REINFORCING EUROPEAN ECONOMIC SECURITY AND CYBER RESILIENCE: GETTING REAL ON STRATEGIC AUTONOMY

Dimitar Lilkov
Wilfried Martens Centre for European Studies

Abstract

Within its current mandate, the European Commission has demonstrated a growing ambition on the EU's positioning on the global stage. From „strategic autonomy" to „geopolitical Union", the bar has been set high. In reality, however, there has been modest progress in truly bolstering the EU's collective toolbox on the supranational level for mitigating economic risks or digital threats from external actors. This article takes stock of the recent Commission strategy on economic security and proposed legislation on improving cyber resilience.

The text analyses the current proposals and makes the case that member states are long overdue in developing improved tools for screening of foreign direct investments, better coordination on the export of dual-use items and preventing the leakage of advanced research and European knowhow to third countries. Moreover, these measures need to be coupled with an upgraded notion of cyber resilience given all the threats stemming from adversarial state and non-state actors, exposure of critical digital infrastructure, compromised Internet of Things devices, as well as malign software and digital applications online. The upcoming Commission mandate (2024-2029) will be crucial for making these ambitions a reality and responding to the rapidly expanding geopolitical challenges and external threats.

Keywords: Economic security - Cyber resilience - Strategic autonomy

Introduction

Scholars of European integration tend to use the famous motto that „*Europe will be forged in crises*" to describe particularly challenging periods of European history. Relevant as ever, the Monnet quote[1] has been specifically applicable

[1] Monnet, J. (1976), *Memoires,* Fayard

to the current '19-'24 mandate of the European Commission. From pandemic peril to energy emergency and a hot war next to its borders, the European Union (EU) has faced a number of severe challenges. Rising to the occasion, national political leaders and European policymakers achieved a series of breakthroughs which delivered on several pressing matters ranging from fiscal to military. The changing geopolitical environment prompted the European institutions to promote a new set of purpose linked with European autonomy and enhancing overall resilience. A number of policy documents[2] from the last half decade permeate with references to „strategic autonomy", „strategic sovereignty" or „resilience". The delivery of the European Recovery and Resilience fund, a reinvigorated common defence policy and joint European response to Russia`s war in Ukraine lend support to the narrative of improved European autonomy.

Looking more closely into the Union's regulatory toolbox, however, shows a number of deficiencies. The EU has a limited number of supranational tools for responding to external trade or economic coercion, as well as an under-developed defensive arsenal for dealing with malign digital threats. This situation has its explanation in the history and dynamics of European integration in the last several decades during which the EU positioned itself as one of the champions of multilateralism and free trade in times of relative peace, liberalised global trade and shared optimism about the benefits of globalisation. Moreover, unlike the United States, the EU never shaped or enforced its economic and international policies through the prism of safeguarding „national security".

Even though „European national security" can be a debatable notion in theory, political leaders seem to agree that, in practice, it is currently under threat. The current article explores the recent proposals of the European Commission for enhancing economic security and aims to analyse the current track record of several supranational initiatives related with foreign direct investment, export controls and enhancing European research security. The article also makes the case that the EU needs to seriously expand its efforts and toolkit for dealing with external threats coming from foreign hardware or software and bolster its overall digital resilience.

Referring back to Jean Monnet's maxim, it is important to consider the citation in full: *„Europe will be forged in crisis, and will be the sum of the solutions adopted for those crises"*. The often omitted second part holds the key to his vision. It is not the crisis and threats *per se* that guarantee European advancement; it is the solutions, the shared will to improve the Union and its policies. This article makes the case that the upcoming EU institutional cycle will witness several breakthroughs and expanded European competences in economic security and digital resilience – touching upon sensitive areas of national prerogative and economic interests.

---

[2] European Parliament Research Service (2022), *„EU strategic autonomy 2013-2023"*, Briefing note

Economic Security

In January 2024, the EC proposed a series of new initiatives aiming to reinforce European economic security while also preserving high trade and investment flows.[3] The rationale for putting forward these measures was laid out earlier in 2023 by the Commission and European External Action Service where both institutions pinpointed a series of risks related to external economic coercion, vulnerability of critical (digital) infrastructure as well as risks to technology leakage.[4] The 2024 EC Communication proposes the following initiatives: improved Foreign Direct Investment (FDI) screening into the EU; more coordinated approach to export controls and better control of the dual-use goods export; identification of potential risks stemming from outbound investment; enhancing specialised Research and Development (R&D) and research security at national and sector level. This section analyses all these proposals in turn by tacking stock of the previous policy background, main challenges faced by member states and potential institutional developments in the upcoming EC mandate.

