CONFEDERATION OF INDUSTRY
OF THE CZECH REPUBLIC

PRAGUE, 18 DECEMBER 2023

Making the 'European Economic Security Strategy' Fit for an Age of Digital Collaboration

Executive Summary

In June, the European Commission published the 'European Economic Security Strategy' to address the EU's supply chain vulnerabilities and exposure to economic coercion. The strategy aims to mitigate the risks of non-competitive or hostile trade practices through measures such as FDI screening and export controls, and will cover the critical technology sectors identified in the Commission's October Recommendation on 'Critical Technology Areas' – including AI, advanced semiconductors, quantum technologies, and biotech.

While we support the strategy's objective of enhancing the EU's economic resilience – robust supply chains make the EU an attractive investment destination and reassure businesses operating within its market – we are concerned that some potential drawbacks have not been sufficiently considered. Excessively restrictive export controls, for example, could hinder global collaboration and innovation across the AI, quantum, semiconductor and biotech industries, while restrictions on inbound investments could negatively impact the EU's innovation ecosystems and global market access. These restrictive measures could lead to retaliation from trade partners and undermine global partnerships.

We suggest a balanced approach that emphasizes collaboration with trusted partners, an open market economy, targeted risk mitigation, and inclusive consultation with industry stakeholders.

Context

On 20 June, the European Commission ('Commission') published the 'European Economic Security Strategy' (Strategy), laying out several steps to mitigate the EU's supply chain vulnerabilities and reduce its exposure to economic coercion. This was complemented on 3 October with the publication of the Commission's Recommendation on 'Critical Technology Areas for the EU's Economic Security', which will be subject to further risk assessments with Member States.

While the Strategy offers only a high-level framework, and will require further operational discussions, it highlights specific measures that can be used to shield the EU from non-competitive or hostile trade practices, such as FDI screening and export controls. One of the focuses of these measures will be the 'critical technology areas' identified in the Commission's October Recommendation, such as AI technologies, advanced semiconductor technologies, quantum technologies and biotech.

We, the undersigned, strongly support the objectives of the Strategy. If effective and proportionate, the EU's ongoing efforts to bolster the resilience of its economy and society have the potential to not only offer increased assurances for businesses operating in the EU market, but also make Europe an attractive destination for business investment. In this regard, a robust digital ecosystem is particularly important for the EU's economic security, as it is a core element of the resilience of the EU's economic structures and supply chains. Given our digital expertise, we are eager to play a constructive rule in shaping and operationalizing the Strategy.

Potential Risks of the 'European Economic Security Strategy'

While we welcome the outlined objectives, we are concerned that, without adequate safeguards to ensure a targeted scope – and without sufficient input from industry to ensure technical feasibility – the Strategy could harm the EU's economic competitiveness and hinder adoption of the advanced technologies that are central to the EU's 'Digital Decade' objectives.[1] These complex trade-offs will have to be considered in the ongoing discussions on how to best deliver the Strategy. Potential risks associated with certain proposed measures include:

1) Stifling global collaboration and innovation through restrictive export controls: Imposing excessively restrictive export controls on advanced technologies could stifle global collaboration and research initiatives, which have been a driving force for technological innovation. In the case of AI, untargeted export controls could significantly hinder cross-border innovation and jeopardize the 'Digital Decade' objective of achieving 75% penetration among EU companies. In the field of quantum computing, which is still a nascent technology, these controls could deter ongoing global research initiatives, hampering the EU's access to cutting-edge technologies. The semiconductor industry, which is deeply interconnected globally, could face disrupted supply chains, leading to shortages and increased costs for users and consumers. In biotech, export controls could impede global clinical trials, shared research, and collaborative drug development, delaying vital drug and treatment discoveries.

2) Deterring inbound investments and technology transfers: Foreign direct investment is a key contributor to the EU's innovation ecosystem, and has a strong positive impact on local employment and wages. While restricting certain inbound investments may prove protective in the short term, if these restrictions lack a strictly delineated focus, they could have negative long-term repercussions – particularly for smaller countries that depend on foreign investment. For sectors such as AI, advanced semiconductors, quantum computing and biotech, which are underpinned by cross-border collaboration and globalized value chains, imposing burdensome restrictions on inbound investments risks cutting off EU businesses from the funding, expertise and global market access they need. In addition, such limitations could reduce the transfer of advanced manufacturing equipment to the EU, weakening the EU's manufacturing base. As outlined in a recent study by the European Investment Bank, "FDI does not only provide needed financing for capital accumulation, but also supports the import of positive externalities in terms of new inputs and foreign technologies in the production function".[2]

3) Retaliation from trade and investment partners: If the EU's economic security measures are broadly targeted and create frictions with key trade and investment partners, such as the US and the UK, European companies may face increased regulatory headwinds abroad.[3] This would reduce their ability to expand globally, as well as potentially limit their access to resources that are not available within the Single Market. Given the strength of the EU's export sector[4], these new trade barriers would cause significant disruptions to the European economy as a whole, and particularly to smaller open economies where businesses are more reliant on a global consumer base. This would be especially challenging for the EU's digital sector, which is

[1] https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en

[2] See 2020 EIB working paper on the 'Impact of FDI on economic growth'.

[3] New trade barriers may generate retaliation in several areas where international cooperation has been vital. According to the Commission, *"the US has been the biggest third country participant in EU research and innovation programmes for many years"*.

