



EUROPEAN
COMMISSION

HIGH REPRESENTATIVE
OF THE UNION FOR
FOREIGN AFFAIRS AND
SECURITY POLICY

Brussels, 20.6.2023
JOIN(2023) 20 final

**JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE
EUROPEAN COUNCIL AND THE COUNCIL**

ON “EUROPEAN ECONOMIC SECURITY STRATEGY”

1. A Strategy to enhance European Economic Security

The global pandemic, Russia's illegal and unprovoked war in Ukraine, hostile economic actions, cyber and infrastructure attacks, foreign interference and disinformation and a global increase in geopolitical tensions have exposed risks and vulnerabilities in our societies, economies and companies that did not exist only a few short years ago.

Over the last years the EU has been successful both in moving forward to deliver on our priorities and at the same time in addressing vulnerabilities, whether on energy security, pandemic preparedness, or the resilience of our economies, supply chains and key technologies more generally.

However this experience has also revealed that Europe was in some cases insufficiently prepared for new and emerging risks that have arisen in the more challenging geopolitical context that we find ourselves in. The COVID-19 pandemic exposed the risks that highly concentrated supply chains can pose to the functioning of the European economy. Russia's war of aggression against Ukraine showed how an overreliance on a single country, especially one with systemically divergent values, models and interests, reduces Europe's strategic options and puts our economies and citizens at risk. Member States and businesses have also had to shoulder the cost of economic coercion, including bans of European exports and boycotts of European brands, designed to force them to comply and conform with the political priorities of another country. All these trends pose a direct risk to the functioning of our societies, economies and of global trade – as well as a direct challenge to the EU's strategic interests and ability to act.

With geopolitical tensions rising and global economic integration deeper than ever before, certain economic flows and activities can present a risk to our security. More than ever, our security is deeply intertwined with our ability to make ourselves more resilient and reduce the risks arising from economic linkages that in past decades we viewed as benign. Profound technological shifts are adding to the intensity of this competition and making the economic and security challenges more complex.

New geopolitical and technological realities requires us to adapt our approach, preserving the vast majority of Europe's highly valuable economic links to the world while ensuring that the new risks we face, which are narrow but critical, are effectively tackled.

The EU is not alone in this process: countries all over the world have started addressing challenges to their economic security. Some advanced economies have already adopted dedicated strategies and are now implementing them. Developing economies are also taking action, diversifying their economic ties to reduce harmful dependencies and increasing local production. This trend reflects the fact that only by completing traditional approaches to national security with new measures to safeguard our economic security can we ensure our prosperity, sovereignty and safety in the current age. Working together with our allies, partners, and the business sector to articulate and execute a vision of economic security will serve as a force multiplier.

While the European Union has done a lot to respond to specific challenges in recent years, it now needs a comprehensive strategic approach to economic security, de-risking and promoting its technological edge in critical sectors. The aim is to provide a framework for a robust assessment and management of risks to economic security at EU, national and business level while preserving and increasing our economic dynamism. This is all the more important to put in place at a time when these risks are both evolving rapidly and merging with national security concerns. A prime example of this is the speed with which critical new technologies are emerging and blurring the boundaries between the civil and military sectors.

The starting point for this strategy is taking a clear-eyed look at the risks and acknowledging the inherent tensions that exist between bolstering our economic security, and ensuring that the European Union continues to benefit from an open economy.

The EU is one of the most attractive destinations for global companies and for investment. **Our economies thrive on open and rules-based trade and investment, on secure cross-border connectivity and collaboration on research and innovation.** These elements will remain critical drivers of European competitiveness and resilience as we speed up the twin green and digital transitions. We need to rely on trade and on the Single Market to spur competition and ensure that we have access to the raw materials, technologies, and other inputs which are crucial for boosting our competitiveness, resilience and for sustaining current and future employment and growth. Similarly, we want our partners around the world to continue to benefit from access to the European markets, capital and technologies for their transition to a clean and resilient economy.

