STUDY

Requested by the EUDS Special Committee

European Parliament

Strengthening Resilience

Towards the European Democracy Shield

Policy Department for Justice, Civil Liberties and Institutional Affairs
Directorate-General for Citizens' Rights, Justice and Institutional Affairs
PE 777.917 – October 2025

EN

Strengthening Resilience

Towards the European Democracy Shield

Abstract

This study reviews the current framework to protect democracy in the EU in view of the forthcoming European Democracy Shield. It provides a comprehensive map of the existing instruments, while identifying and assessing outstanding policy challenges, regulatory gaps and implementation issues. The study also formulates recommendations to strengthen democratic resilience.

The study was commissioned by the European Parliament's Policy Department for Justice, Civil Liberties and Institutional Affairs at the request of the EUDS Special Committee.

This document was requested by the European Parliament's Special Committee on the European Democracy Shield.

AUTHORS

Edoardo BRESSANELLI, Associate Professor, Sant'Anna School of Advanced Studies, Pisa (Italy) and Senior Visiting Research Fellow, King's College London (UK).
Samuele BERNARDI, Researcher, Sant'Anna School of Advanced Studies, Pisa (Italy).

ADMINISTRATOR RESPONSIBLE

Alessandro DAVOLI

EDITORIAL ASSISTANT

Christina MARGELI

LINGUISTIC VERSIONS

Original: EN

ABOUT THE EDITOR

Policy departments provide in-house and external expertise to support EP committees and other parliamentary bodies in shaping legislation and exercising democratic scrutiny over EU internal policies.

To contact the Policy Department or to subscribe for updates please write to:
Policy Department for Justice, Civil Liberties and Institutional Affairs
European Parliament
B-1047 Brussels
Email: poldep-iust-b@europarl.europa.eu

Manuscript completed in October 2025

This document is available on the internet at:
http://www.europarl.europa.eu/supporting-analyses

DISCLAIMER AND COPYRIGHT

CONTENTS

LIST OF ABBREVIATIONS

AVMSD	Audio Visual Media Service Directive
CER	Critical Entities Resilience
CERV	Citizens, Equality, Rights and Values
CFSP	Common Foreign and Security Policy
CRF	Collective Response Framework
CSDP	Common Security and Defence Policy
DDoS	Distributed Denial-of-Service
DEP	Digital Europe Programme
DoD	Defence of Democracy
DSA	Digital Services Act
EBDS	European Board for Digital Services
ECNE	European Cooperation Network on Elections
EDAP	European Democracy Action Plan
EDMO	European Digital Media Observatory
EDS	European Democracy Shield
EEAS	European External Action Service
EMFA	European Media Freedom Act
ENISA	European Union Agency for Cybersecurity
EU-CyCLONe	European Cyber Crisis Liaison Organisation Network
EUMSS	EU Maritime Security Strategy

EUIBAs	European Union Institutions, Bodies and Agencies
FDI	Foreign Direct Investment
FIMI	Foreign Information Manipulation and Interference
GDPR	General Data Protection Regulation
GNSS	Global Navigation Satellite System
IPCR	Integrated Political Crisis Response
MFF	Multiannual Financial Framework
MoU	Memorandum of Understanding
NaD	Network against Disinformation
NIS	Network and Information Systems
PACE	Parliamentary Assembly of the Council of Europe
RAS	Rapid Alert System
RRM	Rapid Response Mechanism
SDP	Security and Defence Partnership
SLAPPs	Strategic Lawsuits Against Public Participation
TTC	Trade and Technology Council
UPCM	Union Civil Protection Mechanism
VLOPs	Very Large Online Platforms
VLOSEs	Very Large Online Search Engines

LIST OF BOXES

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

This study examines the European Union's evolving framework to safeguard democracy in the face of mounting internal and external threats, with a particular focus on the forthcoming European Democracy Shield (EDS). It maps existing instruments, identifies regulatory and implementation gaps, and formulates recommendations to strengthen democratic resilience. The analysis draws on a comprehensive review of EU legislation, policy documents, and recent empirical evidence, complemented by expert consultations and secondary sources.

Key findings

Democracy in the EU is under sustained pressure from hybrid threats, notably foreign information manipulation and interference (FIMI), disinformation, and cyberattacks. These challenges have intensified in recent years, as illustrated by the 2024 European Parliament (EP) elections and multiple national contests, which were targeted by coordinated influence operations. Although large-scale disruptions were avoided, the persistence of malign activities underscores the vulnerability of democratic systems, particularly in the digital sphere. Generative AI has amplified these risks, enabling the rapid creation of deceptive content, while societal polarisation and declining trust in institutions exacerbate the problem.

The EU has progressively shifted from an agenda centred on democratic reform to one prioritising democratic protection. Over the last decade, notably through comprehensive packages such as the European Democracy Action Plan (2020) and the Defence of Democracy package (2023), it has developed a broad toolbox combining legislative and non-legislative instruments. Among the former, key milestones include the Digital Services Act (DSA), which imposes obligations on very large online platforms and search engines to mitigate systemic risks; the European Media Freedom Act (EMFA), introducing provisions to protect media freedom and independence, and the Regulation on the Transparency and Targeting of Political Advertising, which enhances transparency and accountability in the information space.

Despite these advances, significant gaps remain. Enforcement of existing legislation is uneven. There are delays implementing some of the provisions of the DSA and with the transposition of the Network and Information Security 2 (NIS2) and the Critical Entities Resilience (CER) Directives. Compliance by major digital platforms with the DSA and its Code of Conduct – formerly known as Code of Practice on Disinformation – remains partial and inconsistent. Similarly, the EMFA faces challenges in ensuring editorial independence at national level.

Beyond the digital domain, the EU has strengthened measures to protect electoral integrity, promote media pluralism and digital literacy, and foster citizen engagement and civil society. However, youth participation remains low, and younger cohorts are particularly exposed to disinformation through social media. At the same time, the EU's external action has expanded, notably with restrictive measures targeting actors engaged in hybrid operations and the inclusion of FIMI-related commitments in Security and Defence Partnerships. Yet, geopolitical volatility complicates collective responses.

Finally, the EU's governance architecture for democratic protection has become increasingly complex, involving multiple institutions and overlapping mandates. While this reflects the cross-cutting nature of the challenge, it also risks duplication and inefficiencies. The forthcoming EDS offers an opportunity to consolidate efforts, clarify responsibilities, and ensure adequate resources for implementation.

Recommendations

The EDS should adopt a dual approach, addressing both external hybrid threats and internal democratic vulnerabilities. It should consolidate the EU's fragmented toolbox into a coherent strategy, underpinned by clear governance arrangements and robust enforcement mechanisms. A five-year Hybrid Strategy, aligned with the revised Strategic Compass, should set priorities across the full spectrum of hybrid threats, including FIMI, disinformation, and cyber risks, and be accompanied by an actionable roadmap with dedicated funding.

Strengthening enforcement is paramount. The Commission should accelerate infringement proceedings against Member States that fail to implement EU regulations, while providing technical and financial support to facilitate compliance. At the same time, the EU should enhance its capacity to monitor and sanction non-compliant platforms, ensuring that obligations under the DSA and related instruments are effectively applied.

To counter FIMI, the EU should refine its detection methodologies and operationalise a dedicated FIMI Protocol, complementing the existing toolbox. The creation of an EU FIMI Reserve, modelled on the Cybersecurity Reserve, would bolster preparedness and response capabilities. External Action could be reinforced through the deployment of specialised attachés in EU Delegations and deeper engagement in multilateral frameworks.

