Council of the European Union

Brussels, 20 February 2026
(OR. en)

6568/26

Interinstitutional File:
2025/0555 (COD)

LIMITE

COMPET 223	ECOFIN 230
IND 132	COH 33
MI 163	INDEF 60
CADREFIN 73	CULT 23
FIN 289	CYBER 75
RECH 75	JAI 225
ESPACE 30	DIGIT 47
CONSOM 53	DATAPROTECT 58
DUAL USE 15	FREMP 64
EDUC 52	RELEX 246
TELECOM 82	COPS 104
ENER 83	UD 38
ENV 149	AUDIO 29
CLIMA 77	PROCIV 30
AGRI 132	IPCR 18
TRANS 91	MAP 58
SAN 99	FISC 81
PHARM 21	CODEC 289
BIOTECH 13	IA 36
POLMIL 89	CSC 131
POLGEN 40	

NOTE

From:	Presidency
To:	Delegations
No. prev. doc.:	15348/1/25 REV 1
Subject:	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on establishing the European Competitiveness Fund ('ECF'), including the specific programme for defence research and innovation activities, repealing Regulations (EU) 2021/522, (EU) 2021/694, (EU) 2021/697, (EU) 2021/783, and amending Regulations (EU) 2021/696, (EU) 2023/588, (EU) [EDIP] *- Revised Presidency text on Chapter VI (Digital leadership)*

Delegations will find below a revised Presidency text on Chapter VI (Digital leadership) with a view to the meeting of the Ad hoc Working Party on the Multiannual Financial Framework (European Competitiveness Fund) on 2 March 2026.

Changes in comparison to the previous Presidency text (document 15348/1/25 REV 1) are marked in **bold** for additions and in ~~strikethrough~~ for deletions.

The numbering of the Commission proposal remains unchanged until the end of the negotiations.

General scrutiny reservation: All delegations.

PUBLIC

2025/0555 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on establishing the European Competitiveness Fund ('ECF'), including the specific programme for defence research and innovation activities, repealing Regulations (EU) 2021/522, (EU) 2021/694, (EU) 2021/697, (EU) 2021/783, and amending Regulations (EU) 2021/696, (EU) 2023/588, (EU) [EDIP]

PUBLIC

(26) The Union can become a global leader in digital technologies. The ECF should promote the development and deployment of digital solutions and infrastructures and capacities across the Union**, and the development of advanced digital skills, which include cybersecurity skills,** for the benefit of the European society and economy.

(27) Chronic underinvestment in the European tech sector is one of the main reasons for the lack of competitiveness of the Union, as compared to our global competitors. Moreover, European sovereignty in digital technologies and infrastructures has become key for our resilience, security and for democracy, as highlighted in the 2025 State of the Digital decade report which also underlined the remaining significant gaps to reach Union's 2030 goals, notably for the development of Artificial Intelligence (AI) ~~and space technologies~~**,** semiconductors, 5G and **advanced** digital skills**, which include cybersecurity skills**.

(28) While Europe's digital transformation is accelerating, the many critical dependencies on non-Union suppliers (from raw materials, advanced semiconductors, and AI chips to systems, infrastructures and services) require European alternatives that anchor the digital transformation in Europe's economy, with our shared values as the essential differentiator, including by leveraging the power of open-source technologies.

(28a) Support for digital leadership is driven by regulatory and non-regulatory Union policy initiatives in the digital area such as the AI Act, **the** AI Continent ~~and AI~~ Action Plan, the Apply AI Strategy, **[**the Cloud and AI Development Act **proposal]**, the Data Union Strategy, the **Data Act, [the** Digital Networks Act **proposal], the eIDAS2 and the [European Business Wallets proposal], the**~~, the EU~~ Quantum **Europe** Strategy and **[**the Quantum Act **proposal], the Cyber Solidarity Act, the Cyber Resilience**~~, the Cyber-Solidarity Act, the Cyber-Resilience~~ Act and **[**the Cybersecurity Act **2 proposal], the International Digital Strategy for the**~~, the White Paper for~~ European ~~Defence Readiness 2030,~~**Union, the** NIS2 Directive, ~~and the revision of the EU~~**[the** Chips Act **2 proposal]**, **the EU Action Plan on Cable Security** and by future policy initiatives. Support for Digital Leadership should be implemented in coherence with the achievement of the targets and objectives of the Digital Decade Policy Programme 2030 established by Decision (EU) 2022/2481.