[4] According to Eurostat, the EU's trade surplus for services exceeded €175 billion in 2022.

heavily export-oriented. According to a recent study, the EU is already "the world's largest exporter of digitally deliverable services".[5]

4) Undermining trusted global partnerships: Cross-border business partnerships are a key pillar of Europe's economic security. In the digital sector, ongoing collaborations between Europe and its trusted global partners have made the EU a hub for technological innovation, providing European organizations of all sizes with cutting-edge cybersecurity-enhancing technologies. This has bolstered the EU's resilience against cybersecurity threats and other related disruptions. Therefore, any untargeted measures that restrict the ability of European organizations to collaborate with trusted global partners could make the EU's digital ecosystem less secure.

Charting a Balanced Path: Our Recommended Approach for Economic Security

In order to realize the ambitions of the 'European Economic Security Strategy' while also fostering economic competitiveness and delivering the objectives of the 'Digital Decade' programme, the EU should anchor its approach in the following guiding principles:

1) Enhancing collaboration with trusted partners: Delivering the objectives of the 'European Economic Security Strategy' will require the joint efforts and resources of the EU and its closest partners. As summarized by the Commission in June, "the EU cannot achieve economic security on its own"[6]. Therefore, the EU should focus on strengthening ties and developing interoperable solutions with trusted partners who share its fundamental interests and values. International collaboration is particularly important to enhance the resilience of digital value chains. According to a recent study, if the EU and its trusted partners fail to aggregate their research capabilities, they will be at the forefront of research output for only 7 of 44 critical technologies.[7] This data underscores the urgency of deepening technological cooperation with partners, in line with the Commission's 2021 Communication on a 'Global Approach to Research and Innovation'. Instead of reinventing the wheel, the EU can build off existing and emerging governance models, such as the G7's ongoing Data Free Flows with Trust (DFFT) initiative, or the OECD workstream around trusted government access to data, which can act as a robust foundation to develop resilient multilateral solutions.

2) Championing an open market economy: The EU's economic openness is key to Europe's attractiveness as a destination for business investment. Given the cross-border nature of the global digital economy, open markets will continue to be a driving force for the growth and vitality of the EU's economy, creating opportunities for businesses of all sizes to grow, and providing consumers with a wider array of choices. Therefore, reaffirming support for an open market approach (including by tackling existing barriers to intra-EU trade), and taking a global leadership role to underscore the benefits of international trade, will help deliver economic security within an environment where innovation thrives, competition remains healthy, and businesses have the freedom to expand and collaborate. This approach is in line with the May 2023 G7 leaders' statement on 'Economic Resilience and Economic Security', which emphasizes that the pursuit of economic security should be "rooted in maintaining and improving a well-functioning international rules-based system, in particular the multilateral trading system". In a context where the global rules-based order is being increasingly challenged, it is incumbent upon the EU and its trusted partners to stand up for it and enable global solutions to global problems, from climate change to the risks posed by emerging technologies.

3) Targeted and proportionate risk mitigation: Preserving the EU's economic openness will require economic security measures to be narrowly targeted. This will demand a careful assessment of risks based on clear,

[5] See the Jacques Delors Institute's 2023 'Mapping the EU's digital trade' paper.
[6] https://ec.europa.eu/commission/presscorner/detail/en/IP_23_3358
[7] See ASPI's 2023 'Critical Technology Tracker'.

evidence-based and transparent criteria, as well as weighing the potential impacts of new measures on economic activity and trade flows. In light of these assessments, the EU must prioritize measures that are proportionate to the economic and security risks identified. By ensuring that measures are well-targeted, the EU can safeguard its interests without compromising the integrity of global trade and partnerships. Although the Strategy recognizes this trade-off, and the importance of carefully measuring risks, there is a lack of procedural and methodological clarity on how this will be achieved.

4) Timely, inclusive and transparent consultation with industry stakeholders: Economic security measures will have to be implemented by individual businesses, who will be required to design the appropriate compliance solutions and bear the brunt of the associated costs. In order to minimize these costs, leverage industry expertise and avoid supply chain disruptions, the EU should consult with a broad range of industry stakeholders to ensure that its economic security measures are technically and economically feasible. For example, as the EU is currently working on preparing EU-coordinated risk assessments as part of its recently published Recommendation on critical technologies, it is critical that the industry consultation process is conducted in a way that is as structured and thorough as possible, ensuring the necessary time for the relevant stakeholders to provide valuable input.

Conclusion

In order to develop a targeted, transparent and risk-based approach anchored in an open economy, strong partnerships and a level playing field for all, we encourage policymakers to foster a collaborative dialogue with industry, ensuring that its collective insights and expertise guide the EU towards agile, adaptable and global solutions that are fit for the digital age, and ultimately benefit the EU's economy and citizens. On our part, we stand ready to contribute to this process, including under the umbrella of the Belgian EU Presidency and Ireland's D9+ Chairmanship.

AAVIT

adigital

ASSINTEL
ASSOCIAZIONE NAZIONALE
IMPRESE ICT

CYFROWA POLSKA

Danish Industry

FEDIL
The Voice of Luxembourg's Industry

LEWIATAN

NATIONAL UNION
NUE
OF EMPLOYERS

sapie

sp
CONFEDERATION OF INDUSTRY
OF THE CZECH REPUBLIC