Foreign Direct Investment Screening

Positive FDI flows and growing economic investment from abroad are one of the indicators of economic success. Traditionally, FDIs and their potential scrutiny were solely the concern of member states. In 2016, however, two major developments happened which raised the question of economic interference and protecting European interests. In mid-2016, a Chinese firm acquired ownership of German robot maker company Kuka, known for specialised production of advanced robotic units which are used in car and aircraft manufacturing.[5] Later the same year, the Chinese shipping company Cosco acquired the majority shares in the Greek port of Piraeus.[6] These developments pushed forward the debate about potential external economic influence through strategic investment and whether European countries should protect European companies producing high-value products and services. Not to mention the fact that there could be negative effect for the European single market as a whole if third country FDIs provide control over critical physical or digital infrastructure.

In 2019, the EU adopted its Regulation establishing a framework for FDI screening coming into the Union.[7] The new rules set out minimum requirements for establishing national FDI screening mechanisms and a procedure for the

---

[3] European Commission (2024), *Communication on Advancing European economic security: an introduction to five new initiatives,* COM(2024) 22 final

[4] European Commission (2023), *Communication on European Economic Security Strategy*, JOIN(2023) 20 final

[5] Charzan, G. (2016), *Berlin and Brussels wary of Chinese robotics bid,* Financial Times

[6] Bali, K. (2022), In Greece's largest port of Piraeus, China is the boss, Deutsche Welle

[7] Official Journal of the European Union, *Regulation (EU) 2019/452 establishing a framework for the screening of foreign direct investments into the Union,* 19 March 2019

coordination of FDI reviews. Most importantly, the Commission encouraged each member state to set up their own national screening procedures, as more than a third of EU member states did not have such a mechanism at place.[8] The Commission only had a coordination role where different member states could comment on specific FDIs coming in another EU member state. The EC was given the right to provide an opinion on FDIs capable of affecting EU-funded projects (e.g. Horizon Europe research programme) or critical EU infrastructure.[9] All final decisions on approving or prohibiting the considered FDIs is up to the respective member state.

The latest EC annual report on the FDI screening progress from late 2023 notes that all EU member states have an FDI mechanism in place or are currently working on the adoption of such tools.[10] Overall, the coordination of FDI screening in the EU has provided thousands of cases with the majority of them greenlighted by the respective member states without any conditions. In 2023, in 9% of the transactions the Member States imposed mitigating measures as a condition for the go ahead of the transactions while only 1% were blocked by the respective member state.[11]

Almost five years after the entry into force of the original FDI Regulation, there is a wide set of divergence among member states about the application of investment screening, lack of proper harmonisation and national differences when it comes to the specific economic sectors that are covered by such a procedure. The 2024 EC proposal for revising the FDI Regulation puts forward a number of suggestions for better harmonisation of national procedures, as well as identifying the minimum sectoral scope in order to apply to critical areas such as semiconductors, artificial intelligence, critical medicines and military items.[12] An important improvement would also be the extension of the investment screening to the ones coming from „internal" EU investors which are actually controlled by individuals or entities which are non-EU nationals and potentially represent the interests of a third country.

Export controls of dual-use goods

The category of „dual-use" items apply to certain goods, software or hardware technology that can be used for civilian and military applications. These can include certain electronics, sensors, navigation technologies, aerospace and propulsion systems, nuclear materials and a wide array of chemicals, among others. Export controls have been traditionally used by individual countries or

---

[8] Riela, S. (2023), *The EU's foreign direct investment screening mechanism two years after implementation*, European View Journal, 57-67

[9] Art. 8 of Regulation 2019/452

[10] European Commission (2023), *Third Annual Report on the screening of foreign direct investments into the Union*, COM(2023) 590 final

[11] Ibid, 13

[12] European Commission (2024), EU Foreign Direct Investment Screening 2024 Revision, Factsheet

as part of multilateral treaties for ensuring the non-proliferation of certain technologies and the preservation of international peace and human rights. During the Cold War, the US together with European and international allies had a multilateral arrangement for denying certain exports to the Soviet Union.[13] In the early 90s, this grouping was transformed into the Wassenaar Arrangement which pursued multilateral export controls among Western allies but also included countries such as Ukraine, Russia, South Africa and India. In 2021, the EU adopted its framework (the „Dual-Use Regulation") for ensuring the coordination between member states` export control authorities and an annually updated list of control items, which every EU country must follow.[14]

