requires sufficient control over knowledge flows. Moreover, the list goes beyond previous approaches in specifying more clearly which technology fields should be prioritized for technology sovereignty at EU level.

Yet, the way the Recommendation is formulated reveals a high degree of caution on the side of the Commission. Firstly, while being more precise than before, the list of prioritized technologies appears still very broad, an impression that is reinforced by the myriads of concrete examples mentioned (see Table 1). Secondly, while describing technology threats in general terms, the Commission carefully

[39] European Commission (2022b). REPowerEU: affordable, secure and sustainable energy for Europe. Communication COM(2022) 108 final.

[40] European Union (2024a). Regulation (EU) 2024/1252 of the European Parliament and of the Council of 11 April 2024 establishing a framework for ensuring a secure and sustainable supply of critical raw materials and amending Regulations (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1724 and (EU) 2019/1020Text with EEA relevance.

avoids to spell out any concrete risk scenarios. In particular, China as the elephant in the room is left unmentioned. This shows that the Commission is careful not to spur ongoing trade conflicts with China through this initiative. Thirdly, the reference to military and human rights threats intends to downplay any industrial policy ambitions associated with the initiative. For some of the technology areas, this is not very credible, as the mentioned links with military issues are rather far-fetched. Fourthly, apart from continuous monitoring, the initiative avoids to further concretize the potential future countermeasures against identified technology threats loosely presented in the Economic Security Strategy (see previous Subsection). In particular, this holds for technology risks in relation to outbound FDI whose future treatment is still up in the air. Instead, the importance of intensive future exchange before imposing any policy measures is stressed by the Commission.

In all, the purpose of the initiative seems to lie more in sending a wake-up call to Member States and a warning signal to China than in building the backbone of a new policy approach for managing technology risks. It sketches a road of technological protectionism Europe is ready to follow if attempts to restore a (from an EU-perspective) fair global trade order fail. It is thus part of an arsenal of weapons to strengthen Europe's position in ongoing trade talks. Yet, given its coincidence with increased promotion of domestic production and announced tariff increases[41], it raises the risk of hostile countermeasures by China endangering a settlement of the economic disputes.

4 Multidimensional risk mapping: The case of critical technologies

4.1 Method and data

In the following, to discuss the relevance of the different risk categories addressed by the EU's Economic Security Strategy, we conduct an illustrative empirical analysis of existing economic risks related to international exchange in the near-term situation. Such an analysis cannot be undertaken at the macroeconomic level, as this would not reveal specific supply chain dependencies. At the same time, an analysis at the level of single goods or technologies would not provide a holistic picture or (in the case of considering a broad range) easily get lost in detail. We therefore follow a middle approach by comparing different technology fields. As a basis for differentiating fields, we make use of the EU list of critical technologies discussed in Section 3.4. In this way, we can be sure to analyse technologies that are of critical relevance for the EU's future growth model.

In principle, three areas are particularly worthy of investigation: trade in goods, R&D cooperation, capital flows and trade in services. Unfortunately, for the latter two, the currently available public data do not provide a level of disaggregation that would allow distinguishing between specific technology areas. Therefore, our illustrative analysis focuses on trade in goods and R&D cooperation.

Trade data at product level is available from UN Comtrade.[42] To use this data for our purposes, a link between the product classifications offered and our critical technologies needs to be established. To this end, we can draw upon existing work conducted by the European Commission's Advanced Technologies for Industry (ATI) project.[43] For different fields of advanced technologies, they undertook trade analyses by assigning different product categories based on the Harmonized System (HS) product

[41] European Commission (2024e). Commission investigation provisionally concludes that electric vehicle value chains in China benefit from unfair subsidies. Press release, 12 June 2024.
[42] UN Comtrade (2025). UN Comtrade Database.
[43] European Commission (2024). European Monitor of Industrial Ecosystems.

classification to each field. Their system of technology fields frequently overlaps with the EU list, which allows us to adopt their assignment in many cases. Critical technologies which could not be aligned with the ATI nomenclature were dropped from the analysis. In one case (energy technologies), an own assignment based on keyword search was undertaken.

To analyse the external dependence of the EU with respect to merchandise trade, this trade data needs to be mirrored against domestic production. To this end, we draw upon Eurostat's PRODCOM database, which provides annual production figures in value terms for a detailed set of products.[44] To match the PRODCOM product classification with trade data, we can again follow the assignments undertaken by the ATI project.

Concerning the measurement of R&D cooperation, patent data are frequently applied as output-based indicators. Their limitations are well known.[45] They do not provide information about the actual subsequent market success of patented inventions and their general societal impact. They are also not perfect measures of innovation at the development stage, as many types of inventions are not patentable for technical or legal reasons. Nevertheless, main advantages are the high degree of international harmonization and the high level of technological detail in patent statistics. The International Patent Classification (IPC) system allows for an extremely fine-grained subdivision according to fields of technology.[46]

For our analysis of international research cooperation in critical technologies, we use data from PATSTAT, the worldwide patent statistical database of the European Patent Office (EPO).[47] It is one of the world's most comprehensive patent databases and a popular choice for innovation analyses. To identify the IPC classes attached to the different fields of critical technologies defined by the EU (see Subsection 3.4), we again draw upon work conducted by the ATI project.[48] In a series of publications, the ATI project analysed EU patenting activities in a range of advanced technologies, by applying lists of IPC codes established by the detailed technology expertise of the participating institutions.[49] The set of advanced technologies covered by the ATI is similar, yet not identical to the EU's list of critical technologies. Where possible, we adopted or aggregated the ATI technology fields based on the examples mentioned in the EU critical technology list. Fields whose complexity and/or transversal nature did not allow for a clear code assignment (e.g. robotics) were omitted. In one case (energy technologies), an own code assignment compatible with the product assignment in trade analysis was performed. In another case (biotechnologies), an official OECD definition was applied.[50]

For all classes, data on all registered patents over the period 2016 to 2020 was retrieved via search queries in PATSTAT.[51] In the next step, it was merged with data from the OECD REGPAT database.[52] This contains additional information on the names and residential addresses of the inventors

[44] Eurostat (2025). PRODCOM Database.
[45] Wydra, S. (2020). Measuring innovation in the bioeconomy–Conceptual discussion and empirical experiences. Technology in Society, 61, 101242.
[46] WIPO (2024). International Patent Classification (IPC). World Intellectual Property Organization.
[47] EPO (2024). PATSTAT – Backbone dataset for statistical analysis. European Patent Office.
[48] European Commission (2024). European Monitor of Industrial Ecosystems.
[49] ATI (2021). Indicator framework and data calculations. September 2021.
[50] Friedrichs, S., van Beuzekom, B. (2018). Revised proposal for the revision of the statistical definitions of biotechnology and nanotechnology. OECD Science, Technology and Industry Working Papers, 2018/01, OECD Publishing, Paris.
[51] For more recent years, available patent data is currently still incomplete.
[52] OECD (2024). Intellectual property (IP) statistics and analysis. Organization for Economic Cooperation and Development, Paris.

registered in the patents, thus enabling a detailed spatial allocation. Compared to using the addresses of the applicants, which in the case of multinational enterprises can be a parent company or an affiliate located far away from R&D activities, this results in a more precise spatial picture of innovation.