Societal resilience must become a central pillar of the EDS. A pan-European e-initiative on media and digital literacy, targeting specifically young people, should be launched as a joint initiative of EU institutions and Member States, supported by the next Multiannual Financial Framework. This should be complemented by sustained investment in independent media and civil society, as well as measures to protect journalists from strategic lawsuits and surveillance.

Finally, the EU should treat electoral infrastructure as critical, explicitly including it under the CER and NIS2 frameworks. This would ensure a high level of protection against cyber and hybrid threats, particularly during electoral periods. At the same time, deliberative democracy initiatives should be evaluated to ensure they deliver meaningful participation rather than symbolic engagement.

The EDS represents a critical opportunity to move from a reactive to a proactive posture in defending democracy. By integrating legislative, operational, and societal measures within a coherent framework, the EU can strengthen its resilience and uphold the integrity of its democratic systems in an increasingly contested information environment.

1. ATTACKING DEMOCRACY

1.1. Introduction

In her first State of the Union address to the European Parliament (EP), Ursula von der Leyen warned: "Our democracy is under attack. The rise in information manipulation and disinformation is dividing our societies. It is not only eroding trust in the truth – but also in democracy itself".[1] Against a turbulent and unpredictable international backdrop, with no end in sight to the conflict in Ukraine and the catastrophic situation in Gaza, the President of the Commission called for a "European Democracy Shield". This warning was hardly surprising. Ahead of her second term, von der Leyen's political guidelines placed strong emphasis on democracy: "Europe's future in a fractured world will depend on having a strong democracy [..] Our democratic systems are under attack. We have seen a rise in the number of threats from internal and foreign actors".[2] Building on policy initiatives already introduced – such as the Defence of Democracy (DoD) package announced just before the 2024 EP elections – the EU's democracy agenda remains highly salient.

More broadly, it has become almost a truism that these are very challenging times for democracies, both within the EU and globally. Scholars and commentators speak of "democratic decline" and use the term "democratic backsliding" to describe the deterioration or erosion of democratic norms. The rise of a new type of political regime – "illiberal democracies" – was noted long ago and has since consolidated.[3] Global assessments of democratic health reach similar conclusions: the Economist Intelligence Unit's 2024 report highlights a "continuing democratic malaise";[4] the Freedom House 2025 report records the 19th consecutive year of decline of global freedom, often driven by elected leaders undermining democratic institutions;[5] and the V-Dem 2025 report warns of a "truly global wave of autocratisation", which is "also manifest within the European Union".[6]

---

1 European Commission, "2025 State of the Union Address by President von der Leyen", *Speech*, Strasbourg, 10 September 2025. https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_25_2053

2 von der Leyen, U., *Europe's Choice. Political Guidelines for the next European Commission. 2024*-2029, Strasbourg, 18 July 2024, p. 23.

3 For instance, see Plattner, M. F., "Is Democracy in decline?", *Journal of Democracy*, Vol. 26, No. 1 (2015), pp. 5-10; Waldner, D. and Lust, E., "Unwelcome Change: Coming to Terms with Democratic Backsliding", *Annual Review of Political Science*, Vol. 21 (2018), pp. 93-113; Zakaria, F., "The Rise of Illiberal Democracy", *Foreign Affairs*, Vol. 76, No. 6 (1997), pp. 22-43.

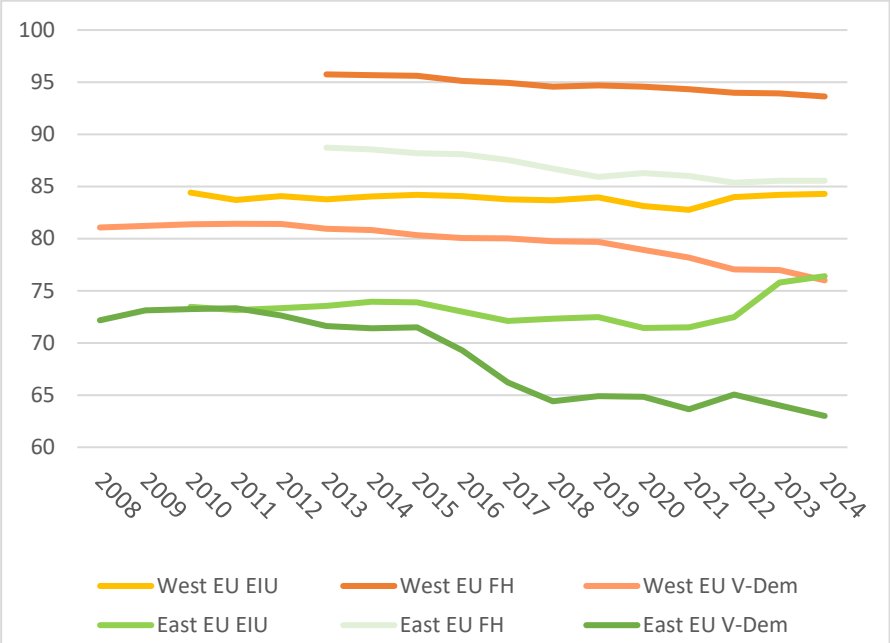
4 Economist Intelligence Unit (EIU), *Democracy Index 2024. What's wrong with representative democracy?*, 2025.

5 Freedom House, *Freedom in the World 2025. The Uphill Battle to Safeguard Rights*, February 2025, pp. 2 and 13-17.

6 Varieties of Democracy (V-Dem), Democracy Report 2025. 25 Years of Autocratization – Democracy Trumped?, University of Gothenburg, V-Dem Institute, March 2025, pp. 9 and 20. This report does not cover rule of law-related issues in the EU. On this, cfr. European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. 2025 Rule of Law Report. The rule of law situation in the European Union*, COM(2025) 900 final, Strasbourg, 8 July 2025. Another important aspect concerns the diffusion of theories against democracy, which are often endorsed by illiberal forces. The European Parliament has launched an own-initiative procedure on EU strategy to face the new theories against democracy - 2025/2050 (INI).

Misinformation and disinformation pose a particularly severe challenge. The World Economic Forum's Global Risks Report ranks them as the top short-term risk,[7] while International IDEA reports the sharpest decline in press freedom in 50 years.[8]

Figure 1: Democracy Scores in the European Union



Source: EIU – Economist Intelligence Unit; FH -Freedom House; V-Dem – Varieties of Democracy

Yet, a counter-narrative is also emerging. In the face of adversities, democracies have demonstrated "resilience". [9] However, this resilience – and, ultimately, their survival – is not a *fait accompli*. As the European Commission stressed in its European Democracy Action Plan (EDAP), democracy "has to be actively nurtured and defended".[10] Political systems cannot merely absorb external shocks; they must anticipate crises and prepare for them. The Commission's latest Foresight Report calls this proactive, transformative approach "resilience 2.0".[11] When democracies are severely tested, they could (and should) "fight back".

Over the past decade, the EU has developed a broad set of legislative and non-legislative instruments to protect its democratic processes from external hybrid threats and strengthen them within its

7 World Economic Forum, *The Global Risks Report 2025. 20th edition*, Cologny/Geneva, January 2025, p. 8.

8 International IDEA, *The Global State of Democracy Report 2025. Democracy on the Move,* September 2025, p. 17.

9 See Youngs, R. et al., "A New Dynamic of Democratic Resilience?", Carnegie Europe, European Democracy Hub, 29 April 2025. https://europeandemocracyhub.epd.eu/a-new-dynamic-of-democratic-resilience/. See also Brownlee, J. and Miao, K., "Why democracies survive", *Journal of Democracy,* Vol. 33, No. 4 (2022), pp. 133-149.

10 European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the European Democracy Action Plan*, COM(2020) 790 final, Brussels, 3 December 2020, p. 1.