In October 2022, the world of export controls and was shaken by the announcement that the United States will unilaterally impose restrictions on the export of advanced chips, semiconductor equipment and related components to the People's Republic of China due to potential threats to the US national security and.[15] What was striking in this case was the wide scope of restricted items, as well as the Washington's claim for the extraterritorial application of these restrictions, with the expectation that other US partners would also impose similar export controls vis-à-vis China. This was followed by extensive diplomatic pressure which resulted in the Netherlands and Japan also applying similar export restrictions against China, even though it negatively affects the international sales of their companies that specialise in chip manufacturing.[16] This dynamic raised concerns about the current operations of the EU export controls regime and whether EU member states should be able to move jointly on such decisions in order to coordinate a Europe-wide response, not individual member state actions. The impetus for reconsidering the EU's treatment of dual-use exports also comes from the current logjam within the wider multilateral agreement which includes all EU member states. Any type of progress within the Wassenaar agreement mentioned above is currently blocked by the Russian Federation which opposes any new changes and prevents all the current members to update the old framework and feature novel technologies.

These developments prompted the EC to put forward its new White Paper on Export controls that drafts several suggestions for improving the currently existing EU Dual-Use Regulation from 2021. The Commission wants to improve the consultations process between member states before updating export controls lists and make sure that the Union collectively moves forward on the restrictions on dual-use items, especially in a global context of fast technological change.

---

[13] The Coordinating Committee on Multilateral Export Controls (COCOM)

[14] Official Journal of the European Union (2021), *Regulation EU 2021/821 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast)*

[15] Bureau of Industry and Security (2022), *Commerce Implements New Export Controls on Advanced Computing and Semiconductor Manufacturing Items to the People's Republic of China (PRC)*, Press Release

[16] Alper, A. and Sheapardson, D. (2023), *U.S. official acknowledges Japan, Netherlands deal to curb chipmaking exports to China,* Reuters

The EC additionally wants to have an increased role in the negotiations of potential export controls and also expand the current EU control list of restricted item, together with better procedures and transparency on updating these items annually.[17] Finally, the Commission proposes bringing forward the evaluation of the current Regulation 2021/821 to early 2025 (instead of 2026) which signals the sense of urgency when it comes to providing the Union with a uniform set of rules on limiting the export of dual-use items internationally.

Outbound investment

Together with its new proposals on FDI screening and export controls coordination, the latest January 2024 Economic security package by the EC puts forward a proposal for the monitoring of EU outbound investment. It appears that the Commission wants to approach all angles of economic risks and even cover the touchy subject of private investments in third countries. Here, the EC is not focusing on all potential outbound investment but rather a very narrow type of key technologies which might be used for enhancing the military or intelligence capabilities of hostile actors against global security. In late 2023, the EC recommended[18] that advanced semiconductors, advanced artificial intelligence systems, breakthrough quantum and biotechnologies be considered as of critical importance for the economic security of the Union. There has never been an official discussion about monitoring (or restricting) European outbound investment on the supranational level.

With the 2024 White paper on outbound investments the EC wants to push forward an EU-wide consultation due to the substantial knowledge gaps on the level of investments in advanced technologies, the potential risks and address the fact that there is no existing monitoring on national or EU level.[19] Currently there is an internal working group featuring member state experts followed by a consultation stage in 2024. In the next one year, the EC will also conduct an assessment together with national capitals to pinpoint the potential risks of certain outbound investments and what would be the most appropriate future measures.

This EC initiative is riddled with uncertainties due to the sensitivity and complexity of monitoring and analysing specific outbound investments. There are numerous questions regarding the potential scope of such initiative, access to reliable data and objectively assessing the long-term vulnerabilities. The willingness of certain member states or specific business communities to take part and openly share information on investment flows is far from certain. However, starting the discussion and objective risk assessment on outbound investment in key advanced technologies is an essential step in exposing risky

---

[17] European Commission (2024), *White Paper on Export Controls*, COM(2024) 25 final, 12-13

[18] European Commission (2023), *Recommendation critical technology areas for the EU's economic security for further risk assessment with Member States*, C(2023) 6689 final

[19] European Commission (2024), *White Paper on Outbound Investments*, COM(2024) 24 final

trends and encourage European member states to consider additional measures at national or EU level.

