



OPINION

European Economic and Social Committee

Roadmap on security and defence technologies

Roadmap on security and defence technologies
[COM(2022) 61 final]

CCMI/189

Rapporteur: **Maurizio MENSI**

Co-rapporteur: **Jan PIE**

www.eesc.europa.eu

EN

Referral	European Commission, 02/05/2022
Legal basis	Article 304 of the Treaty on the Functioning of the European Union
Section responsible	Consultative Commission on Industrial Change
Adopted in section	24/06/2022
Adopted at plenary	14/07/2022
Plenary session No	571
Outcome of vote (for/against/abstentions)	165/1/3

1. **Conclusions and recommendations**

- 1.1 The EESC fully supports the objectives of the Roadmap on Critical Technologies for Security and Defence, which is particularly timely due to the Russian aggression against Ukraine, namely enhancing research, technology development and innovation, and reducing the EU's strategic dependencies in critical technologies and value chains for security and defence.
- 1.2 The EESC welcomes the ambition shown in the goal of developing a comprehensive approach that spans across the civil-military dividing line and combines the EU and national levels. This endeavour is as complex as it is challenging and will not happen overnight, but should be done with high speed. The invasion of Ukraine is a wake-up call to act much faster than usual.
- 1.3 The EESC calls on the Member States to ensure that their immediate responses to the Russian aggression against Ukraine are in line with the content and objectives of the Roadmap, which is a long-term endeavour. Short-term national defence investments must be coordinated at European level to avoid an extension of fragmentation and duplication; off-the-shelf procurements from third countries must not stifle ongoing or planned European development projects.
- 1.4 The EESC recommends that the Observatory of Critical Technologies (OCT) be equipped with clear governance, substantial resources and a strong institutional standing. The EESC welcomes the proposed close coordination with the Member States and calls for an additional forum for exchanges with industry, which has the best knowledge of technologies, supply chains and critical dependencies.
- 1.5 The EESC believes that the uptake of OCT results into roadmaps and their translation into flagships must be ensured. The transition between the different phases of the technology and industrial cycle can only be managed successfully if the ownership of an initiative and responsibilities are clear. Coherence and synergies are needed not only horizontally, between civil and defence RTD&I programmes, but also vertically, between RTD&I and deployment programmes.
- 1.6 The EESC believes that simplification and streamlining of EU programmes and instruments in support of RTD&I are fundamental, for the benefit of the recipients themselves.
- 1.7 The EESC proposes the establishment of an online one-stop shop for SMEs and start-ups, an online "EU SMEs' corner", offering the possibility to enter predefined data and receive in return tailor-made information about the best-suited EU programme(s) that can provide support.

2. **Background**

- 2.1 The Roadmap on Critical Technologies for Security and Defence responds to the European Council's request of 25-26 February 2021, namely to outline a path towards enhancing research, technology development and innovation, and reducing the EU's strategic dependency in the area of critical technologies and value chains for security and defence.