Getting this balance right is essential and can ensure that our economic and security interests reinforce each other. Achieving this will depend on the following three priorities: **(1) promoting our own competitiveness; (2) protecting ourselves from economic security risks; and (3) partnering with the broadest possible range of countries who share our concerns or interests on economic security.**

The priorities of an EU Economic Security Strategy

- **Promoting** our own competitiveness by making our economy and supply chains more resilient bolstering innovation and industrial capacity, while preserving our social market economy. This can be achieved by deepening the Single Market, investing in the economy of the future through sound macroeconomic and cohesion policies, NextGenerationEU, investing in human capital including by upskilling the European workforce. It will require diversifying sources of supply and export markets, or fostering the research and industrial base in strategic areas such as advanced semi-conductors, quantum computing, biotechnology, net-zero industries, clean energy or critical raw materials.
- **Protecting** ourselves from commonly identified economic security risks, by better deploying the tools we already have in place, such as on trade defence, foreign subsidies, 5G/6G security, Foreign Direct Investment screening and export controls, as well as the new instrument to

counter economic coercion. In parallel, we need to assess the effectiveness of the EU toolkit and expand it where necessary to tackle some of the new risks that we face, for instance linked to exports or outward investments in a narrow set of key enabling technologies with military applications (e.g. in the areas of Quantum, Advanced Semiconductors, Artificial Intelligence).

- **Partnering** with countries who share our concerns on economic security as well as those who have common interests and are willing to cooperate with us to achieve the transition to a more resilient and secure economy. In practice this means working together with the broadest possible range of partners to reinforce economic security, foster resilient and sustainable value chains, and strengthen the international rules-based economic order and multilateral institutions. It also means partnering with countries on similar de-risking paths, furthering and finalising free trade agreements, and investing in sustainable development and secure links throughout the world through Global Gateway.

The fundamental principles for any measures on economic security flowing from this strategy will be: **proportionality** to ensure that our tools are in line with the level of the risk and limit any negative unintended spill-over effects on the European and global economy, and **precision** to define exactly which goods, sectors or core industries are targeted and ensure that measures respond to the risks themselves.

This strategy builds on the work already started at European level, taking a critical look at the Union resilience and vulnerabilities in order to make the European economy and industry more competitive and resilient and strengthen our open strategic autonomy. This ranges from bigger investment in the green and digital transitions through NextGenerationEU and the crowding-in of more private investments to the pillars of the EU industrial policy such as the Acts on Chips, Critical Raw Materials and Net Zero Industry. This was reaffirmed by the Versailles Declaration, in which Leaders agreed on the need to strengthen European resilience and sovereignty in areas like energy, health and pharmaceutical products, food security and defense capabilities. This strategy also responds to the concerns of citizens as expressed in the context of the Conference on the Future of Europe.

Implementing this strategy will require joined-up action across internal and external policies. It will also require buy-in beyond policy makers at European and national level. The private sector will be an essential partner and is already advanced in its work on de-risking. Global asset managers have radically changed their allocations of capital in response to growing and increasingly complex risks that exist within the global economy. Seeking resilient, diversified supply chains that enhance economic security will be a core part of a long-term business strategy that protects not only shareholders' interests but also the general interest. Identifying the main risks and designing policy responses should tap into the knowledge of European companies that are already working to mitigate many of these threats.

This Communication lays the groundwork for a discussion on economic security with Member States and the European Parliament with a view to creating a common framework to de-risk and protect the Union's economic security. This Communication will help to define the strategy that should guide the common assessment of risks, the use of existing tools and the identification of possible gaps in the EU's economic security arsenal for which we will develop a common response.

2. Identifying the risks to European economic security

The aim of this strategy is to protect the EU's economic security and reinforce the resilience of our economy, while working to ensure that we maintain and grow our technological edge. This means investing in EU competitiveness, diversifying supply chains, and responding to practices such as economic coercion. It aims to prevent the leakage of sensitive emerging technologies, as well as other dual-use items, to destinations of concern that operate civil-military fusion strategies.

To reach these objectives, we need a clear-eyed view of the risks and their evolution over time.

That is why the Commission and Member States will deepen their analysis of critical supply chains, stress test them and establish the level of risk.

The Commission and the High Representative have identified the following broad and non-exhaustive categories of risks to economic security namely risks related to: (1) resilience of supply chains; (2) physical and cyber security of critical infrastructure; (3) technology security and technology leakage; and (4) weaponisation of economic dependencies or economic coercion. These risks can occur along the entire value chain, from knowledge creation and basic research to commercialisation and manufacturing at scale.