The number of patent applications is a common indicator for quantifying patenting activity. For a country comparison, we must consider that often several people are registered as the inventors of a patent, who may be located in different countries. As is common in the literature, we account for this by applying an equal share for each inventor as a weighting factor. For instance, in the case of a patent with eight registered inventors, each inventor is assigned a share of 0.125. Then, we calculate the total innovation activity of a country in a field as the sum of the shares of inventors residing in the respective country ("inventor counts").

If persons located in different countries are registered as inventors in a patent application, this patent application is interpreted as a case of international research cooperation. With such a broad definition, cooperation can in practice be based on different kinds of motivations and arrangements. For instance, it covers both firm-internal (cross-border R&D activities of MNEs) and firm-external (independent institutions from different countries engage in collaboration) forms of research cooperation. In the country comparisons, the EU27 (as defined by current membership) are always treated as one bloc. Hence, in the figures reported for the EU, international cooperation only includes cases where inventors located in a Member State cooperate with inventors located in a third country.

In all, this has provided us with six critical technology fields for our risk analysis: Advanced materials, AI technologies[53], Biotechnologies, Connectivity technologies, Energy technologies and Semiconductor technologies. Tables A 1-3 in the Appendix show the selection process and the lists of corresponding HS, PRODCOM and IPC codes.

To illustrate the relative exposure of the EU, we compare results for all risk indicators to a set of benchmark countries. Specifically, we consider the USA, South Korea and Japan. This choice is both due to their comparability in terms of economic size and development stage, and due to the fact that they are all strategic rivals of China.

4.2 Results

4.2.1 Merchandise trade

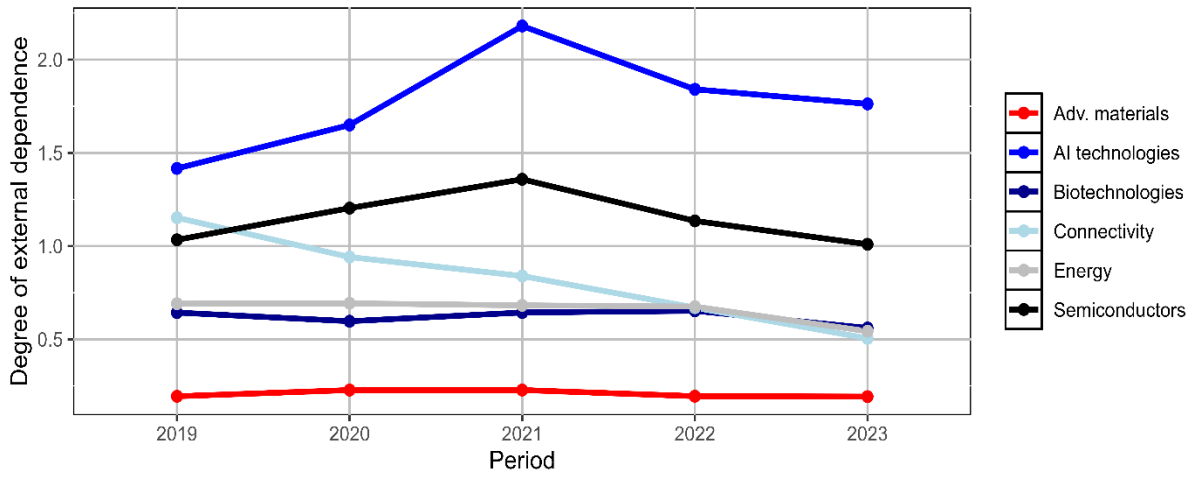
In analyzing trade patterns for products related to critical technologies, we need to cope with the fact that many of these critical technologies are still in an early development stage. A long-term comparison of trade flows would in many cases thus either not be possible or not be meaningful. In the following, we therefore focus on the most recent situation, by considering annual trade volumes over the period 2019-2023.

As a first risk indicator, we are interested in the EU's overall external dependence in the single fields. One simple way to express such a dependence is the relation between imports and domestic production. We consider the ratio of total import volumes obtained from UN Comtrade to domestic production values from PRODCOM. As no comparable production data is available for third countries, this

[53] The definition applied is quite comprehensive, involving both patentable data storage and processing technologies, learn algorithms and speech analysis techniques.

part of the analysis has to be restricted to the EU. Figure 2 shows the comparison by technology field for our five-year-horizon. It reveals significant discrepancies. While external dependencies in advanced materials have been consistently low, third country imports of AI technology goods partly more than doubled domestic production. In detail, this concerns products such as data carriers and signaling devices. A further observation is the overall decline in external dependency for products related to connectivity technologies. Amongst others, this involves components for mobility applications like radars and navigation instruments.

Figure 2: Degree of EU external import dependency in critical technology fields

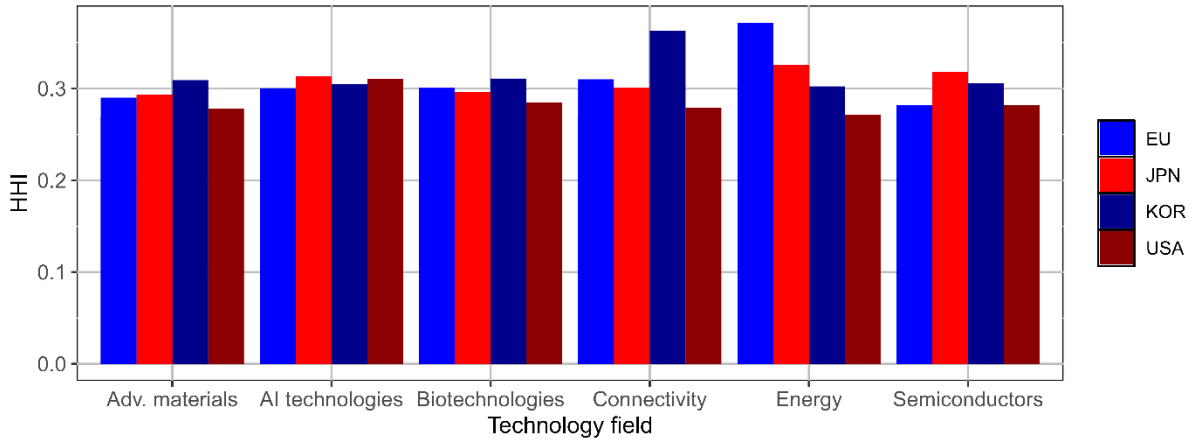


Sources: Eurostat (2025); UN Comtrade (2025); own calculations.

In a world characterized by strong bidirectional trade flows, import dependency as such does not necessarily represent an issue. However, an insufficiently diversified portfolio of trading partners in certain sensitive technology areas does come with a set of risks, both related to direct physical supply and to the vulnerability towards political pressure (see Section 2.1). One simple way to reflect the degree of concentration in the trade portfolio is through the classic Herfindahl–Hirschman Index (HHI).[54] It measures concentration on a scale from 0 to 1. We use it to measure country concentration regarding the origin of imported goods, both for the EU and our benchmark countries. Figure 3 represents the results as annual averages over the period 2019-2023. Accordingly, EU imports in energy technologies showed a very high degree of concentration in comparison to the benchmark countries. This is most pronounced for PV cells/modules and battery components. In comparison to the US, country concentration of EU imports was also higher in the remaining fields, except for AI technologies. South Korea stands out with a highly concentrated partner portfolio in connectivity technologies.

[54] Rhoades, S. A. (1993). The Herfindahl-Hirschman index. Federal Reserve Bulletin, (Mar), 188-189.