Enhancing R&D Support and European Research Security

The EC wants to further improve the EU's standing on global competitiveness by expanding the scope of advanced technology research conducted in Europe. With its latest White paper [20] on options for enhancing support for research and development involving technologies with dual-use potential, the European executive wants to promote better spillovers between civil, defence and space R&D in the EU. Currently, landmark EU programmes like Horizon Europe or the European Defence Fund pursue ambitious goals and operate huge budgets but remain fragmented or managed in silos. The new EC White paper lays out different avenues for consideration before member states with the aim of scaling technology research and opening up opportunities for funding European programmes that can have defence or military application, not only civil. In essence, the EU recognises that global actors such as the US and China pursue their own strategies of military-civil fusion where defence companies, universities and research institutions collaborate on breakthrough innovation.

Finally, the January 2024 package includes a proposal for a Council recommendation on enhancing research security. This is prompted by rising concerns about specific knowledge and technology leakage from the EU to third countries. Even though research and education remain a national competence, the European Commission is sounding the alarm about international research collaborations. For example, for years now there have been allegations about Chinese espionage or deliberate research agreements with EU academic institutions which benefits Chinese interests.[21] The Netherlands has already considered legislative proposals for thorough checks on third-country PhD students which want to do technical research in Dutch universities.[22] The Commission is advising the inclusion of risk appraisals for research institutions and specific due diligence procedures when dealing with international projects. The Commission has also pledged to create a European centre of expertise on research security in order to provide guidance and best practices for European research organisations.

Cyber resilience

During the current mandate, the European institutions demonstrated a growing ambition in the digital domain. From new rules against digital monopolies which disrupt fair competition online to regulating the use of AI across the continent, the EU is trying to set the global golden standard for novel regulation fit for the

---

[20] European Commission (2024), *White Paper on options for enhancing support for research and development involving technologies with dual-use potential*, COM(2024) 27 final

[21] Aneta Zachova et al., (2023), *EU academia accepts Chinese money in return for know-how*, Euractiv

[22] Reuters (2023), *Dutch government to screen foreign PhD tech students, denies targeting* China

digital age. In parallel to these efforts, the European institutions have also made progress on the development of tools for common „digital defence" that ensure a high-level of cybersecurity, protection of hardware devices and secure digital infrastructure. Notably, the EU updated its previous cybersecurity rules with the revamped NIS2 Directive which updated the current regulatory framework. The updated text aims to address the evolution of highly complex cyber threats, as well as protecting the expanding attack surface due to increased vulnerabilities from growing use of digital devices and software.

The EC's efforts to ensure better digital protection culminated in September 2022 with the proposal of the Cyber Resilience Act (CRA). The Regulation introduces a number of obligatory conformity assessments and stringent cyber-security requirements by design and by default for most of the user products that have digital elements. Manufacturers are obliged to provide security support and the necessary software updates so that the whole European single market has the same basic protection for the majority of digital devices. The CRA has been approved by the European Parliament, but the text is yet to be formally adopted by the Council. The final confirmation of the text will likely come in the beginning of the new institutional mandate.

One must not assume that a high-level of software cybersecurity can guarantee the security and protect the interests of European users and businesses. In the age of ubiquitous connectivity, the European Commission actively tried to advise member states on strengthening the security requirements for network operators and avoid dependence on single suppliers of hardware services. This was specifically pertinent to 5 G network security where certain suppliers might be considered high-risk and pose a threat to core network functions or enable large-scale surveillance. The 5G security toolbox of 2020 specifically designed several recommendations for the roll-out of secure infrastructure which fulfils common security standards and makes sure that each member state has the same level of minimum protection. The EC event went so far as to recommend that member states avoid exposure to Chinese companies Huawei and ZTE which are considered as high-risk vendors.[23]

The current Commission has certainly set-up the fundamentals for Union-wide cyber resilience, but much remains to be done in the upcoming mandate. Implementation of these rules and overcoming the reluctance of all member states to step up remains a challenge. For example, even though the EC's 5 G toolbox clearly outlines the risks behind using untrusted vendors, just 10 EU countries have excluded risky suppliers from the digital networks.[24] There is a clear risk here with many of these member states becoming depended on only one specific network vendor and getting locked-in in the future. Given the complexity of 5 G networks, cloud infrastructure and growing in popularity

[23] European Commission (2023), 5G Security: The EU Case for Banning High-Risk Suppliers, Statement by Commissioner Thierry Breton

[24] Kroet, C. (2024), *Most EU members not implementing Huawei, ZTE 5G ban, data* shows, Euronews

Internet of Things (IoT) devices the European executive must push forward additional tools and *ex ante* measures (standards and certifications) for protecting European interests.