The types of risks that European economies face

Risks to the resilience of supply chains, including energy security – *Risks of price surges, the unavailability or scarcity of critical products, or inputs in the EU, including but not limited to those linked to the Green Transition, those needed for a stable and diversified energy supply and pharmaceuticals.*

Risks to the physical and cyber-security of critical infrastructure – *Risk of disruptions or sabotage of critical infrastructures, such as pipelines, undersea cables, power generation, transportation, electronic communication networks, that undermine the secure and reliable provision of goods and services or data security in the EU.*

Risks related to technology security and technology leakage – *Risk to the EU's technological advancements, technological competitiveness, and access to leading-edge technology, including through malicious practices in the digital sphere such as espionage or illicit knowledge leakage. In some cases, technology leakage risks strengthening the military/intelligence capabilities of*

those that could use them to undermine peace and security, especially for dual-use technologies such as Quantum, Advanced Semiconductors or Artificial Intelligence, and therefore require specific risk mitigation measures.

Risk of weaponization of economic dependencies or economic coercion – *Risk of third countries targeting the EU, its Member States and EU businesses through measures affecting trade or investment to bring about a change of policy falling within legitimate policymaking space.*

Finally, it is important to bear in mind that certain risks listed above could also go so far as to threaten **national security** in certain circumstances. This could be the case, most notably, with dual use technology leakage, foreign direct investment threatening security and public order; dual use exports or outbound investment in a narrow set of advanced technologies that could enhance military and intelligence capacities of actors who may use these capabilities to threaten international peace and security; and the secure treatment of sensitive information

On this basis, **the Commission proposes to identify and assess, collectively with EU Member States and with inputs from private stakeholders, risks to the EU's economic security** that threaten its key interests within clearly defined parameters, taking into account the evolving geopolitical context and, where appropriate, stakeholders' views. This should be a dynamic and continuous process.

For this purpose, the Commission proposes the following process, to be carried out with Member States and, where appropriate, in coordination with the High Representative:

- Risks to the resilience of supply chains, to be assessed by the Commission, by deepening the EU's strategic dependencies analysis, with a particular focus on dependencies that are more likely to be weaponised for geopolitical purposes.
- Risks to the physical and cyber security of critical infrastructure, to continue to be assessed in line with the Council Recommendation of 8 December 2022.
- Risks related to technology security and technology leakage, to be assessed on the basis of a list of strategic technologies critical for economic security. With regard to the most sensitive risks, the Commission will propose a list of dual-use technologies for risk assessment that could be adopted by the Council by September 2023. The list will be based on narrowly defined and forward-looking criteria such as the enabling and transformative nature of a technology, the risk of civil military fusion, and the risk of their misuse for human rights violations. The priority technologies should be assessed collectively with Member States by the end of 2023, with a view to identifying the relevant protection and promotion measures.

- Risks of weaponisation of economic dependencies or economic coercion, to be assessed including in the context of the recently agreed upon EU anti-coercion instrument.

With a view to maintaining a coherent, targeted, and up-to-date approach to economic security, the Council should review, based on input from the Commission and, where appropriate, the High Representative, the overall progress on risk assessment in these four areas every six months, and report yearly to the European Council.

Moreover, the High Representative, together with the Member States, will enhance the **Single Intelligence Analysis Capability (SIAC)** in order to increase its ability to detect threats to the EU economic security.

3. Putting the economic security strategy into action

To mitigate these risks, the EU Economic Security Strategy is based on:

- 1) **Promoting** the EU's competitiveness and growth, strengthening the Single Market, supporting a strong and resilient economy, and fostering the EU's research, technological and industrial base.
- 2) **Protecting** economic security through a range of policies and tools, including targeted new instruments where needed.
- 3) **Partnering** and further strengthening cooperation with countries worldwide.

3.1 Promoting the EU's economic base, competitiveness and growth

The Single Market is the EU's best asset to keep its economy prosperous, innovative, and resilient. It is most often associated with economies of scale for cooperating across borders within the EU and a level playing field. At the same time, through its **trade, Global Gateway investment and other policies**, the EU is leveraging the Single Market to keep global supply chains open and shape standards, which further contributes to strengthening EU competitiveness and security of supply. Implementation of the **NextGenerationEU** and of the **Cohesion Funds** are triggering major reforms and investments across a wide range of sectors, including critical infrastructures, and is already contributing to EU's economic growth, competitiveness and resilience.