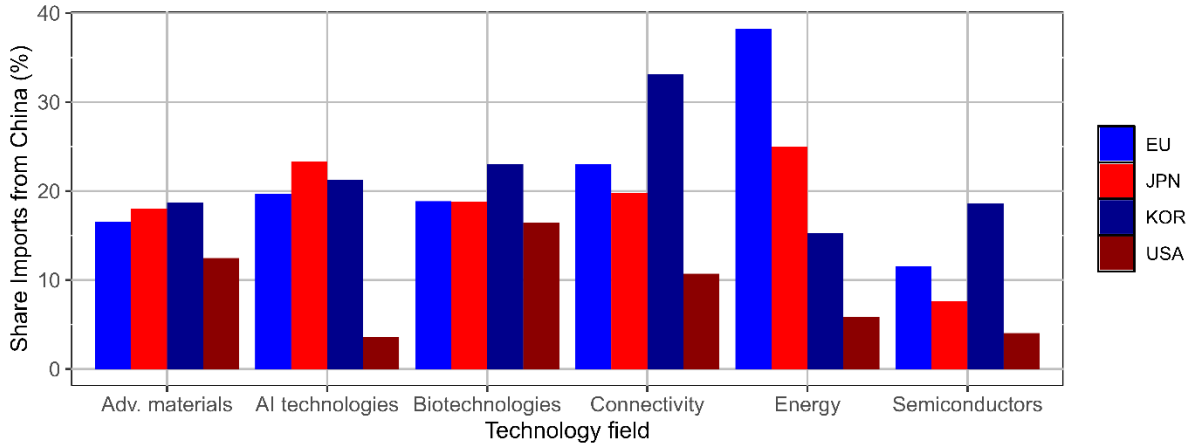
Figure 3: Degree of country concentration in imports 2019-2023 (annual averages)



Source: UN Comtrade (2025); own calculations. HHI: Herfindahl–Hirschman Concentration Index (0 – 1).

Apart from a diversification analysis, a risk assessment also requires partner-specific investigations. These should comprise the general political (rule of law, regulatory stability) and economic (industry structure, openness, own import dependencies) environment as well as the country's industrial policy strategy. In our illustrative analysis, we restrict our attention to the particular role of China, given its economy-wide importance as a trading partner and its role as a disruptive force in the international trade system. Figure 4 shows for the same time frame as above the share of Chinese products in total imports by technology field. The EU again stands out in energy technologies, with almost 40 % of annual import value attributable to Chinese products. US imports exhibited the by far smallest reliance on China in all technology fields considered. The overall China dependence of Japan and South Korea is at a similar level than the EU's China dependence, but is distributed very differently across fields.

Figure 4: Share of Chinese products in imports 2019-2023 (annual averages)



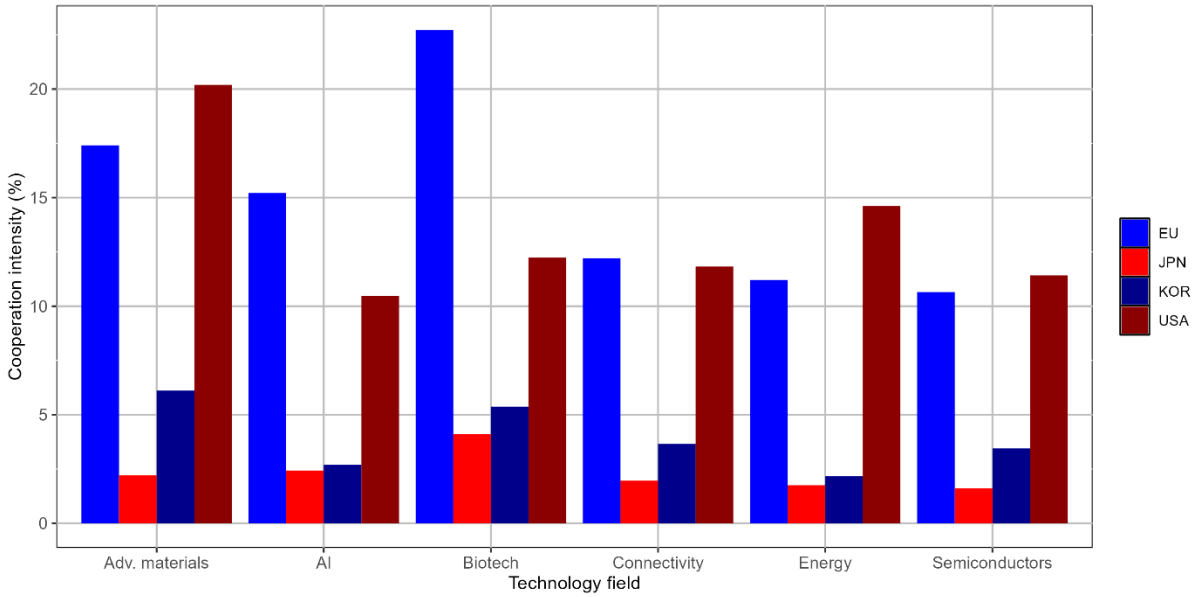
Source: UN Comtrade (2025); own calculations.

4.2.2 R&D cooperation

To assess the degree of R&D cooperation, the number of innovations obtained through international cooperations can be set in relation to the overall innovation activity of a country. To this end, we define a simple indicator of cooperation intensity, the share of patent applications involving international cooperation in the total patent applications of a country/region within the specific period and field.

Figure 5 presents the results for selected countries/regions. Overall, the EU and the US have built their innovation activities to a comparatively high degree on international cooperations. For the EU, particularly high cooperation intensities are reported for advanced materials and biotechnologies. Cooperation intensities of Japan and South Korea are consistently low and have largely even declined in the more recent period.

Figure 5: Intensity of international patent cooperation by technology field 2016-2020



Source: PATSTAT (2025); own calculations.

A specific look at the cooperation partners of the EU reveals further interesting patterns. In all fields, the US were consistently the by far most important partner. In four fields, more than half of the EU's bilateral patent connections were established with US researchers. Connections with researchers in China were significantly less frequent in all of the fields, they accounted for less than 10 % of the EU's patent collaborations. The maximum level of engagement with China is observed for advanced materials and energy technologies. India is a further relatively significant non-European partner of the EU, at least in the fields of AI and connectivity technologies.