11 European Commission, *Foresight Report 2025. Resilience 2.0: Empowering the EU to thrive amid turbulence and uncertainty*, COM(2025) 484 final, Strasbourg, 9 September 2025, p. 5. On the institutional responses to the polycrisis, see also Bressanelli, E. and Natali, D., "Tested by the polycrisis? Reforming or Transforming the EU?", *Politics and Governance*, Vol. 11, No. 4 (2023), pp. 246-251.

borders.[12] This study begins by presenting recent empirical evidence that democracy in the EU is "under attack" (Chapter 1). It then maps the policies and tools already in place (Chapter 2), identifies gaps and implementation challenges (Chapter 3), and concludes with specific policy recommendations (Chapter 4).

Box 1: The youth: attitudes on democracy and disinformation

Within democratic systems, certain socio-demographic groups are particularly vulnerable. A recent survey shows that one in five Europeans aged 16-26 would accept authoritarian rule under certain circumstances, while an additional 10 percent are indifferent to whether government is democratic. Youth participation in elections is also significantly lower than that of older cohorts. In the 2024 EP elections, overall turnout was 50.7%, but only 36% of those aged 15-24 and 46% of those aged 25-39 voted.

Young people also rely on different sources of political and social information. According to the 2025 *Eurobarometer Youth Survey*, social media platforms are the most widely used source across the Union – surpassing all others in all but four Member States. This trend is strengthening. Respondents aged 16-18 are more likely than those aged 25-30 to obtain socio-political information from social media. Consequently, disinformation—particularly on these platforms—poses a critical challenge. In all Member States, a large majority of respondents reported exposure to disinformation or fake news in the week preceding the survey. Although young people express confidence in their ability to identify 'fake news', evidence suggests that this confidence is often misplaced. Exposure to disinformation has tangible negative effects, including reduced civic engagement and erosion of trust. Policies to counter disinformation must therefore pay particular attention to the youngest age groups.

Sources: Tui Stiftung and YouGov Institute, Jugendstudie 2025, Berlin, 3 July 2025; European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Report on the 2024 Elections to the European Parliament, COM(2025) 287 final, Brussels, 6 June 2025, pp. 6-7; European Parliament, Eurobarometer Youth Survey, Brussels, January 2025, pp. 26-29 and 38; Kops, M., Schittenhelm, C. and Wachs, S., "Young people and false information: A scoping review of responses, influential factors, consequences, and prevention programs", Computers in Human Behavior, Vol. 169 (2025); Marta, E., Damia-Martinez, S. and Riva, G. (eds), Alfabetizzazione digitale e fake news, Istituto Toniolo, Osservatorio giovani, 2025; Our Rule of Law, Our Democracy Report, September 2025.

1.2. Recent evidence

1.2.1. The 2024 European Parliament elections

The European Commission's assessment of the 2024 European Parliament elections was broadly positive. It reported that "the elections run smoothly overall, without any major incidents", despite challenges such as increased EU-related disinformation and several cases of Foreign Information

[12] In its Conclusions, the European Council enumerates the following hybrid threats: "intimidation, sabotage, subversion, foreign information manipulation and interference, disinformation, malicious cyber activities and the instrumentalisation of migrants by third countries". European Council, *Conclusions*, EUCO 15/24, Brussels, 27 June 2024, p. 10

Manipulation and Interference (FIMI).[13] More specifically, the Commission noted that "no large-scale disinformation incident or campaign was detected during election days", although some significant Kremlin-linked operations, such as the Doppelganger campaigns, were identified.[14] Highly-manipulative 'deepfakes' were "not prominent", while Artificial Intelligence (AI) was mainly used to create 'shallowfakes' and 'cheapfakes'. Regarding cybersecurity, only minor incidents were recorded, primarily Distributed Denial-of-Service (DDoS) attacks by pro-Russian hacktivist groups".[15]

In its regular report, the EEAS detected and analysed FIMI incidents between November 2023 and November 2024,[16] confirming that democratic institutions and processes were major targets. For the EU Elections alone, the EEAS detected 42 cases of FIMI activity, which intensified as polling day approached. Pro-Kremlin outlets sought to weaken support for Ukraine, discredit European leaders, and encourage voter abstention.[17] In a more recent assessment, the EEAS noted an intensification of Russian hybrid activities in the last 12 or 18 months, with its actions becoming "more aggressive, more violent and more reckless".[18]

The European Digital Media Observatory (EDMO) and its dedicated Task Force closely monitored the information environment during the election campaign. Their final report shows that disinformation about the EU rose significantly in the run-up to the elections, peaking at about 15% of all disinformation cases in the final month.[19] Recurring narratives focused on the escalation of the war in Ukraine, climate change, election manipulation, and fears of migrants seizing power.

---

13 European Commission, *Report on the 2024 Elections to the European Parliament*, *cit.*, p. 3. See also European Commission, *Staff Working Document Accompanying the document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Report on the 2024 Elections to the European Parliament,* SWD(2025) 147 final, Brussels, 6 June 2025 and European Commission, *Memo: Known information interference operations during the June 2024 elections for the European Parliament*, October 2024.

14 EUvsDisinfo*, Doppelganger Strikes Back: Unveiling FIMI Activities Targeting European Parliament Elections*, 19 June 2024. https://euvsdisinfo.eu/doppelganger-strikes-back-unveiling-fimi-activities-targeting-european-parliament-elections/

15 DDoS attacks target systems and data availability and occur when users of a system cannot access relevant data, services or other resources. This is the most frequent type of cyber incident in the period July 2023 to July 2024 also based on data collected by the European Union Agency for Cybersecurity (ENISA). See ENISA, *2024 Report on the State of Cybersecurity in the Union*. *Condensed version*, Athens, December 2024, p. 7.

16 European External Action Service, *3rd EEAS Report on Foreign Information Manipulation and Interference Threats. Exposing the Architecture of FIMI Operations*, Strategic Communication and Foresight (SG.STRAT), Brussels, March 2025.

17 *Ibid.*, pp. 10-11. See also EUvsDisinfo, "*Elections are battlefields for the Kremlin*", 24 June 2024. https://euvsdisinfo.eu/elections-are-battlefields-for-the-kremlin/

18 Barbara Gallo, Head of Division Hybrid Threats and Cyber, EEAS**.** Committee on Security and Defence (SEDE). Committee meeting. *Russia's hybrid warfare against the European Union*. Brussels, 25 September 2025 https://www.europarl.europa.eu/doceo/document/SEDE-OJ-2025-09-24-1_EN.html

19 European Digital Media Observatory (EDMO), *Final Report – Outputs and outcomes of a community-wide effort,* 2025, p. 13. In its 'Final Remarks', the report acknowledges that "the European elections concluded properly and peacefully", but it warns that "winning an important battle against disinformation, only to lose the attrition war would be unforgivably short-sighted" (pp. 27-28).

Academic research corroborated these findings. Analysing 278 hoaxes collected by fact checkers between 1 May and 30 June 2024, Casero-Ripollés *et al*. found that disinformation primarily affected Southern and Eastern Europe and increased sharply in the days before the vote.[20] Topics varied widely across Member States, with electoral integrity and migration being the most frequent, though no single theme dominated. National contexts largely determined the main narratives.[21]

1.2.2. Elections in the EU Member States and Candidate Countries

There is substantial evidence of mis- and disinformation affecting multiple elections across Europe during 2024-25. A comprehensive mapping of the "super-election year" found that hybrid operations – conducted by actors from China, Iran, and Russia – targeted elections in EU countries as well as Georgia, Moldova, Taiwan and the USA. The study identified mis- and disinformation in 43 national elections and noted that, consistent with findings from the EP elections, AI was primarily used "for satirical purposes rather than explicit manipulation, proving less disruptive to elections than feared".[22]

The Alliance for Securing Democracy's *Authoritarian Interference Tracker* documented 40 incidents since 2024 (28 linked to Russia), involving tactics such as information manipulation, cyber operations, malign finance, civil society subversion, economic coercion, and kinetic actions. Most incidents targeted EU Member States – particularly Germany, Belgium, and France – and focused on information manipulation and cyberattacks.[23]

A prominent case occurred during Romania's presidential elections. On 6 December 2024, the Constitutional Court annulled the first-round vote and cancelled the second round, originally scheduled for 8 December, thus triggering the repetition of the entire electoral process. The decision was based on intelligence reports revealing attempts to manipulate the election through cyberattacks, undeclared funding, and the activation of thousands of TikTok accounts two weeks before the vote. The European Commission subsequently launched formal proceedings against TikTok for allegedly breaching the Digital Services Act (DSA).