In recent years, **the Commission has adopted several concrete proposals to increase resilience and strengthen supply chains.** The **EU Industrial Strategy** identified several measures to enhance the resilience of the Single Market, such as industrial alliances to accelerate activities in clean tech, raw materials, processors and semiconductors, data, edge and cloud; important projects of common European interest to pool resources for breakthrough innovations; promoting the circular economy; enhancing green and digital skills; and a new strategy to secure the EU's leadership in global standard-setting. Likewise, the energy transition in line with the European Green Deal and RepowerEU objectives is key to strengthen the EU's energy security of supply.

Significant progress has been already achieved in this area but further necessary efforts will be identified in the upcoming State of the Energy Union report.

The proposal for the **Critical Raw Materials Act** aims at facilitating the extraction, processing and recycling of critical raw materials in the EU, reducing dependencies and increasing preparedness. The **European Chips Act** will ensure a secure supply of semiconductors, while the proposed **Net-Zero Industry Act** will help scale up manufacturing of net-zero technology in the EU. The initiatives include effective governance mechanisms allowing timely cooperation and exchange of information among the Commission, the Council and Member States.

These initiatives have also a direct impact on further securing supply chains and access to resources (increasingly challenged by strategic competitors, as highlighted by the Strategic Compass for Security and Defence) which is vital for an innovative, competitive and resilient **European Defence Technological and Industrial Base**. Their timely adoption is therefore of vital importance for Europe's economic security.

The **Single Market Emergency Instrument** aims at ensuring the availability and free circulation of critical products in case of future emergencies. In the future, the Single Market Emergency Instrument will allow monitoring strategic products and services, including disruptions of supply chains and related shortages, and react fast and collectively once needed.

More investments are urgently needed both to ensure EU's leadership and competitiveness in the research and development of strategic emerging technologies. In order to crowd-in private investments, the Commission continues to develop the **Capital Market Union**. The Commission is also proposing a new Regulation to establish a Strategic Technologies for Europe **Platform ('STEP')**. This Platform will support the development, manufacturing or strengthening of the respective value chains in the Union of deep and digital technologies, clean technologies, and biotechnologies to meet the objectives of the green and digital transitions. This will enable the Union to reduce or prevent strategic dependencies.

The Commission will also report by the end of 2023 on options to ensure adequate, strategically targeted support for dual-use technology development, after reviewing the scope of existing instruments.

3.2 Protecting against economic security risks

The EU has already put in place specific de-risking tools and measures to protect against economic security risks. As the risks keep evolving, we need to assess the effectiveness of these tools in addressing them and consider upgrades or new tools that may be needed.

Addressing weaponization of economic dependencies and economic coercion

Strategic dependencies, which may give rise to economic security risks, can be exacerbated by non-market policies and practices used by third countries that tilt the playing field. The Commission will make rigorous use of Trade Defence Instruments to address such unfair

policies and practices and is ready to deploy the Foreign Subsidies Regulation to ensure a level playing field with the Single Market.

As a response to the EU and its Member States being the target of deliberate economic pressure in recent years, the EU has adopted the **EU Anti-coercion Instrument**. The instrument's objective is first and foremost to deter countries from restricting or threatening to restrict trade or investment to bring about a change of legitimate policy in the EU, but also foresees the possibility for the EU to take countermeasures as a last resort. The EU will also cooperate with partner countries to monitor instances of coercion and assess and identify the scope for coordinated responses.

Inbound investments affecting security and public order

The **Foreign Direct Investment (FDI) Screening regulation** has created a cooperation mechanism for Member States and the Commission to exchange information, raise security-related concerns and identify solutions related to specific FDIs with a view to ensuring the protection of security and public order. Since October 2020, the Commission and Member States have reviewed more than 1,000 FDI transactions. The Commission is also in the process of evaluating the current framework and will propose its revision before the end of 2023. Member States who have not yet implemented national FDI screening mechanisms should do so without further delay.

Technology security and technology leakage

Being able to develop, and keep up with, new technologies is key for the EU's economic security, as it reduces strategic dependencies and enables us to protect or create a technological advantage.

Openness and international cooperation are at the heart of European research and innovation (R&I). In order to help prevent EU-funded technology leakage, the Commission can for example, in duly justified cases exclude certain third country entities or EU entities controlled by certain third countries from participating in research and innovation and digital capacities deployment projects to protect the Union's strategic assets, interests, autonomy, or security. It can also assess the impact of the transfer of results of Horizon Europe (including intellectual property) generated by EU funded research to non-associated third countries and object to such transfers.