(28b) The key digital areas to invest in include artificial intelligence, high performance computing, quantum technologies, semiconductors, robotics, data**, interoperability**, connectivity, cybersecurity, digital identity and trust services, new and emerging digital technologies as well as cross-sectoral digital technologies and applications, including those with dual-use potential. ~~This includes~~**Detailed examples include, among others,** AI Factories and Gigafactories, AI-powered digital twins, industry specific AI models, augmented reality ~~and~~**,** virtual worlds **and media-relevant technologies**, sustainable AI, quantum chips pilot lines, quantum computing and simulation, photonics, wide bandgap, chip design, ~~advanced materials,~~ supply chain analytics, process technologies, **digital** manufacturing**, microelectronics**, additive manufacturing**, digital infrastructure**, automation, large data technologies, data spaces, data ~~centers~~**centres**, telco-edge and cloud technologies, distributed ledger technology, internet-of-things, communication networks, communication and sensing infrastructures, guidance and navigation technologies, ~~advanced underwater observation infrastructure,~~ digital connectivity networks, advanced connectivity infrastructures, (transnational) digital networks, 5G, 6G and other wireless technologies, submarine cables~~,~~ (including repair capacities)~~, non-terrestrial networks~~, sensing technologies, radio spectrum monitoring infrastructure and technologies or spectrum efficiency measures, network resilience, software engineering, EU Digital Identity Wallets, European Business Wallets, interoperable digital technologies, testing and experimentation facilities, ~~(~~**advanced cybersecurity solutions,** national and regional Cyber Hubs~~)~~, the EU for Business Network, European Digital Innovation Hubs~~, defence or space capacities, space technologies~~, advanced digital skills, upskilling and reskilling, specialised skills programmes, industry-led deployment networks for AI and other strategic technologies, backbone, backhaul and access networks, post-quantum cryptography and quantum key distribution pilots.

(28c) Fostering key digital areas across private and public sectors makes our entire economy more competitive, secure, sovereign, and sustainable, fortifying societal resilience and preparedness. Moreover, interoperable digital technologies are driving the modernisation of the public sector, serving for the integration of the single market, which is our most valuable stepping stone for European digital startups to become globally competitive.

PUBLIC

(28d) Support for Digital Leadership shall be implemented in particular through the following activities: developing and shaping sustainable core digital technologies; building attractive**, competitive** and resilient digital ecosystems and strengthening the security of supply; building, developing, modernising, completing and deploying state-of-the-art and sustainable digital applications, infrastructures and services, including trans-European digital networks; supporting the digital transformation and interoperability of public and private sectors; supporting the development, implementation, monitoring and enforcement of relevant Union legislation and policy; **strengthening the EU cybersecurity ecosystem** and enhancing the high level of cybersecurity in the Union. **Considering that funding is essential for the long term development and autonomy for the cybersecurity sector, coordination of cybersecurity investments between the Union and the Member States should, as far as possible, be ensured at European level, including through the possible successor of the European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC) and the Network of National Coordination Centres (NCCs), within the parameters of the funding Regulation (EU) 2021/887, or through any other initiative that may be established for this purpose.**

(29) Technological progress and innovation in every economic sector, and thus their productivity and competitiveness are essentially driven by the integration of sector-specific digital developments and use of digital solutions that should be supported across the Fund in the context of the activities developed in the different policy windows of the ECF.

(29a) Enhancing the high-level of cybersecurity in the Union is fundamental to ensure its resilience and competitiveness. The ECF should therefore both promote cybersecurity-by-design by incorporating cybersecurity measures in all relevant activities as well as support the competitiveness of the Union cybersecurity ecosystem, notably SMEs, startups and scaleups.

PUBLIC

(29b) Dependency on third countries high-risk suppliers in critical sectors can pose a strategic risk of foreign interference and jeopardise the Union's security, resilience and sovereignty. The NIS Cooperation Group, in cooperation with the Commission and the European Union Agency for Cybersecurity (ENISA), plays a key role in carrying out EU Coordinated security risk assessments of critical supply chains, taking into account technical and, where relevant, non-technical risk factors in accordance with Article 22 of Directive (EU) 2022/2555.[1]

(30) Europe must protect its security interest against suppliers which could represent a persistent security risk due to the potential interference from third countries as well as their security, notably cybersecurity. It is therefore necessary to reduce the risk of persisting dependency on high-risk suppliers in the internal market, including in the ICT supply chain, as they could have potentially serious negative impacts on security for users and companies across the Union and the Union's critical infrastructure in terms of the **confidentiality, the** integrity**, and the availability** of data ~~and services~~**,** as well as the availability of ~~service~~**services** . This restriction should be based on a proportionate risk assessment and associated mitigation measures as defined in the Union policies and laws.

(31) A successful deployment of interoperability across borders and sectors has a substantial, untapped potential, especially for the competitiveness of European businesses. Therefore, it is imperative to invest in the development of pan-European digital public infrastructures encompassing interoperable, secure and sovereign digital networks, solutions and services to address the fragmented interoperability landscape across the Union, notably to transform the Member States' public sector into an interconnected, frictionless, and agile digital ecosystem. The implementation of interoperability by European public administrations at all levels is a precondition for a resilient and innovation-driven public sector which contributes to the Union's goals of competitiveness, technological sovereignty and security.

---

[1] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148; Text with EEA relevance, ELI: http://data.europa.eu/eli/dir/2022/2555/2022-12-27.