Disinformation and FIMI campaigns have also been documented in candidate countries. In Moldova, ahead of the parliamentary elections on 28 September 2025, investigative journalists and fact-checkers identified several videos – some using AI-generated deepfakes – also disseminated by the Russian-backed Matryoshka network.[24] In 2024, before the presidential elections and the constitutional

[20] The data used in the analysis are from the Elections24Check database collected by the European Fact Checking Standards Network (EFCSN) in collaboration with Google News Initiative. As indicated in the official website, "the public facing dataset is no longer available [but] researchers and journalists can still request access" (https://efcsn.com/advancing-fact-checking/ retrieved on 16 September 2025).

[21] Casero-Ripollés, A., Alonso-Muñoz, L., and Moret-Soler, D., "Spreading false content in political campaigns: Disinformation in the 2024 European Parliament elections", *Media and Communication*, Vol. 13 (2025), pp. 1-20.

[22] International IDEA, *Review of the 2024 super-cycle year of elections. Trends, challenges and opportunities*, Stockholm, June 2025, p. 5.

[23] Alliance for Security Democracy (ASD), *Authoritarian Interference Tracker,* German Marshall Fund of the United States. https://securingdemocracy.gmfus.org/toolbox/authoritarian-interference-tracker/?fwp_date_range=2024-01-01%2C2025-06-19 (Last searched 20.06.2025).

[24] Gwyn Jones, M., "Online disinformation intensifies ahead of Moldovan parliamentary elections", *Euronews*, 3 September 2025. https://www.euronews.com/my-europe/2025/09/03/online-disinformation-intensifies-ahead-of-moldovan-

referendum on the EU, pro-Russian actors deployed Telegram chatbots, coordinated social media campaigns, and paid ads on Facebook and Instagram.[25] More broadly, in both the Eastern Neighbourhood and the Western Balkans, external disinformation efforts often interact with domestic actors, amplifying and adapting content to local contexts.[26]

parliamentary-elections; The Insider, "Russian bots from the "Matryoshka" network target EU summit in Moldova with fake videos impersonating The Insider and other media", 24 June 2025. https://theins.ru/en/news/282450.

[25] Olari, V., Calmis, D. and Gigitashvili. G., "Malign interference in Moldova ahead of presidential elections and European referendum", DFRLab, 18 October 2024. https://dfrlab.org/2024/10/18/malign-interference-moldova/; EUvsDisinfo, "Who is afraid of the European Moldova?", 17 October 2024. https://euvsdisinfo.eu/who-is-afraid-of-the-european-moldova/.

[26] Borràs, J., *Disinformation in enlargement countries: Sowing instability, Distorting EU's perception*, CIDOB Briefing, Barcelona, December 2024; Institute for Strategic Dialogue, *Monitoring Influence and Disinformation Campaigns in the Western Balkans* (MEDIWEB), Berlin, 18 December 2024; Kovalčíková, N., De Agostini, L. and Catena, B., *Strengthening Resilience in the East*, Brief 15, European Union Institute for Security Studies, Paris, April 2025.

2. STATE OF THE ART

KEY FINDINGS

- The EU agenda on democracy has shifted from an inward focus on democratic reform to an outward focus on democratic protection.
- The EU toolbox to protect democracy has strongly expanded over the last decade and currently includes a broad set of legislative and non-legislative instruments, spanning across multiple policy areas.
- Following the rise of incidents impacting on physical and digital infrastructure, EU legislation – notably the CER and the NIS2 directives – identifies and lists critical sectors placing additional obligations on Member States and critical entities. Election infrastructure is not explicitly included.
- The EU has invested heavily in its external action and, through the Security and Defence Partnerships and multilateral cooperation, has enhanced coordinated responses to FIMI activities and hybrid threats. However, recent geopolitical developments represent a challenge for cooperation at the international level.
- While significant differences of approach on hybrid threats exist between Member States, dedicated agencies and specific policy responses have been introduced by several of them.

2.1. Reframing the EU agenda: From democratic reform to democratic protection

The EU's toolbox for protecting democracy has expanded significantly over the past decade, in response to an evolving threat landscape and a more turbulent international environment. A clear illustration of this shift can be seen by comparing the "Political Guidelines" of the last three Commission Presidents and related policy documents.

In 2014, Jean-Claude Juncker's programme emphasised "democratic change", focusing on measures such as a "special partnership" between the Commission and the EP and a mandatory transparency register for the Commission and the co-legislators. These initiatives were framed primarily as responses to the EU's perceived "democratic deficit".[27]

This approach changed markedly after the 2014 Ukraine crisis and Russia's illegal annexation of Crimea, which highlighted the role of disinformation in supporting military aggression. At the time, the debate in the EU centred on strengthening "strategic communication", which can be broadly defined as the "purposeful use of communication by an organization to fulfil its mission".[28] In March 2015, the European Council tasked the High Representative/Vice-President (HR/VP) with developing an "action

[27] Juncker, J.-C., *A New Start for Europe: My Agenda for Jobs, Growth, Fairness and Democratic Change. Political Guidelines for the next European Commission*, Strasbourg, 15 July 2014.

[28] Hallahan, K., Holtzhausen, D., van Ruler, B., Verčič, D. and Sriramesh K., "Defining Strategic Communication", *International Journal of Strategic Communication*, vol. 1, no. 1, p. 3.

plan on strategic communication",[29] adopted in June 2015. Its main objectives were to (i) communicate and promote EU policies and values towards the Eastern neighbourhood, (ii) strengthen the media environment and (iii) increase public awareness on disinformation activities and improve the EU's capacity to act against them.[30]

The March 2015 Conclusions also called for a dedicated "communication team",[31] which became the East StratCom Task Force later that year. Additional regional task forces were subsequently created for the Western Balkans, the Middle East and North Africa, and Sub-Saharan Africa.[32] In November 2016, the EP welcomed these initiatives in its resolution on EU strategic communication, while stressing the need for complementary measures such as awareness raising, education, online media and information literacy.[33]

Following Russia's actions in Ukraine, the concepts of "hybrid warfare" and "hybrid threats" gained prominence in EU and international security debates. In April 2016, the Commission and the HR/VP, acting on mandate from the Council, issued a *Joint Framework on countering hybrid threats*, defining them as:

> "a mixture of coercive and subversive activity, conventional and unconventional methods (i.e. diplomatic, military, economic, technological), which can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare".[34]

The framework outlined 22 concrete actions to promote a "holistic approach" to hybrid threats, identifying strategic communication as a key priority to counter disinformation aimed at radicalizing individuals, destabilizing societies, and controlling political narratives.[35] This framework was reinforced by the *Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats*, issued after the Salisbury chemical attack.[36]

In the wake of the "Brexit" referendum and the 2016 US Presidential elections, the Commission intensified its efforts against disinformation by establishing the High Level Expert Group (HLEG) on Fake News and Online Disinformation in 2017. Its influential report abandoned the term "fake news" in

---

29 European Council, *Conclusions*, EUCO 11/15, Brussels, 20 March 2015, para. 13.

30 European External Action Service, *Action Plan on Strategic Communication*, Ares(2015)2608242, 22 June 2015, 2.

31 European Council, *Conclusions*, EUCO 11/15, *cit*., para. 13.

32 European External Action Service, *Report from the High Representative of the Union for Foreign Affairs and Security Policy. Common Foreign and Security Policy Report – Our Priorities in 2025*, HR(2025) 148, 25 June 2025, 35.