The Commission has also developed a **Toolkit on Tackling Foreign R&I Interference**, which helps to raise awareness and build resilience in the R&I sector across Europe at national and sectoral levels to bolster research security more broadly.

For technologies deemed to be critical for economic security (identified as per section 2 above), the Commission will, after assessment, propose measures to improve research security ensuring a systematic and rigorous enforcement of the above-mentioned tools and identifying and addressing any remaining gaps. It will do so while preserving the openness of our system, which is the bedrock for our innovative economies.

Standardization is important as part of the ‘soft power’ influence over the shape of tech developments and has therefore an indirect bearing on the EU’s economic security (including by allowing it to limit possibilities of abusive use of technologies that could threaten its economic security). As set out in the **EU standardisation strategy**, the EU needs to be able to shape international standards in line with its values and interests – and with its legal acquis. With respect to the future artificial intelligence, data or cyber resilience acts, the EU will work on European standards and towards congruent international standards together with partners. In the same vein, effective enforcement of intellectual property rights, especially patents, will also contribute to prevent technology leakage

Under its 2020 Cybersecurity Strategy, the EU is deploying measures to counter malicious practices in the digital sphere to protect from illegitimate influence, industrial espionage and illicit knowledge leakage. The proposed **Cyber Resilience Act** will improve the cybersecurity, for the public and private sector, of hardware and software sold in the Union. The EU will continue to address cyber-enabled theft of intellectual property, including by using its **EU Hybrid and Cyber Diplomacy Toolboxes**, to respond to such malicious activities.

Protecting economic security by protecting infrastructure

The EU has adopted the **Directive on the Resilience of Critical Entities** and the **Revised Directive on the security of network and information system (NIS2 Directive)**. They provide an updated and comprehensive legal framework to strengthen both the physical and digital resilience of critical infrastructure (including energy, transport, health, digital infrastructure, water and food). Further to the Council Recommendation of December 2022, targeted actions are already being carried out to ensure a common EU response to incidents.

To increase the security and resilience of 5G networks, the **5G Toolbox** establishes a set of measures to be applied by all Member States, including measures to restrict or exclude high-risk suppliers. On 15 June 2023, the Commission urged Member States that have not yet fully applied these measures to high-risk suppliers to do so without delay.

The proposed **Cyber Resilience Act** will also play an important role in securing the supply chain for the EU’s critical infrastructure. Cyber risk assessments and scenarios are also being developed specifically for the electronic communication infrastructure and energy sectors and will serve to guide actions supported under the proposed **Cyber Solidarity Act**, notably the coordinated testing of critical entities.

Better EU coordination on export controls of dual-use items

Some strategic technologies are of dual use nature and require specific attention. Under section 2 above, the EU will identify a list of technologies critical to economic security and assess their risks collectively. While subject to a multilateral and EU framework, decisions on the

implementation and enforcement of export controls of dual use items are mainly in the hands of the Member States.

The established dual-use export control architecture – with the multilateral export control regimes as standard-setters – has in recent decades addressed the Union’s security policy objectives, while at the same time nurturing openness and a conducive climate for research and innovation and non-proliferation at large. The EU will strengthen its support for the work of multilateral regimes, although its effectiveness is hindered by the fact that it is only a member of one of the existing Multilateral Control Regimes, and an observer in a second.

However, in light of the new challenges related to the increased military potential of a range of strategic technologies, Russia’s illegal war of aggression against Ukraine, heightened geopolitical tensions and risks to national security, some EU Member States and third countries have stepped up national controls to limit the export of critical technologies outside, or in some cases building on, the processes established in the multilateral export control regimes such as manufacturing equipment for advanced semiconductor chips or equipment related to quantum computing. Recent development have also shown the need for greater flexibility in the regime, to respond to current and fast changing events.

The **EU’s Regulation on dual-use export controls** was revised in 2021 to better address risks associated with the rapidly evolving security, technology, and trade environment, with a particular focus on the exports of sensitive, emerging technologies. It includes provisions that allow one Member State to introduce export controls based on another Member State’s legislation, amounting to a coordinated and cross-border effect, among EU Member States and supported by the Commission, of export controls whose implementation is a national prerogative. These provisions are currently being tested.