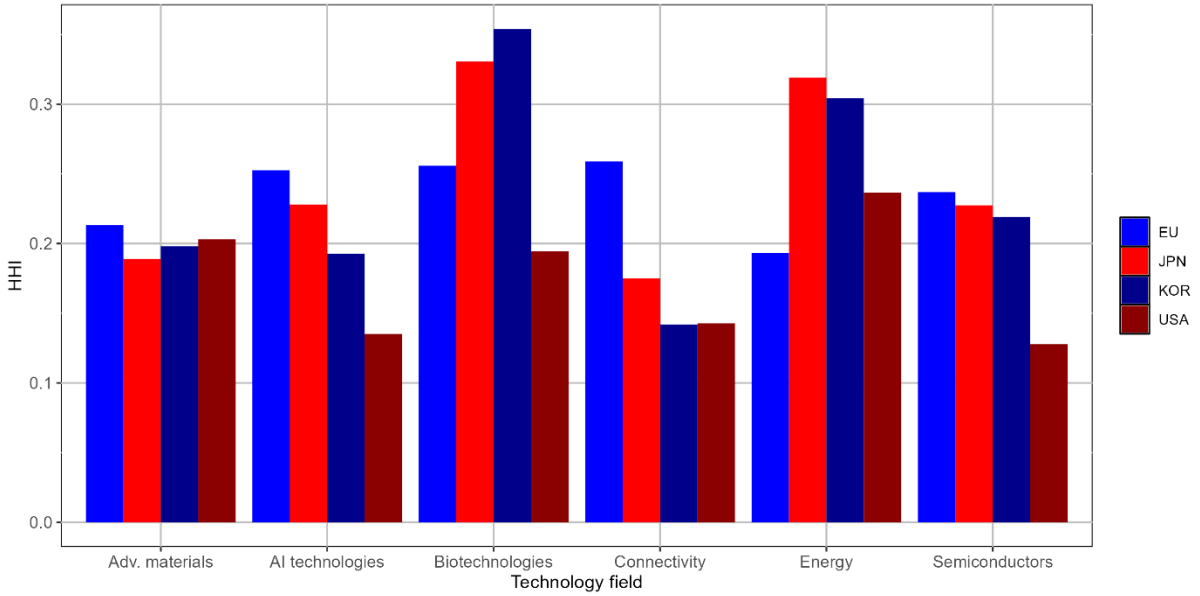
For any institution, the expected benefits of international research cooperation must be weighed against the risks associated with sharing own resources and knowledge with foreign partners. As discussed in Section 2, these risks include potential inefficiencies caused by institutional mismatch, but also insufficient control over the partner's use of pre-existing or jointly generated knowledge. The latter is especially problematic if foreign laws on intellectual property protection are less strict or difficult to enforce. From a country-wide perspective, the risks related to unintended knowledge outflows also touch upon the issue of national competitiveness. Through this channel, domestic resources spent on R&D activities could accidentally improve the market position of competitors of national champions.

Similar to trade, partner portfolios in R&D can be assessed from a geostrategic perspective. In this regard, a strong concentration of research ties on single partner countries can be seen as a source of-long-term risk. It implies a high sensitivity of own international research activities to changes in the innovation and property rights policies of specific partner countries. It can also increase the exposure towards general political pressure, especially if researchers in the partner country possess exclusive

knowledge indispensable for deep innovation. Establishing a diverse portfolio of partner countries represents a form of insurance against these country-specific policy risks.

To assess the degree of country concentration in international research cooperation, we again apply the Herfindahl–Hirschman Index (HHI). Figure 6 depicts the results. Accordingly, the US exhibited the by far most diversified partner portfolio, reflecting its central role within global research networks. The EU portfolio was more concentrated in all fields except for energy technologies. Europe's international collaborations were least diversified in the fields of AI technologies, Biotechnologies and Connectivity, research, mainly due to the dominance of partnerships with US researchers.

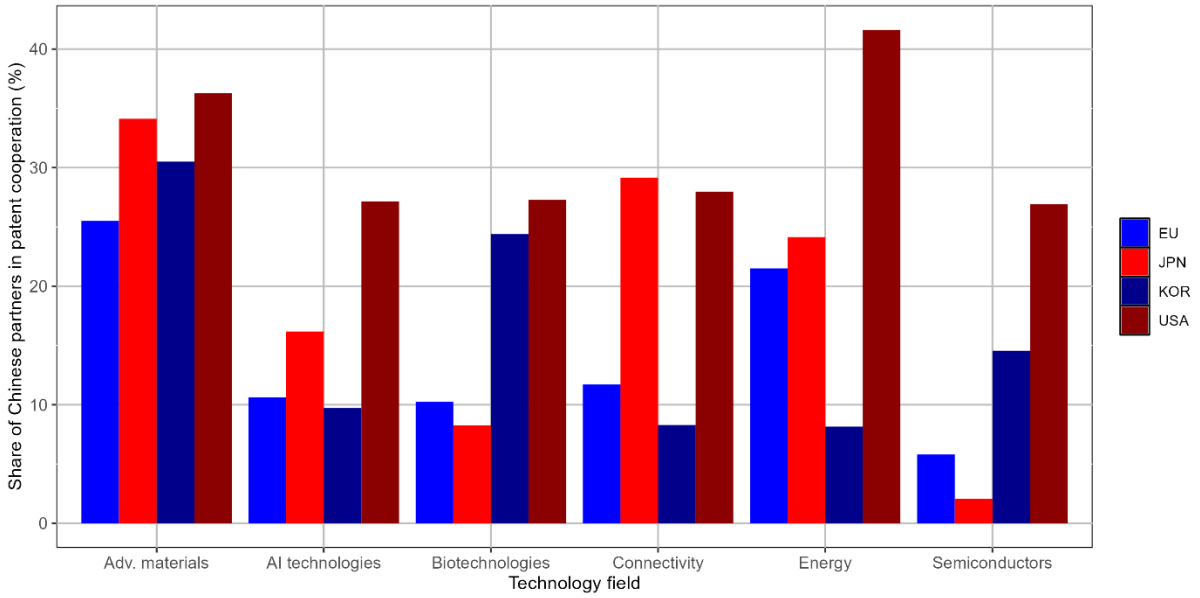
Figure 6: Country concentration in international patent cooperation by technology field 2016-2020



Source: PATSTAT (2025); own calculations. HHI: Herfindahl–Hirschman Concentration Index (0 – 1).

Finally, another perspective on cooperation patterns is the degree of cooperation with researchers based in China. As we identify international cooperation based on the home addresses of the inventors, this includes forms of both intra- and extra-firm cross-border cooperation and does not allow any conclusions to be drawn about the nationality of the inventors. Figure 7 shows the share of international research partners resident in China by technological field. As can be seen, EU R&D cooperation with China is rather modest compared to the benchmark countries in all fields examined. This is mainly due to the high importance of transatlantic research cooperation with the United States for EU patenting activity. China was most important as an R&D partner in advanced materials and energy technologies. For US researchers, transatlantic cooperation was of relatively lower importance during this period. Instead, China was a very significant research partner of the US, again especially in advanced materials and energy technologies.

Figure 7: Share of partners located in China in international patent cooperation 2016-2020



Source: PATSTAT (2025); own calculations.