33 European Parliament resolution of 23 November 2016 on EU strategic communication to counteract propaganda against it by third parties (2016/2030(INI)), *Official Journal of the European Union*, C 224, 27 June 2018, para. 46.

34 European Commission and High Representative, *Joint Communication to the European Parliament and the Council. Joint Framework on countering hybrid threats*, JOIN(2016) 18 final, Brussels, 6 April 2016, 2.

35 *Ibid*., pp. 3 and 4-5.

36 European Commission and High Representative, *Joint Communication to the European Parliament, the European Council and the Council. Increasing resilience and bolstering capabilities to address hybrid threats*, JOIN(2018) 16 final, Brussels, 13 June 2018.

favour of the more precise concept of "disinformation", and laid the ground for future initiatives, particularly regarding online platforms. In April 2018, the European Commission issued its Communication on *Tackling online disinformation: a European Approach*, introducing a working definition of "disinformation" as

> "verifiably *false or misleading information* that is created, presented and disseminated for economic gain or to intentionally deceive the public, and may cause public harm. Public harm comprises threats to democratic political and policy-making processes as well as public goods such as the protection of EU citizens' health, the environment or security" (*emphasis added*).[37]

This Communication significantly broadened the EU's approach to disinformation, making it comprehensive and cross-sectoral. It addressed multiple domains, including online platforms, fact-checking, media literacy and election processes, with a particular focus on the 2019 EP elections.[38] Later that year, the European Commission and the High Representative issued the *Action Plan against Disinformation*, reinforcing the "whole-of-government", cross-cutting approach, and introducing key innovations such as the Rapid Alert System (RAS).[39]

Before taking office, President von der Leyen presented to the EP a "new push" for European democracy, positioned at the intersection of internal reforms and protection from external threats. On the reform side, her ambitious guidelines included an unprecedented exercise of deliberative democracy (the Conference on the Future of Europe), institutional reforms such as granting the EP the right of legislative initiative, extending co-decision powers and qualified majority voting in the Council, a stronger partnership between the EP and the Commission, improvements to the lead candidate system and the creation of an independent ethics body. At the same time, the agenda shifted toward safeguarding democracy from external interference. This included developing a joint approach and common standards to tackle disinformation and online hate speech, as well as legislative proposals under the EDAP to increase transparency in paid political advertising and strengthen rules on the financing of European political parties.[40]

The 2020 EDAP reaffirmed the EU's whole-of-government and whole-of-society approach, with the overarching goal of enhancing "democratic resilience", including the protection of critical infrastructure. These efforts were further advanced through the 2023 DoD package. A key feature of the 2020 EDAP was its conceptual clarification of information-related phenomena. It defined misinformation as "false or misleading content shared without harmful intent though the effects can

---

[37] European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Tackling online disinformation: a European Approach*, COM(2018) 236 final, Brussels, 26 April 2018, pp. 3-4.

[38] *Ibid*., pp. 6 ff.

[39] European Commission and High Representative, *Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions. Action Plan against Disinformation*, JOIN(2018) 36 final, Brussels, 5 December 2018, pp. 5 ff.

[40] von der Leyen, U., *A Union that strives for more. My agenda for Europe. Political Guidelines for the next European Commission*, Strasbourg, 16 July 2019.

still be harmful"; information influence operation as "coordinated efforts by either domestic or foreign actors to influence a target audience using a range of deceptive means, and foreign interference in the information space as "coercive and deceptive efforts to disrupt the free formation and expression of individuals' political will by a foreign state actor or its agents".[41] This conceptual clarification reflected growing concern about foreign interference in the EU democratic processes. The EP INGE and ING2 special committees[42] examined this issue in depth, while the EEAS introduced the concept of Foreign Information Manipulation and Interference (FIMI), defined as a

> "*pattern of behaviour* that threatens or has the potential to negatively impact values, procedures and political processes. Such activity is manipulative in character, conducted in an intentional and coordinated manner. Actors of such activity can be state or non-state actors, including their proxies inside and outside of their own territory" (emphasis added).[43]

The concept has become increasingly associated with the broader notion of 'information integrity', which offers a constructive framework for fostering a healthy information ecosystem in the EU. This evolution is evident in the establishment of the EEAS Division for "Information integrity and countering foreign information manipulation and interference".[44] The EU's decision to impose restrictive measures on selected Russian media outlets (see below) following Russia's war of aggression against Ukraine further illustrates this shift towards a more security-oriented approach.

In her address to the EP before her second term, President von der Leyen emphasized security, acknowledging that "our democratic systems and institutions are under attack", she promised to "do more to protect our democracy".[45] The European Democracy Shield (EDS) is central to this effort, with a strong focus on countering FIMI threats online.[46] The guidelines also stress the importance of societal resilience and preparedness, promoting digital and media literacy, and supporting independent media and journalists. Prevention through pre-bunking and the creation of a European network of fact-checkers are also endorsed. Timely implementation and enforcement of existing regulations, such as the EMFA and DSA, are highlighted as crucial steps. Furthermore, deliberative democracy and active citizen participation – such as through European Citizens' Panels – are encouraged.

These political guidelines and related documents demonstrate a clear shift in how the Commission Presidents frame democracy. First, the external dimension and security concerns have become

---

41 European Commission, *European Democracy Action Plan, cit.,* p. 18.

42 European Parliament's Special Committees on Foreign Interference in all Democratic Processes in the European Union, including Disinformation (INGE and ING2 Committees). Parliament adopted the relevant resolutions on 9 March 2022 and 1 June 2023.

43 European External Action Service, *2021 StratCom Activity Report*, Strategic Communication Task Forces and Information Analysis Division (SG.STRAT.2), Brussels, 2022, p. 2.

44 Bentzen, N., *Information integrity online and the European democracy shield*, PE 767.153, European Parliamentary Research Service, Brussels, 2024, p. 2.

45 von der Leyen, U., *Europe's Choice*, *cit*.

46 In the chapter on "a new era for European Defence and Security", President von der Leyen adds that the strategic approach to sanctions will be revised, to allow the Union to "react flexibly to new threats [...and] hybrid attacks". *Ibid.*, p. 15.

increasingly prominent, moving from a secondary issue in Juncker's guidelines to a central theme in von der Leyen's 2019 and 2024 guidelines. The latter present democracy under a security umbrella with the telling image of the 'shield'. Second, the initial focus on strategic communication in the EU's eastern neighbourhood has expanded into a whole-of-government and whole-of-society approach, aiming to strengthen democratic and societal resilience. Finally, there is a marked trend towards relying on more stringent instruments, such as regulations and restrictive measures.

2.2. Towards a 'Democracy Shield': the EU toolbox to protect democracy

Over the past decade, the EU has developed a comprehensive set of instruments to strengthen democratic resilience and counter external threats. These instruments vary in legal status – ranging from regulatory to non-regulatory measures – and span multiple policy areas, including civil liberties, institutional affairs, foreign affairs, media and culture, and the single market. Given the complexity and cross-cutting nature of challenges to democracy, the EU's responses are often presented as 'packages' that combine legislative proposals, recommendations to Member States, and guidance on the application of legislation.