The need for more rapid and coordinated action at EU level in the area of export controls has become pressing as an uncoordinated proliferation of national controls by Member States would create loopholes and undermine the effectiveness of export controls and the integrity of the Single Market. As more technologies are developed that are key to national security and subject to national controls, possible divergences between Member States would weaken the economic security of the EU as a whole. To prevent this from happening, the current Regulation should be fully implemented. At the same time, a reflection should begin on building on the existing framework to develop a more coordinated European approach that goes beyond the current obligation of ensuring transparency among Member States.

The Commission will therefore **table a proposal at the latest by the end of this year to improve the effectiveness and efficiency of the current framework**. It should make it fit for purpose in the rapidly changing technology and security environment, reinforcing the capacity of the EU to play fully its role as a global actor in a context where the multilateral export control regimes are under pressure, in full respect of the EU’s and Members States’ respective competences.

Outbound investment

The EU and Member States also have a common interest in **preventing the narrow set of technological advances that are assessed to be core to enhancing military and intelligence capabilities of actors who may use them to undermine international peace and security from being fuelled by our companies' capital, expertise and knowledge.**

Strategic trade and investment controls require a holistic approach to enable us to protect our essential security interests. This raises the question on the need to subject not only exported goods, but also certain outbound investment to controls to counter the risk of technology and know-how leaking as part of that investment.

Moreover, increased cooperation is required to prevent the leakage of sensitive emerging technologies, as well as other dual-use items, to destinations of concern that operate civil-military fusion strategies, and to avoid the backfilling of any controlled exports and investments.

The Commission will examine what security risks can result from **outbound investments**, in liaison with Member States. It will set up a **new dedicated group of Member States' experts**, to assist in these tasks, building a new structured, confidential cooperation mechanism. The Commission, with input from this new expert group, will also conduct outreach and consultations activities with business and other stakeholders, and partner countries, as appropriate.

On this basis, the Commission will examine possible measures to address security risks related to outbound investments, with a view to proposing an initiative by the end of the year.

.

In sum, we need the unity at EU level for a bolder and faster use of existing EU instruments when they are required and a more assertive approach to enforcement. The EU and its Member States should ensure that these are used to their full potential to bolster economic resilience and protect essential security interests, bearing in mind also the impacts outside the EU. EU businesses should also be encouraged to integrate economic security risks in their due diligence and risk management processes. Moreover, in some areas this Communication identifies **the need to strengthen or develop new tools to match today's risks.**

3.3 Partnering on economic security

The EU cannot achieve economic security on its own. Neither can its policy response be unilateral. The global economy will remain integrated and interconnected, and effective EU action depends on cooperation and coordination with others. Transparency and cooperation are essential to ensuring that economic security policies do not have unwanted consequences on third countries, particularly on the most vulnerable ones. De-risking supply chains and mitigating disturbances involves diversification of supply and access to a diverse set of import and export markets. Moreover, the EU's vulnerabilities linked to critical dependencies in strategic sectors are

very similar to those of many other global actors, including its closest partners, while all countries are potentially vulnerable to various forms of economic coercion.

This makes a strong argument for cooperation with the broadest possible range of partners, including long-standing like-minded partners, such as the members of the G7, as well as others with whom we share common interests and who are willing to cooperate with us.

This cooperation will be flexible, and will vary in form, scope and types of participants in function of shared interests and common dependencies and depending on the specific policy area or the risks identified.

Bilateral and plurilateral cooperation

The EU is vastly expanding its bilateral and plurilateral cooperation instruments to be a nimbler actor where this is necessary for greater economic security. This is a core element of the Union's policy response, implementing the notion of security through diversification of partners. Intensive cooperation on economic security is already taking place with various partners including the **US** and **India** as part of the respective **Trade and Technology Councils (TTC)**. The EU – Japan High Level Economic Dialogue will incorporate a dedicated workstream on economic security issues.

The **G7** provides an important avenue for cooperation on economic security. The May 2023 Hiroshima Summit statement on economic resilience and economic security confirms the G7 Leaders' commitment to work together and with partners beyond the G7 to enhance global economic resilience and economic security, by building resilient supply chains and critical infrastructure, responding to harmful practices such as non-market policies and economic coercion, and preventing leakage of critical and emerging technologies.