4.2.3 Summary

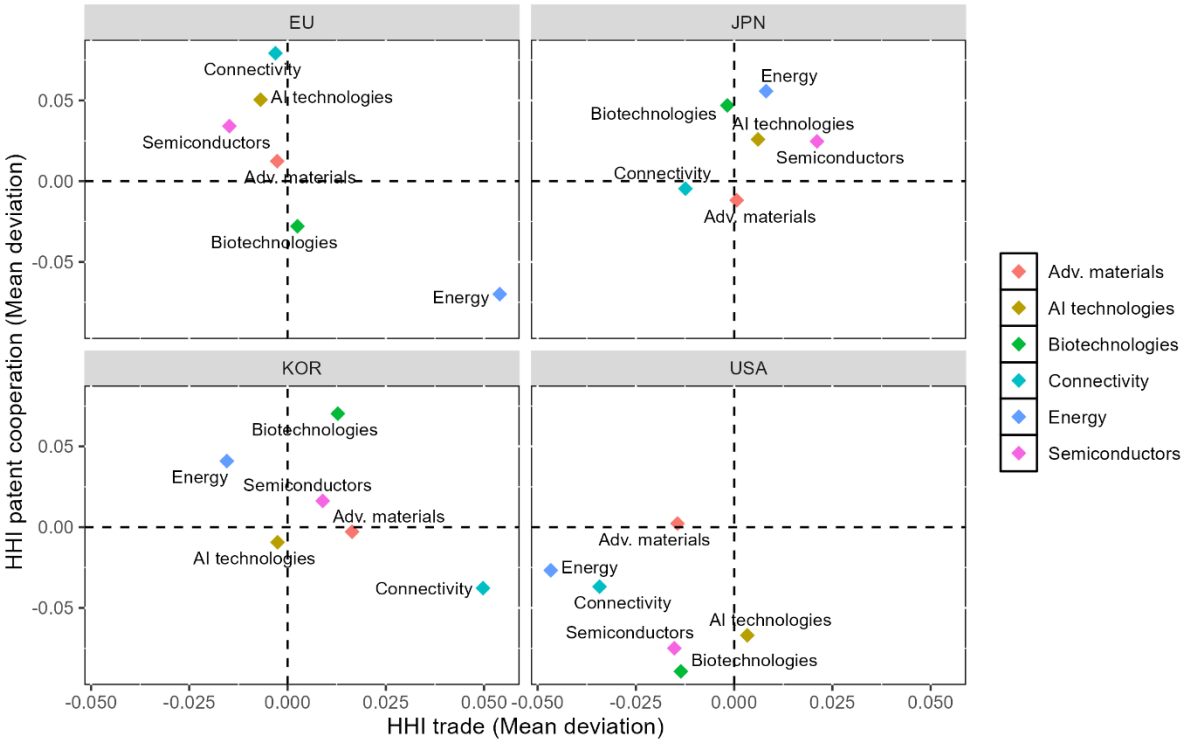
The preceding analysis demonstrates the strong embeddedness of European value chains for critical technologies into global trade and R&D networks. At the same time, even our stylized investigation at technology group level reveals that the extent of these interconnections is highly specific to: i) technology segments and ii) value chain stages. Regarding cross-border goods flows, the EU currently exhibits the highest external dependence in the field of AI technologies. Conversely, in domains such as advanced materials, the EU's external dependence is comparatively lower. Furthermore, significant technology discrepancies are evident in the intensity of international R&D cooperation, though these disparities vary significantly across different fields. Notably, biotechnologies and advanced materials demonstrate the strongest integration into global R&D networks, underscoring the necessity for a value chain approach in the monitoring of external economic risks.

In addition to the overall degree of interdependence, significant technology-related differences in risk exposure have been identified with regard to the composition of partner portfolios in merchandise imports. Energy technologies are an outlier in this respect, with a particularly high concentration of imports on a few suppliers, most notably China. By comparison, the degree of concentration of EU partners in R&D co-operation is very similar across technology fields. However, a more pronounced divergence in the relative importance of China as a research partner is observed across different technology fields. Co-operation with researchers in China is more than twice as intensive in the development of advanced materials and energy technologies than in biotechnology or semiconductors.

A direct comparison with the results for the benchmark countries shows that the EU's technology risk profile is highly specific. Figure 8 shows the HHI measures for trade and patent cooperation as deviations from the means of the four countries/regions analyzed. It shows that for the EU, technology fields with comparatively high (low) partner concentration in trade were associated with comparatively low (high) partner concentration in R&D. The situation is different for Japan, where partner concentration

in merchandise imports and R&D was clearly positively correlated, implying a strong multiple risk exposure in areas such as AI, energy and semiconductor technologies.

Figure 8: Relative partner concentration in trade and R&D across technology fields



Sources: UN Comtrade (2025); PATSTAT (2025); own calculations. HHI: Herfindahl–Hirschman Concentration Index (0 – 1).

5 Policy recommendations

While our anecdotal empirical analysis of critical technologies cannot fully illuminate economic security risks, it does demonstrate the value of a differentiated risk management approach. Because external dependencies and partner portfolios vary widely across technology areas and value chain segments, any serious risk monitoring must necessarily be value chain-based. This not only improves the general knowledge base, but also increases the accuracy of potential policy responses. This in turn reduces the risk that policy responses will have unintended harmful effects on economic cooperation partners and provoke unpredictable countermeasures. It also sheds light on the long-term interplay between technological development and future trade patterns.

However, the delineation of individual value chains still does not fully reflect the interdependencies created by alternative uses of necessary raw materials and intermediates. This is particularly relevant in areas where different critical technologies compete for access to the same hard-to-substitute materials and products (e.g. permanent magnets for battery electric vehicles or wind turbines). Taking account of these interdependencies requires a methodological approach that fully reflects market interactions, e.g. by using computable general equilibrium models. However, any sophisticated methodology must remain pragmatic in terms of information needs and avoid imposing additional information requirements on EU companies.

Based on these general concerns, we define the following five guiding principles for the future formulation of an EU Economic Security Doctrine.

1. **Consistency with overarching policy goals and internal coherence:** When formulating a risk management strategy, the EU must adhere to the thought that risk minimization is not a policy goal per se. Instead, risk mitigation must remain consistent with the EU's general foreign economic policy goals, as recently summarized by the concept of open strategic autonomy. In particular, it must not reduce the EU's capability to maintain and gain economic allies for enforcing its vision of restoring a global system of rules-based economic cooperation in an era of increasingly fragmented trade blocs. Moreover, proposed measures must be coherent in terms of their effects.
2. **Long-term thinking in prioritization:** The multitude of sector- and technology-specific risks entails a wide range of potential policy responses. Given the complexity of their economic repercussions, the formulation of clear principles for prioritizing areas of action and measures is indispensable. These should be in line with ongoing structural change and emerging future specialization patterns of EU economies. In particular, any risk mitigation and crisis response measure must be carefully examined in terms of potential lock-in effects, i.e. the effect of accidentally cementing unsustainable specialization patterns. This requires a long-term understanding of economic risk beyond the evaluation of current market positions.
3. **Scientific rigor in impact analysis:** To account for interlinkages and resulting economic repercussions on other supply chains and markets, future impact analyses of any policy responses to external shock should be based on state-of-the-art economic cross-sector models. These should be able to account for the impact of structural change to address any long-term impacts. Moreover, forecasts should always include scenarios reflecting the imposition of targeted countermeasures by negatively affected third countries, to document the sensitivity to policy backlash.
4. **Transparency in decision-making:** Decisions on risk mitigation and crisis response measures need to be based on transparent ex-ante rules. The EU must resist the temptation to respond to disruptive policy switches and attempts of economic blackmailing by trading partners with own unpredictable short-term actions. This would not only undermine the EU's central values and thus its global credibility, but also seriously overestimate its capability to steer global trade and knowledge flows in critical areas with strong external dependencies. Instead, contributing to the emergence of a new-rules based global economic order requires the EU to make the first step and act as a role model. This also requires any response to be proportionate, both regarding the intensity of intervention and its sectoral scope.
5. **Pragmatism concerning information needs:** The quest of implementing a detailed and scientifically sound monitoring framework must not lead to a further escalation of information needs**,** potentially imposing additional information obligations on EU companies. Instead, future methodologies should focus on better exploiting existing public datasets and aligning formal technology definitions with empirical classification systems. In this regard, public-private initiatives bringing together experienced actors from administrative statistics and affected industries will be key for overcoming data silos and harmonizing data collection approaches at different levels.