In anticipation of the forthcoming Democracy Shield, the policy content of previous 'democracy' packages – namely, the 2018 "Securing Free and Fair Elections" package, the 2020 EDAP and the 2023 DoD – has been carefully reviewed. The key instruments and tools are outlined below according to the four overarching themes identified for the EDS: (1) countering disinformation and foreign information manipulation and interference; (2) ensuring the fairness and integrity of electoral processes and strengthening democratic frameworks; (3) enhancing societal resilience and preparedness; and (4) fostering citizens' participation and engagement.[47]

2.2.1. Disinformation and FIMI

The Communication on the 2018 package references the Commission's Communication *Tackling online disinformation: a European approach*, which endorses a multi-dimensional strategy to address disinformation. Notably, this includes engagement with online platforms through the development of a voluntary *Code of Practice*.[48] The Communication also acknowledges the work of the EEAS, which since 2015 has developed an Action Plan on Strategic Communication, established Task Forces (notably the East Strategic Communication Task Force), and launched the *EUvsDisinfo* programme to counter disinformation activities.[49]

The EDAP, conceived during the challenging period following the outbreak of the COVID-19 pandemic in early 2020, dedicates an entire chapter to the issue of disinformation. It focuses on strengthening cooperation structures within the EU and with international partners, enhancing coordination at the

[47] European Commission, *Call for evidence for an initiative (without an impact assessment)*, Ares(2025)2555098, 31 March 2025, p. 2. On 27 May 2025, Presidency Conclusions on strengthening EU democratic resilience were issued to contribute to the ongoing debate on the EUDS. Council of the European Union, *Presidency Conclusions on strengthening EU democratic resilience*, 9463/25, 27 May 2025.

[48] European Commission, *Tackling online disinformation: a European approach*, *cit*.

[49] European External Action Service, *Action Plan on strategic communication*, *cit*.

Member State level, adopting a more robust regulatory approach through the DSA and a strengthened Code of Practice, and enforcing the GDPR with the possibility of sanctions for repeated violations.

The Communication on DoD notes, in the section "taking the EDAP forward", the progress achieved in this area. It highlights strengthened internal and international cooperation, enhanced strategic communication responses, and improved situational awareness – facilitated respectively by the Commission's *Network against Disinformation* (NaD) and the EEAS's *Rapid Alert System* (RAS). The DSA and the revised Code of Practice have introduced stronger accountability requirements for platforms and search engines, particularly for Very Large Online Platforms and Search Engines. Several initiatives have also been implemented to support digital literacy and fact-checking, including the *European Media Digital Observatory* (EDMO) and various research programmes.

Following the 2020 EDAP, a toolbox to identify and respond to FIMI activities has been developed,[50] complementing the broader EU Hybrid Toolbox.[51] The *FIMI Toolbox* outlines the full range of tools available to counter FIMI, structured along four pillars – situational awareness, resilience building, regulation and disruption and the EU's external action.[52]

Regarding the first pillar, the EU's situational awareness has significantly improved in recent years, beginning with the developing of a behaviour-based definition of FIMI and a comprehensive methodology to identify, track, and expose such activities. Notably, the first EEAS FIMI Threat report introduced a standardized methodology for investigating FIMI activities; the second report presented a Response Framework, and the third report highlighted the underlying digital infrastructure by proposing a FIMI Exposure Matrix.[53] The EEAS-based RAS – which consists of a digital platform and a network of 27 national contact points – along with the Single Intelligence Analysis Capacity (SIAC) and its Hybrid Fusion Cell (HFC), play a critical role in maintaining the EU's situational awareness of FIMI threats. Additionally, the Helsinki-based *Hybrid Centre of Excellence* (CoE), established in 2017, conducts research on hybrid threats, including hybrid influence.[54]

It will be important to observe how the recently announced *European Centre for Democratic Resilience*, bringing together expertise and capacity across Member States and neighbouring countries,

---

[50] European External Action Service, *1st EEAS Report on Foreign Information Manipulation and Interference Threats. Towards a framework for networked defence*, Strategic Communication, Task Forces and Information Analysis (STRAT.2), Brussels, February 2023.

[51] Council of the European Union, *A Strategic Compass for Security and Defence*, 7371/22, 21 March 2022, pp. 22-23. In this context, the Council approved the guiding framework for the establishment of EU Hybrid Response Teams to support Member States, partner countries and CSDP missions and operations in countering hybrid threats in May 2024.

[52] Section 2.4 will specifically focus on the EU's External Action and diplomacy.

[53] European External Action Service, *1st EEAS Report on Foreign Information Manipulation and Interference Threats. Towards a framework for networked defence*, Brussels, February 2023, pp. 27 ff; European External Action Service, *2nd EEAS Report on Foreign Information Manipulation and Interference Threats. A Framework for Networked Defence*, Brussels, January 2024, pp. 12 ff; European External Action Service, *3rd EEAS Report on Foreign Information Manipulation and Interference Threats. cit.*, pp. 14 ff. Additional reports published by the EEAS have addressed the 'Doppelgänger' and 'False Façade' operations, among others.

[54] EU-funded research, notably under Horizon Europe, has also focused on promoting greater knowledge on FIMI and disinformation.

will interact with existing structures within this institutional framework.[55] In February 2025, such structures were expanded with the establishment of a dedicated Task Force on strategic communication and countering information manipulation within the European Commission's DG COMM.[56] In this context, it is also noteworthy that the 2025-2027 *Digital Europe Programme* (DEP) allocates 14 million EUR for the creation of a Situational Awareness and Operational Centre (SAOC) to "enhance the EU's capacity to detect and counter disinformation, including foreign interference".[57]

A wide range of activities fall under the "resilience building" pillar, beginning with awareness-raising measures. *EUvsDisinfo* is the flagship project in this area, featuring over 18,000 documented cases of pro-Kremlin disinformation exposed and debunked as of December 2024.[58] Strategic communication is another key work strand, with the EEAS – particularly through its StratCom Task Forces – playing a central role by implementing communication projects, conducting TAIEX missions, and supporting independent media and EU Delegations on the ground.[59] Cooperation with civil society and fact-checking organizations has intensified in recent years. Notably, the *FIMI Information Sharing and Analysis Centre* (FIMI ISAC), launched in 2023, brings together like-minded organizations to foster collective situational awareness and promote interoperability.[60] Additionally, the European Commission has recently launched a call for proposals (worth approximately €5 million) to strengthen a *European Network of Fact Checkers* under the Digital Europe Programme.[61] Finally, internal organizational structures and mechanisms are essential for ensuring the EU's resilience against FIMI. In this context, it is important to recall the *Integrated Political Crisis Response* (IPCR) arrangements, which were activated in information-sharing mode on foreign interference in the run-up to the 2024 EP elections.[62]

Within the "disruption and regulation" pillar, the Digital Services Act (DSA) stands out as the landmark piece of legislation. The strengthened Code of Practice on disinformation was integrated as a Code of Conduct under the DSA starting from July 2025. Chapter 3 will provide a detailed analysis of the current

---

55 European Commission, "2025 State of the Union Address by President von der Leyen", cit.

56 European Commission, "Daily News", 3 February 2025. https://ec.europa.eu/commission/presscorner/detail/en/mex_25_399

57 European Commission, *Annex to the Commission Implementing Decision on the financing of the Digital Europe Programme and the adoption of the multiannual work programme for 2025 – 2027*, C(2025) 1839 final ANNEX, Brussels, 28 March 2025, pp. 172-173.

58 European External Action Service, *2024 Report on EEAS Activities to Counter Foreign Information Manipulation and Interference (FIMI)*, Brussels, August 2025, p. 10.

59 Ibid., p. 9 ff. Media freedom and pluralism, as well as media and digital literacy, within the EU are analysed in subsequent sections.