Enhancing supranational tools in this domain comes from practical necessity. An expanded toolkit is necessary to limit the threats from compromised ICT products/services (and apps) which could serve the purposes of foreign adversaries. Here, the EC needs to consider a more comprehensive blueprint for digital deterrence. It would be interesting to observe whether the Commission pushes for better harmonization of software and app security. An ambitious idea for consideration is also the option for the EC to flag certain applications or software services as 'malign' or going against pre-defined European standards.

Conclusion

For years now, „Strategic autonomy" has become a trendy narrative and a widely debated theoretical concept. During the next EU institutional mandate, the EC should remain focused on concrete measures and add „more flesh to the bone" by expanding the necessary toolkit for handling economic coercion and improving cyber resilience. These efforts would also correspond to the recent progress of novel supranational tools in the field of trade (e.g. the Anti-Coercion Instrument) or protecting the integrity of the single market (e.g. the Foreign Subsidies Regulation). All these proposals and new instruments send an important signal that European capitals are wary of the new types of challenges ahead and recognise the need for strengthened collective action in several important domains.

It is interesting to note that the EC is venturing in novel waters in sensitive areas which were historically solely the prerogative of European member states. Perhaps these developments lend support to authors such as Alan Milward who see pure economic necessities (or threats to economic interests) as the main reason for sovereign member states to „surrender" certain competences to the supranational level.[25] Or we might consider more contemporary scholars such as Luuk van Middelaar who sees the EU as a community driven and changing mostly due to transformative world events, rather than norm-setting and institutional rules.[26]

Such a theoretical discussion remains outside the limits of the current article. What we can state with certainty is that all current and proposed EU policies on economic security and cyber resilience signal that the Union is adapting to a reality of increasing economic coercion, external threats and a dramatically changing geopolitical landscape. Only a nimble and ambitious legislative agenda in the next mandate can respond to such challenges.

---

[25] Milward, A. (2000), *The European Rescue of the Nation State*, Routledge, 2nd ed., London

[26] Van Middelaar, L. (2020), *Alarums and Excursions: Improvising Politics on the European Stage*, Agenda Publishing

Bibliography

- Aneta Zachova et al., (2023), *EU academia accepts Chinese money in return for know-how*, Euractiv, accessed https://www.euractiv.com/section/politics/news/eu-academia-accepts-chinese-money-in-return-for-know-how/ on 25 May 2024
- Reuters (2023), *Dutch government to screen foreign PhD tech students, denies targeting China,* 12 June 2023, accessed https://www.reuters.com/world/europe/dutch-government-screen-foreign-phd-tech-students-denies-targeting-china-2023-06-12/ on 25 May 2024
- *Kroet, C. (2024), Most EU members not implementing Huawei, ZTE 5G ban, data shows,* Euronews, accessed https://www.euronews.com/next/2024/02/12/most-eu-members-not-implementing-huawei-zte-5g-ban-data-shows on 25 May 2024
- Alper, A. and Sheapardson, D. (2023), *U.S. official acknowledges Japan, Netherlands deal to curb chipmaking exports to China,* Reuters, accessed https://www.reuters.com/technology/us-official-acknowledges-japan-netherlands-deal-curb-chipmaking-exports-china-2023-02-01/ on 25 May 2024
- Bureau of Industry and Security (2022), *Commerce Implements New Export Controls on Advanced Computing and Semiconductor Manufacturing Items to the People's Republic of China (PRC)*, U.S Department of Commerce, Press Release accessed https://www.bis.doc.gov/index.php/documents/about-bis/newsroom/press-releases/3158-2022-10-07-bis-press-release-advanced-computing-and-semiconductor-manufacturing-controls-final/file on 25 May 2024
- Riela, S. (2023), *The EU's foreign direct investment screening mechanism two years after implementation*, European View Journal Vol. 22(I), accessed https://journals.sagepub.com/doi/pdf/10.1177/17816858231164292 on 25 May 2024
- Bali, K. (2022), In Greece's largest port of Piraeus, China is the boss, Deutsche Welle, accessed https://www.dw.com/en/greece-in-the-port-of-piraeus-china-is-the-boss/a-63581221 on 25 May 2024
- Charzan, G. (2016), *Berlin and Brussels wary of Chinese robotics bid,* Financial Times, accessed https://www.ft.com/content/acbda1cc-3186-11e6-bda0-04585c31b153 on 25 May 2024
- European Parliament Research Service (2022), „*EU strategic autonomy 2013-2023: From Concept to Capacity*", Briefing note, accessed https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)733589 on 25 May 2024