Rooted in these principles, we make the following concrete recommendations for the risk management framework, differentiated into the steps of risk monitoring, ex-ante risk mitigation/avoidance and policy responses in the event of external shocks.

Proposals for risk monitoring

- **Harmonize monitoring schemes among Member States:** EU-wide risk monitoring is only effective if all Member States install monitoring schemes that are equally ambitious and comparable in terms of monitoring results. To this end, the EU should accelerate the implementation of the revised FDI screening regulation (see Subsection 3.3.1). Moreover, Member States should follow the proposals of the Council Recommendation on enhanced research security for a closer cooperation in the exchange of data and development of joint guidelines to tackle risks related to R&D cooperation. In particular, the foundation of an EU Centre for Research Security could help to overcome information lacks and facilitate the development of joint solutions.
- **Limit risk monitoring to a restricted set of critical technologies:** To reduce monitoring costs and ensure sufficient focus on value chains critical for future overall competitiveness of the EU, any future systematic risk monitoring approach should be restricted to a limited list of critical technologies. Criticality needs to be identified based on objective criteria, involving close collaboration with industry and input from researchers and other technology experts. As foreseen, the list requires regular updating based on recent market and technology trends. Moreover, the Commission should stick to its approach of differentiating two priority levels, with the most information-intensive analysis steps being restricted to high-priority technologies.
- **Develop specific indicators to represent different types of risks:** For a continuous and transparent monitoring of the various forms of risks related to critical technologies (see Subsection 2.1), the Commission should develop an overarching methodology that quantifies specific risks in the form of official, easy-to-interpret indicators. For this, it can draw upon existing work by the Joint Research Centre, such as the list of critical raw materials[55], as role models. Indicators should primarily be based on publicly and timely available data. To stress the specificity of different risk types, the EU should refrain from calculating an overall "criticality score", but rather investigate potential complementarities between different risks.
- **Cooperate with partner countries in methodology development:** Partner countries with similar risk exposure as the EU, in particular from the G7, should be involved in setting up a risk monitoring framework, both regarding the identification of critical technologies and the development of indicators for risk monitoring. In this way, methodologies are able to account not only for the risk profile of the EU, but also of potentially differing risk profiles (see Section 4) of partner countries. This facilitates the implementation of a joint risk response framework (see below).

[55] European Union (2024b). Regulation (EU) 2024/1252 of the European Parliament and of the Council of 11 April 2024 establishing a framework for ensuring a secure and sustainable supply of critical raw materials and amending Regulations (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1724 and (EU) 2019/1020

Proposals for risk mitigation

- **Foster the implementation of strategic partnerships:** To reduce the EU's exposure to external economic risks, coordinated efforts with like-minded countries to develop new value chains for critical technologies are of crucial importance. In addition to concluding bilateral free trade agreements, the EU has recently begun to make increasing use of the instrument of bilateral strategic economic partnership agreements. Besides facilitating mutual trade, these initiatives aim to develop joint value chains by creating institutions for knowledge exchange and cross-border capital investment. Partnerships so far either center on access to critical raw materials and energy sources[56] or technology cooperation.[57] Many of these initiatives are still in a very early implementation stage without any or with only vaguely defined roadmaps. The EU should speed up the implementation by intensifying bilateral talks and improve the involvement of the private sector. Moreover, to address the risk of long-term instability in partnerships, the EU should work on creating partnership-specific assets. This can include e.g. public EU-funding of joint R&D projects and collaboration in the development of industry standards.
- **Merge existing partnership initiatives to Economic Security Clubs:** To keep track of the multitude of partnership initiatives at EU and Member State level, information on aims and scope of single initiatives should be collected by a central data repository. Based on this information, the Commission should - in close coordination with Member States - develop an overarching management strategy of partnerships, with the goal of maximizing their contribution to risk mitigation in the field of critical technologies. In the medium term, single initiatives should be increasingly merged to plurilateral Economic Security Clubs. Their purpose is to institutionalize long-term economic security cooperation, offering reduced joint exposure to external risks and a perspective on common technological leadership as club goods. Consistent with the EU-internal approach, cooperation should take a value chain perspective, by involving joint investment in both production capacities and technological innovation. Besides working on the diversification of value chains, clubs should establish a common defense strategy towards outside shocks through close coordination of countermeasures (see below).

Proposals for shock response measures

- **Formulate clear case-based decision rules:** To address external trade shocks caused by hostile foreign policies in a proportionate manner, the EU should develop a transparent catalogue of tailor-made measures, drawing on the available mix of legal defense instruments (see Section 2). This should involve different stages of escalation. In any case, the attempt of solving the conflict through direct consultation with the responsible third country should represent the first step, followed by exploring the option of conflict settlement through multilateral institutions. The recently implemented Anti-Coercion Instrument (see Subsection 3.3.1) provides a suitable general decision-making framework for this. However, it needs further concretization regarding the choice of countermeasures in different constellations.
- **Coordinate countermeasures with partner countries:** As an important step towards Economic Security Clubs, the imposition of any unilateral countermeasure by the EU should be preceded by consultation with partner countries. In particular, this concerns the risk of undesired trade diversion effects or other forms of spillovers to partner countries. Within institutionalized

[56] Wolf, A. (2023). Strategic resource partnerships. cepInput No. 04/2023.
[57] Wolf, A. (2024). The future of global technology cooperation. cepStudy.

Economic Security Clubs, cooperation could be extended to agreeing on harmonized countermeasures in the event of targeted policy attacks on single club members. This would strengthen the economic weight of countermeasures and thus provide an additional insurance service to club members.

- **Follow a cross-sectoral and pre-emptive approach in impact analysis:** The decision on countermeasures presupposes a careful case-based investigation of potential wider economic effects. Future impact analyses should always take a cross-sectoral and international perspective, keeping a close eye on indirect effects on trade flows and supply chains through input-output-linkages. This should involve dedicated downside risk scenarios, including scenarios featuring an escalation of trade conflicts.
- **Strengthen the EU's capacity for non-protectionist unilateral crisis response:** Even with Economic Security Clubs being firmly established, the EU will always require a certain capacity for unilateral action as a fallback option. This should not be limited to trade and investment policies, but also include ways to compensate for economic losses induced by external policy shocks in a more direct form. For instance, in the event of external supply shocks, the maintenance of internal strategic reserves of highly critical materials can provide such a fallback option.[58] However, its societal costs need to be carefully weighed against the benefit of extending the scope for action.

6 Conclusion

Recently, the indispensable benefits of external economic cooperation for the EU have been overshadowed by a public debate focused on geopolitical risks. This is reflected in the new European Commission's plans for the coming legislature. A new Economic Security Doctrine will provide a strategic toolkit to deal with different forms of external threats to the EU's prosperity from third countries. To this end, the mix of available defense instruments needs to be structured in a way that allows both strategic risk mitigation and targeted crisis response. At the same time, the EU needs to remain aware of the limitations defined by its founding principles like rule of law, especially in comparison to countries like China. This cepInput examines the landscape of risks and potential countermeasures.

An anecdotal analysis of partner portfolios in R&D cooperation and trade in goods shows that risk profiles are highly technology-specific. Moreover, for most technologies, innovation risk exposure differs significantly from trade-related risks. This calls for a value chain-centered approach to risk management. The main task of an economic security doctrine should be, first, to develop guidelines for the implementation of the EU's economic security toolbox, including the formulation of transparent conditions and decision rules, a roadmap of case-based implementation steps, and a methodology for monitoring the necessity and success of implemented measures. Second, it should develop means to improve cooperation between Member States in this area and to tackle the problem of free riders in enforcement within the EU. Third, it should seek to export and develop the EU approach to economic security through institutionalized dialogues with both high- and low-income third countries, building economic security clubs as a bulwark against bad trade and investment practices.