60 European External Action Service, *Annual Progress Report on the Implementation of the Strategic Compass for Security and Defence. Report of the High Representative of the Union for Foreign Affairs and Security Policy to the Council*, Brussels, March 2024, p. 15.

61 European Commission, *Digital Europe Programme*, *cit.*, pp. 169-171.

62 Council of the European Union, "Foreign interference: Presidency reinforces exchange of information ahead of the June 2024 European elections", *Press release*, 24 April 2024. https://www.consilium.europa.eu/en/press/press-releases/2024/04/24/foreign-interference-presidency-reinforces-exchange-of-information-ahead-of-the-june-2024-european-elections/

state of enforcement. For now, it is worth noting that the European Commission has recently complemented the DSA with a Delegated Regulation on data access for qualified researchers and an Implementing Regulation specifying rules and templates for transparency reporting, among others.[63] Considering technological developments, the provisions of the AI Act are also relevant. For example, Annex III of the Regulation classifies "AI systems intended to influence the outcome of an election or referendum or the voting behaviour of individuals" as high-risk, subject to additional obligations. Article 50(4) further requires that deployers of AI-generated "deep fakes" disclose that the content has been artificially generated or manipulated.[64] Proactively, EU institutions are also increasing efforts to use generative AI to counter FIMI and disinformation, as seen in initiatives such as EUvsDisinfo.[65] The EU rules applicable in the digital space are set to expand with the Digital Fairness Act, which is expected to address dark patterns and other unfair techniques, among others.[66]

2.2.2. Electoral processes and democratic frameworks

Recognizing the competences and role of Member States in this area, the 2018 Communication – which laid the groundwork for the 2019 EP elections – presents several recommendations to safeguard the integrity of electoral processes. It calls for extending conventional ("offline") electoral safeguards – such as rules on political communications during election periods, transparency and limits on electoral spending, respect for silence periods, and equal treatment of candidates – to digital media and platforms. The Communication also endorses the use of sanctions to combat fraud and other deliberate attempts to manipulate elections. Member States are encouraged to establish national election networks and appoint contact points to participate in the *European Cooperation Network for Elections* (ECNE), fully supported by the Commission. Cybersecurity is identified as a common challenge, with the *Compendium on Cyber Security of Election Technology*, prepared by the NIS Cooperation Group, providing practical guidance for cybersecurity authorities and election management bodies.

To support resilient electoral processes, the EDAP proposed the establishment of a new *Joint mechanism for electoral resilience*, coordinated through the ECNE.[67] While the organization of national and EP elections remains the responsibility of Member States, the EU directly regulates and funds EU-level political parties and foundations. The existing regulation governing their statute and funding –

---

[63] Commission Implementing Regulation (EU) 2024/2835 of 4 November 2024 laying down templates concerning the transparency reporting obligations of providers of intermediary services and of providers of online platforms under Regulation (EU) 2022/2065 of the European Parliament and of the Council, *Official Journal of the European Union*, L, 2024/2835, 5 November 2024; European Commission, "Delegated act on data access under the Digital Services Act (DSA)", 2 July 2025. https://digital-strategy.ec.europa.eu/en/library/delegated-act-data-access-under-digital-services-act-dsa

[64] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), *Official Journal of the European Union*, L, 2024/1689, 12 July 2024, Art. 50(4) and Annex III.

[65] Cfr. *EUvsDisinfo* Youtube channel: https://www.youtube.com/@euvsdisinfo/videos.

[66] European Commission, *Call for Evidence for an Impact Assessment*, Ares(2025)5829481, 17 July 2025, p. 2.

[67] For more information on the ECNE and the Joint mechanism for electoral resilience, see E. Bressanelli and S. Bernardi, *Resilience of democracy*, *cit.*, pp. 37-38.

particularly to address financing from outside the EU – had to be revised accordingly. To mitigate cybersecurity risks, the EDAP also foresaw an update to the *Compendium on Cyber Security of Election Technology*, to be complemented by a new compendium focused on e-voting practices.

In late 2023, the Communication on DoD – adopted a few months ahead of the 2024 EP elections – endorsed the adoption of code of conducts and campaign pledges by political parties to promote fair campaigning and transparency. It emphasised the need to strengthen both the physical and cyber security of election technology, in line with the requirements of the *revised NIS2 Directive* and the *Critical Entities Resilience (CER) Directive*. The Communication also called for a review of the abovementioned *Compendium on Cybersecurity of Election Technology* to ensure it remained aligned with technological developments and emerging threats. The Commission pledged continued support to national administrations in reinforcing democratic processes through the *Technical Support Instrument.*

In the lead up to the 2024 EP elections, the European Commission issued a *Recommendation on inclusive and resilient electoral processes* as part of the DoD package. This sets out a broad range of measures to safeguard election integrity including the protection of electoral infrastructure and the strengthening of existing election networks.[68]

More recently, electoral integrity has been embedded within the scope of the *European Preparedness Union Strategy*[69] and the *Internal Security Strategy*, [70] underscoring the growing importance of resilience and crisis prevention in the face of an evolving hybrid threat landscape.

2.2.3. Societal resilience, preparedness and media literacy

Prior to the 2019 EP elections, key legislation was already in place to regulate electoral contexts. This included the General Data Protection Regulation (GDPR) governing the use of personal data, the Directive on Privacy and Electronic Communications addressing unsolicited communications – including political messaging – and the Directive on Attacks Against Information Systems, which harmonized definitions of cyber offences and penalties across Member States.

The EDAP significantly expanded these efforts. It proposed a legislative initiative on the *transparency of sponsored political content*, complementing the DSA rules on online advertising, and called for the extension of the list of EU crimes to include hate speech and hate crime. The *Regulation on the transparency and targeting of political advertising*, adopted in April 2024, introduces transparency requirements for political advertising services in the internal market. Most of its provisions enter into

[68] Commission Recommendation (EU) 2023/2829 of 12 December 2023 on inclusive and resilient electoral processes in the Union and enhancing the European nature and efficient conduct of the elections to the European Parliament, *Official Journal of the European Union,* 2023/2829, 20 December 2023.

[69] European Commission and High Representative*, Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on the European Preparedness Union Strategy*, JOIN(2025) 130 final, Brussels, 26 March 2025.

[70] European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on ProtectEU: a European Internal Security Strategy*, COM(2025) 148 final, Brussels, 1 April 2025.

force in October 2025, including rules on the use of personal data in targeting and ad delivery techniques.[71]

In parallel, several initiatives were launched to promote media freedom, journalist safety, and media literacy. These include the implementation of the *Audio-Visual Media Services Directive* (AVMSD), the creation of a *Media Ownership Monitor*, legislation to protect journalists and civil society from Strategic Lawsuits Against Public Participation (SLAPPs), and common guidelines for educators. Funding mechanisms such as *Creative Europe* and the *Rights and Values Programme* were mobilized to support media literacy and civil society. The Commission also issued a *Recommendation on the safety of journalists* and established an expert group on SLAPPs in 2021. An anti-SLAPPs legislative package was presented in April 2022. Moreover, the EP investigated the use of Pegasus and similar surveillance spyware through a dedicated Committee of Inquiry, culminating in a June 2023 Resolution strongly condemning such practices and calling for appropriate safeguards.[72]

These efforts were further advanced in the DoD package. Most notably, it introduced a legislative proposal to enhance transparency and public scrutiny of interest representation activities funded by third countries. It also called for the implementation of the *anti-SLAPPs Directive*, the enforcement of the *European Media Freedom Act* (EMFA), and a revision of the financial regulation to exclude EU funding for entities promoting discrimination, hatred, or violence. Continued support for independent media was reaffirmed, including through funding under Creative Europe. In her latest State of the Union address, President von der Leyen reiterated this commitment, announcing the launch of a "Media Resilience Programme".[73]

Over time, targeted measures have also been introduced to support awareness-raising, capacity-building and media and digital literacy among the general public. The *Communication on the Union of Skills*, issued in March 2025, reinforced this agenda, stating that "building skills for life, including media, digital literacy, critical thinking or basic cybersecurity, is vital for Europe's overall preparedness in the face of crises, including in terms of democratic resilience".[74] This approach was later confirmed by the *European Preparedness Union Strategy*, which emphasised the importance of fostering "population preparedness" across the EU.[75]

---

[71] Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on the transparency and targeting of political advertising, *Official Journal of the European Union*, 2024/900, 20 March 2024, Art. 1.