- 2.2 The update of the new 2020 Industrial Strategy ("Building a Stronger Single Market for Europe's Recovery" in May 2021) confirmed that technology leadership remains a key driver of EU competitiveness and innovation, particularly for critical technologies. The Commission's February 2021 Action Plan on Synergies between Civil, Defence and Space Industries recognised the growing importance of disruptive and enabling technologies originating in the civil sector for Europe's security and defence, and the need to promote cross-fertilisation between civil and defence technologies.
- 2.3 Hence the decision to draw up the Roadmap, a strategic document that aims at developing a comprehensive approach towards defence and security technologies, across the civil-military dividing line and combining both EU and national programmes. The Roadmap's objective is to strengthen Europe's technological sovereignty in key strategic sectors by enhancing the coherence of all relevant EU policies and instruments, from Horizon Europe to the European Defence Fund, from the Chips Act¹ to the Data Act², from the Foreign Direct Investment Control Regulation³ to the Foreign Subsidy Control Regulation⁴, and from the proposed NIS 2 Directive⁵ to the CER Directive⁶. The document outlines a wide-ranging conceptual policy framework that touches on several interconnected topics, with the objective of contributing to the EU's "strategic compass" on security and defence⁷. It was issued together with a Communication on the Commission's contribution to European defence, which calls for a more integrated and competitive European defence market in a constantly evolving geopolitical and technological context, in particular by strengthening cooperation within the EU, decreasing costs and improving operational effectiveness.
- 2.4 The Roadmap on Critical Security and Defence Technologies outlines a path towards improving the competitiveness and resilience of the EU security and defence sectors based on the following elements: mapping critical technologies and strategic dependencies, monitoring and assessing critical technologies and supply chains, technology gaps and dependencies (through the Observatory on Critical Technologies currently being set up); encouraging dual-use research and innovation at the EU level; inviting the Member States to develop a coordinated EU-wide approach to critical technologies in the context of the strategic compass; supporting innovation and entrepreneurship in security and defence through a range of new tools; and creating, together with the European Defence Agency, an EU Defence Innovation Scheme to bring together their respective efforts under a single "umbrella".

1 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A Chips Act for Europe, COM(2022) 45 final, 8 February 2022.

2 Proposal for a regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), COM(2022) 68 final, 23 February 2022.

3 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, OJEU 21 March 2019, L 79.

4 Proposal for a regulation of the European Parliament and of the Council on foreign subsidies distorting the internal market, COM(2021) 223 final, 5 May 2021.

5 Proposal for a directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing directive (EU) 2016/1148, 16 December 2020, COM(2020) 823 final.

6 Proposal for a directive of the European Parliament and of the Council on the resilience of critical entities, COM(2020) 829 final, 16 December 2020.

7 Council of the European Union Brussels, 21 March 2022.

2.5 An important aspect of the Roadmap is the goal of reducing identified dependencies in the area of critical technologies and value chains. With this in mind, the Commission proposes integrating defence considerations, where appropriate, into key EU industrial and technology initiatives (e.g. alliances and standards), reporting on the need to carry out risk-assessments on supply chains of critical infrastructure (particularly in the digital sector), and strengthening foreign direct investment screening by encouraging all Member States to establish a national screening mechanism.

3. **General comments**

3.1 The Roadmap accurately reflects the evolving technology landscape, where critical technologies for security and defence are increasingly driven by innovation from commercial sectors. The EESC welcomes the Commission's intention to develop a comprehensive approach across the civil-military divide, combining the EU and national levels. However, this will be a challenging and complex task, as it implies a general reconfiguration of the current approach. This will not happen overnight, but should be done with high speed. The EESC firmly believes that the Russian invasion of Ukraine must be viewed as a wake-up call to act much faster than usual.

3.2 At the same time, the EESC would stress that the Roadmap is a long-term plan and care must be taken not to create a disconnect with Member States' current procurement decisions aimed at closing the most urgent capability gaps as quickly as possible. The EESC strongly believes that national short-term investments must be coordinated at the European level to avoid an extension of fragmentation and duplication, and to ensure that off-the-shelf procurements from third countries do not undermine the EDTIB by stifling ongoing or planned European development projects.

3.3 The EESC also takes the view that in order to foster synergies, it is important to look not only at individual technologies and value chains, but also at the ecosystem in which these value chains are embedded. Indeed, technology transfers are most likely to occur (or start) between companies within such an ecosystem.

3.4 The attention given in the Roadmap to dual-use technologies and synergies between security, defence and space is important for achieving the EU's aims in these areas. At the same time, dual-use and synergies are neither ends in themselves nor sufficient. The overarching objective of the Roadmap is for the EU to become resilient and able to defend itself also against large-scale attacks (hybrid and military). This means that there is a need to also scale up investment in defence and security and to include in the Roadmap "pure" defence technologies.

3.5 The EESC calls upon the EC to make an assessment of the economic and social cost of critical dependencies and the absence of technological sovereignty in defence.