These clubs could provide a kind of double insurance for their members. First, by developing common value chains for critical technologies, they help mitigate external risks by diversifying existing supply

[58] Wolf, A. (2022). Strategic reserves of critical metals. cepInput No. 14/2022.

channels. Second, through the coordinated implementation of defense measures, they ensure both a more efficient response to external political shocks and a stronger deterrent effect against future attempts at economic blackmail. The price of such enhanced coordination for the EU is a partial loss of policy autonomy. However, in an external economic environment dominated by increasingly unpredictable disruptive forces, this seems a justifiable price to pay to secure its position in future value chains.

7 Appendix

Table A 1: Technology fields and HS codes

Critical technology (EU definition)	Considered	Source	Abbreviation	Assigned HS Codes
Advanced semiconductor technologies	Yes	ATI (2021): Micro- and Nanoelectron-ics, Photonics	**Semiconductors**	854110, 854121, 854129, 854130, 854140, 854150, 854160, 854231, 854232, 854233, 854239, 845610, 852340, 853120, 854140, 854190, 854470, 900110, 900120, 900190, 900211, 900219, 900220, 900290, 900510, 900580, 900610, 900630, 900661, 900669, 900720, 900810, 900830, 900840, 901010, 901050, 901060, 901110, 901120, 901310, 901320, 901380, 901820, 902221, 902229, 902730, 902750, 903141, 903149
Artifical intelligence technologies	Yes	ATI (2021): Artificial intelligence	**AI**	847010, 847149, 847150, 847170, 847321, 852329, 852351, 852359, 852380, 852841, 852851, 852861, 853180, 854320, 854370, 900711, 900719, 950410
Quantum technologies	No (no meaningful assignment of IPC codes)			
Biotechnologies	Yes	ATI (2021): Indust-rial biotechnology	**Biotech**	291521, 291811, 291812, 291813, 291814, 291815, 291816, 291818, 291819, 291829, 291830, 291891, 291899, 292221, 292229, 292231, 292239, 292241, 292242, 292243, 292244, 292249, 293621, 293622, 293623, 293624, 293625, 293626, 293627, 293628, 293629, 293690, 350790, 380891
Advanced connectivity, navigation and digital technologies	Yes (aggregate with sensing technologies)	ATI (2021): Internet of Things, IT for mobility, Security	**Connectivity**	844331, 847149, 850610, 850630, 850640, 850650, 850660, 850680, 850690, 851762, 851769, 851950, 852340, 852351, 852352, 852359, 852380, 852610, 852691, 852692, 852713, 852719, 852791, 852799, 852990, 853010, 853080, 853090, 853120, 853400, 854320, 854390, 854470, 900110, 902810, 902830, 903040, 903180, 852329, 852351, 852352, 852359, 852380, 853110, 853120, 854232, 854233, 854290, 903040, 852380, 852610, 852691, 852990, 853010, 853080, 853090, 860110, 900580, 901410, 901420, 901480, 901580, 902910
Advanced sensing technologies	Yes (aggregate with connectivity technologies)			
Space and propulsion technologies	No (not separated by API (2021))			
Energy technologies	Yes	Own keyword search	**Energy**	8412, 841861, 841911, 841912, 841919, 8506, 854142, 854143, 854149, 854330
Robotics and autonomous systems	No (no meaningful assignment of IPC codes)			
Advanced materials, manufacturing and recycling technologies	Yes	ATI (2021): Advanced materials	**Adv. materials**	281810, 284210, 284610, 284690, 285200, 300510, 300590, 300670, 321590, 340700, 380110, 380120, 380130, 380190, 380210, 381220, 381230, 381800, 382430, 390950, 391400, 400520, 400591, 400599, 540310, 540331, 540332, 540333, 540339, 540500, 550200, 550410, 550490, 690911, 690912, 690919, 700711, 700719, 700721, 700729, 760310, 760320, 850519, 850730, 850740, 850780, 852210, 854590, 900140, 900150

Table A 2: Technology fields and PRODCOM codes

Critical technology (EU definition)	Considered	Source	Abbreviation	Assigned PRODCOM Codes
Advanced semiconductor technologies	Yes	ATI (2021): Micro- and Nanoelectron-ics, Photonics	**Semiconductors**	26112120, 26112150, 26112180, 26112220, 26112240, 26112260, 26112280, 26113003, 26113006, 26113023, 26113027, 26113034, 26113054, 26113065, 26113067, 26113080, 26113091, 26113094, 26112220, 26112240, 26114070, 26202200, 26403400, 26512020, 26515330, 26515350, 26516470, 26516630, 26518100, 26601115, 26601130, 26601170, 26601300, 26701100, 26701250, 26701600, 26702153, 26702155, 26702170, 26702180, 26702230, 26702250, 26702270, 26702310, 26702330, 26702390, 26801200, 27311100, 27311200, 27402500, 27403300, 27403910, 27902050, 28411110, 32501335
Artifical intelligence technologies	Yes	ATI (2021): Artificial intelligence	**AI**	26201400, 26201500, 26201700, 26202100, 26202200, 26403300, 26406050, 26701300, 26801100, 26801300, 27901150, 27902080, 27904530, 28231000, 28232210
Quantum technologies	No (no meaningful assignment of IPC codes)			
Biotechnologies	Yes	ATI (2021): Indust-rial biotechnology	**Biotech**	20143271, 20143473, 20143475, 20144290, 20146470, 20201100, 20201590, 20595957, 20595990, 21102010, 21102020, 21105100
Advanced connectivity, navigation and digital technologies	Yes (aggregate with sensing technologies)	ATI (2021): Internet of Things, IT for mobility, Security	**Connectivity**	26121080, 26122000, 26123000, 26201400, 26201800, 26202200, 26203000, 26302320, 26302370, 26401100, 26512020, 26512050, 26512080, 26514400, 26516330, 26516370, 26516690, 26518100, 26801200, 26801300, 27201100, 27201200, 27311100, 27311200, 27902050, 27903330, 27903370, 27904530, 27907010, 27907030, 26113027, 26113034, 26113054, 26113065, 26113067, 26113080, 26114090, 26122000, 26123000, 26202200, 26203000, 26305020, 26305080, 26514400, 26801100, 26801300, 27902050, 26511120, 26511150, 26511180, 26511200, 26512020, 26512050, 26516430, 26518100, 26702250, 26801300, 27903330, 27907010, 27907030, 29102430, 29102450, 30201100
Advanced sensing technologies	Yes (aggregate with connectivity technologies)			
Space and propulsion technologies	No (not separated by API (2021))			
Energy technologies	Yes	Own keyword search	**Energy**	25302100, 25302200, 26112240, 27201200, 27521400, 28121200, 28251380, 28491283, 27201100
Robotics and autonomous systems	No (no meaningful assignment of IPC codes)			
Advanced materials, manufacturing and recycling technologies	Yes	ATI (2021): Advanced materials	**Adv. materials**	20135275, 20136270, 20136500, 20165670, 20165970, 20593000, 20595230, 20595300, 20595400, 20595640, 20595650, 20595740, 20595940, 20602150, 20602140, 20602200, 20602320, 20602340, 20602390, 20602400, 21202420, 21202430, 21202440, 22192019, 23121210, 23121230, 23121250, 23121270, 23441100, 23441210, 23441230, 23991400, 23991500, 24101290, 24422100, 24422450, 26114010, 26702153, 27202300, 27901390, 32502235, 32502253, 32502255, 32502259, 32502290, 32504153, 32504155, 32504159, 32504170, 32504290, 32505010, 32505020