Chapter I

General Provisions

SECTION 1

OBJECTIVES AND STRUCTURE OF THE FUND

Article 3

Objectives

2. Under the general objectives set out in paragraph 1, the ECF shall in particular pursue the following specific objectives:

(c) For support to Digital Leadership, the specific objectives of fostering innovation, competitiveness and sovereignty of the digital sector for a competitive and secure Union, bringing its benefits to citizens and society, public administrations and businesses across the Union. This shall include, but not be limited to, supporting the entire scope of the digital sector and value chains in a comprehensive and strategic manner including support to startups, scaleups and SMEs, with a focus on key digital areas such as artificial intelligence, high performance computing, quantum technologies, semiconductors, robotics, data, **cloud,** connectivity, cybersecurity, digital identity and trust services, new and emerging digital technologies as well as cross-sectoral digital technologies and applications, including those with dual-use potential, in particular by:

(i) developing and shaping sustainable core digital technologies~~;~~

(ii) building attractive**, competitive** and resilient digital ecosystems and strengthening the security of supply;

PUBLIC

(iii) building, developing, modernising, completing and deploying state-of-the-art and sustainable digital applications, infrastructures and services, including trans-European digital networks;

(iv) supporting the digital transformation and interoperability of public and private sectors;

(v) supporting the development of advanced digital skills including cybersecurity skills;

(vi) supporting the development, implementation, monitoring and enforcement of relevant Union legislation and policy;

(vii) ~~and~~ enhancing the high level of cybersecurity in the Union~~.~~**;**

(viii) and supporting cultural and creative industries.

PUBLIC

CHAPTER VI
SUPPORT FOR DIGITAL LEADERSHIP

PUBLIC

Article 38

Specific provisions for support to digital leadership policy

1. Actions supported under this chapter shall contribute to the general objectives set out in Article 3(1) and the specific objectives set out in Article 3(2), point (c).

2. Support for actions under this chapter shall be financed from the budget set out in Article 4(2), point (d), and any additional contributions assigned in accordance with Article 5.

Article 39

Specific activities to support digital leadership policy

1. *deleted*

2. Support for Digital Leadership shall be implemented in particular through the following activities:

(a) Developing and shaping sustainable core digital technologies**, products and services** that reflect Union values, including by research and innovation, applied research, technology transfer, industrial deployment, and market uptake.

(b) Building attractive**, competitive** and resilient digital ecosystems including for disruptive innovative companies, SMEs, startups and scaleups, as well as emerging industry leaders in the digital sector to remain, grow and thrive within the Union, supporting them in scaling up, expanding their markets, including through procurement and standardisation, as well as strengthening the security of supply of advanced digital technologies and services by supporting needed capacities, including production capacity, and advanced digital skills.

(c) Deploying state-of-the-art**, secure** and sustainable digital applications, infrastructures and services across the Union**, with cybersecurity-by-design and cybersecurity-by-default principles embedded throughout their lifecycle,** including through actions to research and innovate, develop, produce, manufacture, build, modernise, complete or deploy advanced **European** digital infrastructures, trans-European digital networks and secure and interoperable digital public infrastructure at scale and across borders that act as key enablers of the digital transformation that support societal resilience and preparedness, bringing clear added-value to businesses, public services and citizens. Where relevant, these actions shall be coordinated with national investments and exploit untapped potential to create a domestic market for advanced digital technologies in accordance with Article 10.

(d) Supporting the Union's digital transformation of public and private sectors, including ~~to~~**cross-border interoperability and integration of services and the** support **for** the development and the circulation of **advanced** digital **skills which include cybersecurity** skills, providing the necessary support to accelerating and deepening the uptake and deployment of digital solutions across the private sector with a focus on complex technologies, and to digitalisation of the public sector including ensuring cohesive Union-wide interoperable digital public services maximising efficiency for businesses and citizens.

(e) Support actions for the development, implementation, monitoring and enforcement of relevant Union legislation and policy. This includes supporting the relevant institutions, the **coordination and** cooperation between national authorities and with stakeholders, studies, the development and deployment of tools and infrastructures, including IT infrastructure and tools.

PUBLIC

3. Activities under this Chapter shall support the development, innovation, deployment**,** and procurement of advanced cybersecurity capacities, infrastructures, products, **services,** technologies and capabilities, with a view to **strengthen the European cyber ecosystem and to** ensure the **resilience and** security of critical infrastructures ~~&~~, digital supply chains, **as well as to** further strengthen Union situational awareness of the threat landscape ~~as well as~~**and to** improve detection capacities and incident response capabilities~~;~~ ~~supporting~~**. These activities shall also support** the competitiveness of the Union cybersecurity industrial base, cybersecurity skills development ~~together with~~**and improve** the cyber maturity of the European industrial basis, including SMEs.

4. Work programmes adopted in accordance with the rules of this Regulation under this chapter shall integrate in a specific dedicated part and ensure coherence with Competitiveness and Society activities under the Regulation (EU) [XXX] [Horizon Europe Framework programme for Research and Innovation.

PUBLIC