4. **Specific comments**

4.1 The Observatory of Critical Technologies (OCT) will be the centrepiece of the proposed approach. It will identify, monitor and assess critical technologies, their potential application and related value and supply chains, and monitor technology gaps and root causes of strategic

dependencies and vulnerabilities. To fulfil these tasks, the EESC underlines the need to equip the observatory with substantial resources, a strong institutional standing and clear governance.

- 4.2 The EESC believes that it is important to understand how the observatory will be established and how it will operate in practice. To fulfil its remit, the OCT needs to establish objectives, rules and criteria for assessing technologies. To identify critical technologies, it will have to establish close links with capability-needs identification and planning processes, and in order to match capabilities with technologies, it will have to develop a suitable taxonomy that will ideally be applicable to defence, security and space. Here, it is essential that the OCT works closely with the EDA and others. Finally, if it is to identify critical dependencies, the OCT will have to gather a very robust knowledge and understanding of the underpinning value and supply chains.
- 4.3 The plan is to present a classified report to the Member States once every two years. The EESC questions this long interval between reports, given the rapidly evolving technological and industrial environment. The information collected by the observatory will be highly sensitive, as mapping critical dependencies is equivalent to reporting vulnerabilities; hence the need to classify and manage the information properly and ensure that the positions it takes are rapidly adapted to the changing strategic environment.
- 4.4 The Roadmap also envisages the establishment of an expert group with the Member States in the framework of the OCT, in order to exchange information in a classified environment. The EESC strongly advocates also establishing a strong and permanent link with the European defence, security and aerospace industries, which have the best knowledge of supply chains and critical dependencies. Appropriate mechanisms must be found to allow for a trustful exchange of confidential information with industry.
- 4.5 The EESC believes that the uptake of OCT results into roadmaps and their translation into flagships is also crucial. Transitions between the different phases of the technological and industrial cycle can only be managed successfully if the ownership and responsibilities are clear at each stage. Coherence and synergies are therefore needed not only horizontally, between civil and defence RTD&I, but also vertically, between RTD&I and deployment programmes.
- 4.6 To strengthen cybersecurity and cyber defence, the Commission will propose regulatory action on cyber resilience and ask European standardisation organisations to develop harmonised cybersecurity and privacy standards. Together with the Member States, it will also strengthen preparedness for large-scale cyber incidents. The EESC firmly believes that cyber capabilities should be developed not only in a defensive but also in an offensive sense.
- 4.7 The EESC believes that the EU programmes and instruments in support of RTD&I, outlined in Box 2 (on pages 7 and 9) of the Roadmap, are complex and poorly coordinated; therefore, simplification and streamlining are needed for the benefit of the recipients themselves. An online one-stop shop for SMEs and start-ups is proposed. Starting in a pilot phase with defence and security SMEs, this online "EU SMEs' corner" would enable predefined data to be entered and get an initial assessment of the best-suited programme(s) that can provide public support at EU level.

- 4.8 The Roadmap rightly points out that the EU has policy tools beyond its RTD&I programmes and instruments that can contribute to reducing strategic dependencies in the security and defence sectors. The EESC believes that these tools are important for bridging the gap between development and industrialisation, i.e. the market-uptake of RTD&I results.
- 4.9 A major problem is also ensuring that EU Member States buy from European suppliers once the critical technology has been developed and partially financed by EU public support. In the case of a lack of a consistent purchasing policy both at EU and Member States levels, the EESC expresses concern that the European markets, due to their fragmentation and overall small size on a global scale, risk neither being able to reach the needed economy of scale to reduce the costs nor being able to generate sufficient activity to ensure the existence of nascent start-ups. Overall, the combined European market is potentially very large, but spending is uncoordinated⁸.

Brussels, 14 July 2022

Christa Schweng
The president of the Economic and Social Committee

⁸ The US spends USD 750 billion a year on defence; China spends between USD 200 and USD 300 billion (sources differ widely), while NATO (limited to European countries, without the UK and Turkey, but with Norway) spends USD 250.7 billion.