Having **as large a geo-economic toolbox as possible** – from Free Trade Agreements to Digital Partnerships, Green Alliances and Partnerships, Raw Materials Partnerships, and the Raw Materials Club and strengthened cooperation with countries in the EU neighbourhood – allows us to respond to a broad range of economic security related challenges with the appropriate tool for greatest possible coordination and effect. We will continue to use these instruments and adapt them to better contribute to supply chain resilience and EU economic security.

We will continue to make the most of the EU's vast network of **Free Trade Agreements** through full implementation while also working to expand it. These agreements facilitate business de-risking, diversification and reduction of dependencies by opening new markets, help build mutual beneficial economic ties especially in regions where the EU would otherwise leave a void that third countries would fill, as well as support social and environmental sustainability.

A key dimension of economic security is the readiness of the EU to reinforce its **partnerships with developing countries** that could play a bigger role in global value chains. EU financial and technical support to low- and middle-income countries for industrialisation, the green transition

and bridging the digital divide is not only valuable on its own and creates positive effects for the local communities, but also contributes to our economic resilience by promoting a more diversified global economy.

In this respect, the **Global Gateway** and the **Partnership for Global Infrastructure Investments** will be key in contributing to the economic security of their beneficiaries tighten economic links and integration with global economies. These initiatives will help the EU and its partners to tackle major challenges together, including fighting climate change, deploying secure digital infrastructures, improving health systems, and achieving the Sustainable Development Goals, while offering partners sustainable alternatives to investment practices that would make them more vulnerable to economic coercion by their creditors. They also contribute to the EU's economic security, notably by helping to diversify supply chains and integrate value chains with partners in key sectors.

The EU will continue to build-up other forms of cooperation with various partners on issues of interest, for example on critical raw materials within a **Critical Raw Materials Club**.

Multilateral cooperation

At global level, multilateral cooperation and the rules-based framework provide the foundation for the economic security of the EU and all members of the international community. Even in an environment of strategic rivalry and economic competition, there is scope for international cooperation on common challenges and a need for clear rules guaranteeing fair and open trade, thus putting guardrails on the trend towards “might is right”, economic fragmentation or protectionism.

The EU's interest therefore is to strengthen multilateral cooperation through international fora and organisations such as the G20, the UN or the Multilateral Development Banks. In the trade realm, the EU will **continue efforts to reform the World Trade Organization (WTO)** and restore its dispute settlement function, given the critical role an effective WTO plays in minimising the risk of arbitrary behaviour and narrowing the scope of possible trade restrictions.

Next steps

The Commission and the High Representative, within their respective competences, will:

- develop with Member States a framework for **assessing risks** affecting the EU's economic security; this includes establishing **a list of technologies which are critical to economic security and assess their risks** with a view to devising appropriate mitigating measures.

- engage in a **structured dialogue with the private sector** to develop a collective understanding of economic security and encourage them to conduct due diligence and risk management in light of economic security concerns.
- further support EU technological sovereignty and resilience of EU value chains, including by developing critical technologies through **STEP**.
- review the **Foreign Direct Investment Screening Regulation**.
- explore options to ensure adequate targeted support for **research and development of dual-use technologies**.
- fully implement the **EU's export control regulation** on dual use and make a proposal to ensure its effectiveness and efficiency.
- propose an initiative to address security risks related to **outbound investments**.
- propose measures to improve **research security** ensuring a systematic and rigorous enforcement of the existing tools and identifying any remaining gaps.
- explore the targeted use of **CFSP instruments** to enhance EU economic security including Hybrid and Cyber Diplomacy toolboxes and foreign information manipulation and interference (FIMI) toolbox.
- instruct the **EU Single Intelligence Analysis Capacity (SIAC)** to work specifically on the detection of possible threats to EU economic security.
- ensure that the protection and promotion of EU economic security is fully integrated in European Union's external action and **intensify the cooperation with third countries** on economic security issues.

Conclusion

In an interconnected world, no country can act alone to ensure its economic security. In today's world, Member States' economic and national security interests, vulnerabilities and responses can rarely be seen or identified in isolation from those of other Member States or those of the Union as a whole. Individual Member State's interests are inextricably linked to the proper functioning of the internal market, the integrity of the EU trade policy and the security interests of the EU as a whole.

The alternative to an EU approach to economic security is that our partners will pick and choose alliances, while less well-intentioned players will seek to divide and conquer. Therefore, a common and coordinated EU action across policies, through cooperation between the EU and the Member States, is essential for the Union's economic security. The key to success will be to act in unity.