Table A 3: Technology fields and IPC codes

Critical technology (EU definition)	Considered	Source	Abbreviation	Assigned IPC codes
Advanced semiconductor technologies	Yes	ATI (2021): Micro- and Nanoelectron-ics, Photonics	**Semiconductors**	B82Y 25, F21K, F21V, F21Y, G01D 5/26, G01D 5/58, G01D 15/14, G01G 23/32, G01J, G01L 1/24, G01L 3/08, G01L 11/02, G01L 23/06, G01M 11, G01P 3/36, G01P 3/38, G01P 3/68, G01P 5/26, G01Q 20/02, G01Q 30/02, G01Q 60/06, G01Q 60/18, G01R 15/22, G01R 15/24, G01R 23/17, G01R 31/26, G01R 31/27 , G01R 31/28 , G01R 31/303 , G01R 31/304,G01R 31/308, G01R 31/317, G01R 31/327, G01R 33/032, G01R 33/26, G01S 7/481, G01V 8, G02B 5, G02B 6 (excl. subclasses 1, 3, 6/36, 6/38, 6/40, 6/44, 6/46), G02B 13/14, G03B 42, G03G 21/08, G06E, G06F 3/042, G06K 9/58, G06K 9/74, G06N 3/067, G08B 13/186, G08C 19/36, G08C 23/04, G08C 23/06, G08G 1/04, G09G 3/14, G09G 3/32, G11B 7/12, G11B 7/125, G11B 7/13, G11B 7/135, G11B 11/03, G11B 11/12, G11B 11/18, G11C 11/42, G11C 13/04, G11C 19/30, H01F 10/193, H01G 9/028, H01G 9/032, H01H 47/32, H01H 57, H01J 3, H01J 5/16, H01J 29/46, H01J 29/82, H01J 29/89, H01J 31/50, H01J 37/04, H01J 37/05, H01J 49/04, H01J 49/06, H01L 31/052, H01L 31/055, H01L 31/10, H01L 33/06, H01L 33/08, H01L 33/10, H01L 33/18, H01L 51/50, H01L 51/52, H01S 3, H01S 5, H02N 6, H03B 5/32, H03C 3/22, H03F 3/04, H03F 3/06, H03F 3/08, H03F 3/10, H03F 3/12, H03F 3/14, H03F 3/16, H03F 3/183, H03F 3/21, H03F 3/343, H03F 3/387, H03F 3/55, H03K 17/72, H05B 33, H05K 1
Artifical intelligence technologies	Yes	ATI (2021): Artificial intelligence	**AI**	G06F 15/18, G06F 17/20-17/28, G06F 17/30∗#, G06F 17/50∗#, G06F 19/10∗#, G06K 9, G06N∗#, G06Q 30/02∗#, G06T 7, G10L 13/027, G10L 15, G10L 17, G10L 25/63, G10L 25/66
Quantum technologies	No (no meaningful assignment of IPC codes)			
Biotechnologies	Yes	Friedrichs & van Beuzekom (2018)	**Biotech**	A01H 1/00, A01H 4/00, A01K 67/00, A61K 35/12 - 768, A61K 38/00, A61K 39/00, A61K 48/00, C02F 3/34, C07G 11/00, C07G 13/00, C07G 15/00, C07K 4/00, C07K 14/00, C07K 16/00, C07K 17/00, C07K 19/00, C12M, C12N, C12P, C12Q, C40B 10/00, C40B 40/02, C40B 40/06, C40B 40/08, C40B 50/06, G01N 27/327, G01N 33/50, G01N 33/53, G01N 33/54, G01N 33/55, G01N 33/57, G01N 33/68, G01N 33/74, G01N 33/76, G01N 33/78, G01N 33/88, G01N 33/92, G06F 19/10 - 24
Advanced connectivity, navigation and digital technologies	Yes (aggregate with sensing technologies)	ATI (2021): Internet of Things, IT for mobility, Security	**Connectivity**	A61B 1/00%, A61B 5/00%, A61B 5/02%, A61B 5/04%, A61B 5/05%, A61B 5/103, G01C 11, G01C 19, G01C 21, G01S, G01V 3/17%, G01V 15/00%, G05D 1/03%, G06F12/14, G06F 17/00, G06F 19/00, G06F21, G06K19, G08B 5/22%, G08B 6/00%, G08B 13/14%, G08B 13/24%, G08B 21/00%, G08B 25/10%, G08B 29/00%, G08C 17/% , G08G, G09F 3/00%, G09C, G09F 3/03%, G11C8/20, H01Q 7/00%, H01Q 9/04%, H02J 17/00%, H04B 1/48%, H04B 1/59%, H04B 5/00%, H04B 7/00%, H04B 7/08%, H04B 7/185, H04B 10/105, H04K, H04L9, H04M1/66, H04M1/67, H04M1/68, H04M1/70, H04M1/727, H04N7/167, H04N7/169, H04N7/171, H04Q 5/22%, H04Q 7/00%, H04Q 9/00%, H04W12
Advanced sensing technologies	Yes (aggregate with connectivity technologies)			
Space and propulsion technologies	No (not separated by API (2021))			
Energy technologies	Yes	Own keyword search	**Energy**	C10L 5/40, C25B 1/02, F03D , F24S, F25B 30/00, G21B, H01L 31/04-31/05, H01M
Robotics and autonomous systems	No (no meaningful assignment of IPC codes)			
Advanced materials, manufacturing and recycling technologies	Yes	ATI (2021): Advanced materials	**Adv. materials**	B32B 9, B32B 15, B32B 17, B32B 18, B32B 19, B32B 25, B32B 27, B82Y 30, C01B 31, C01D 15, C01D 17, C01F 13, C01F 15, C01F 17, C03C, C04B 35, C08F, C08J 5, C08L, C22C, C23C, D21H 17, G02B 1, H01B 3, H01F 1/0, H01F 1/12, H01F 1/34, H01F 1/42, H01F 1/44, H01L 51/30, H01L 51/46, H01L 51/54

Source: own depiction

Centrum für Europäische Politik
FREIBURG | BERLIN

Author:

Dr. André Wolf, Head of Division Technology, Infrastructure and Industrial Development
wolf@cep.eu

Centrum für Europäische Politik FREIBURG | BERLIN
Kaiser-Joseph-Straße 266 | D-79098 Freiburg
Schiffbauerdamm 40 Räume 4205/06 | D-10117 Berlin
Tel. + 49 761 38693-0

The **Centrum für Europäische Politik** FREIBURG | BERLIN, the **Centre de Politique Européenne** PARIS, and the **Centro Politiche Europee** ROMA form the **Centres for European Policy Network** FREIBURG | BERLIN | PARIS | ROMA.

The cep institutes are specialised in the analysis and evaluation of European Integration Policy. They publish their scientific work independently of any vested interest, in favour of a European Union that respects the Rule of Law and the principles of the social market economy.