[72] European Parliament recommendation of 15 June 2023 to the Council and the Commission following the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware, *Official Journal of the European Union*, C/2024/494, 23 January 2024, spec. paras. 3 ff.

[73] European Commission, "2025 State of the Union Address by President von der Leyen", cit.

[74] European Commission, *Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions. The Union of Skills*, COM(2025) 90 final, Brussels, 5 March 2025, p. 7.

[75] European Commission, *European Preparedness Union Strategy*, *cit.*, spec. p. 9.

2.2.4. Citizens' participation and civil society's engagement

The Communication accompanying the 2018 package emphasised the importance of early and sustained engagement with citizens on European issues. It called for earlier campaign launches by political parties for the elections to the EP, greater transparency regarding the links between national and European political parties, and stronger promotion of voting rights by Member States. It underlined that "meaningful results will only be achieved if all the relevant actors work together".

The EDAP reaffirmed this commitment, stating that such efforts were at the core of the Commission's work in many areas. Its flagship initiative was the *Conference on the Future of Europe*, complemented by other citizen engagement tools such as *Citizens' Dialogues*. Particular attention was given to youth participation through the *EU Youth Strategy*. Financial support for deliberative democracy was provided through programmes such as *Creative Europe, Horizon2020* and *Horizon Europe*. For instance, the 2025 Horizon Europe Work Programme includes calls focused on civic and citizenship education and the creation of a community of democracy practitioners and researchers.[76] Additionally, a *Competence Centre on Participatory and Deliberative Democracy* was established within the *Joint Research Centre* (JRC) in September 2021.[77]

The DoD package further reinforced support for civil society. It introduced a legislative initiative to facilitate the cross-border activity of associations by removing barriers in the single market, and proposed updates to the Better Regulation Guidelines to enhance stakeholder participation. Election observation was also promoted as a best practice. As part of the DoD package, the European Commission issued a *Recommendation on promoting the engagement and effective participation of citizens and civil society organisations in public policy-making processes*. It encourages Member States to establish frameworks that enable citizen and civil society participation in policymaking, including citizen-led participatory and deliberative exercises.[78]

New initiatives, such as the forthcoming *Civil Society Strategy*, continue this trajectory, reinforcing the EU's commitment to inclusive and participatory democracy.[79]

---

[76] European Commission, *Commission Implementing Decision of 14.5.2025 on the financing of the Specific Programme implementing Horizon Europe and the adoption of the work programme for 2025-2027 ('Work Programme 2025'). Work Programme 2025. Culture, Creativity and Inclusive Society*, C(2025) 2779 final, Brussels, 14 May 5, pp. 49 and 55.

[77] European Commission, *Annex to the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Defence of Democracy*, COM(2023) 630 final, Strasbourg, 12 December 2023, p. 6.

[78] Commission Recommendation (EU) 2023/2836 of 12 December 2023 on promoting the engagement and effective participation of citizens and civil society organisations in public policy-making processes, *Official Journal of the European Union*, L, 2023/2836, 20 December 2023, spec. paras. 3 and 11.

[79] European Commission, *Call for Evidence for an initiative (without an impact assessment)*, Ares(2025)4722887, 13 June 2025.

Table 1: The EU toolbox to protect democracy

	Countering Disinformation and FIMI	Fairness and integrity of elections	Societal resilience and preparedness	Citizens' participation and engagement
Legislation	DSA	CER directive; NIS2 directive; regulation on European political parties and foundations; Regulation on transparency and targeting of political advertising	Anti-SLAPPs directive; AVMSD; EMFA	Directive on EU mobile citizens; Proposal for a regulation on cross-border activity of associations
Institutions	RAS; FIMI ISAC; HFC; Hybrid CoE; EDMO; NaD; EBDS	ECNE; NIS cooperation group	EDMO; Media Board	CoFE; JRC
Instruments	Code of conduct (formerly Code of practice) on disinformation; EuvsDisinfo; EU FIMI Toolbox.	Code of conduct for political parties; compendium on cyber security of election technology and compendium on e-voting practices; mechanism to support resilient electoral processes; sanctions	Extension of the EU crime list including hate crime and hate speech; common guidelines for teachers and educational staff; media ownership monitor	Better regulation guidelines; Citizens' dialogues; EU Youth Strategy; observation of elections
Funding	Digital Europe programme; EU Preparatory actions	Technical Support Instrument	Creative Europe, Rights and Values programme	Creative Europe; H2020; Horizon Europe

2.3. Protecting critical infrastructure in the EU

In recent years, the EU's critical infrastructure has faced an increasing range of natural and man-related threats. The *European Internal Security Strategy*, released in April 2025, confirmed a rise in sabotage targeting critical infrastructure – particularly throughout 2024 – following Russia's war of aggression against Ukraine.[80] These developments have underscored the urgent need to strengthen infrastructure resilience and accelerated efforts to modernise the EU's framework, which had remained largely unchanged since the establishment of the *European Programme for Critical Infrastructure Protection* (EPCIP) and the adoption of the first *Directive on European Critical Infrastructure* in 2008.

In response to the sabotage of the Nord Stream 1 and 2 pipelines in September 2022,[81] President von der Leyen proposed a five-point plan to strengthen the protection of critical infrastructure within EU

[80] European Commission, *ProtectEU: a European Internal Security Strategy*, *cit.*, p. 11.

[81] On 26 September 2022, several underwater explosions hit the Nord Stream 1 and 2 pipelines, built to facilitate gas exports from Russia to Germany, causing gas leaks.

territory. The plan laid the groundwork for subsequent EU-level initiatives and called for: (i) improved preparedness through the implementation of relevant Union legislation; (ii) stress testing of critical infrastructure; (iii) mobilisation of the Union Civil Protection Mechanism (UPCM), (iv) use of satellite surveillance capacities and (v) strengthened cooperation with NATO and other key partners.[82]

Building on this momentum, in October 2022 the European Commission proposed a *Council Recommendation on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure*, which was adopted two months later. The Recommendation outlines targeted actions at both national and EU levels across three main dimensions: preparedness, response and international cooperation.[83] Notably, it includes a commitment by the Council to work towards a Blueprint on a coordinated response to disruptions affecting critical infrastructure with significant cross border implications.[84]

The *Critical Infrastructure Blueprint* was adopted in June 2024 through a Council Recommendation.[85] It establishes detailed cooperation arrangements between Member States and relevant EU institutions, bodies, offices, and agencies (EUIBAs) for responding to incidents affecting critical infrastructure. The Blueprint aims to (i) promote a shared threat assessment, (ii) coordinate public communication and (iii) achieve a coordinated and effective response.[86] It is designed to complement existing EU crisis and emergency management mechanisms, including the IPCR arrangements, the Commission's ARGUS, the EEAS Crisis Response Mechanism, the UPCM, the EU Protocol for countering hybrid threats ("EU Playbook") and the NIS2 provisions on the coordinated management of large-scale cybersecurity incidents.[87]

These initiatives form part of a broader framework anchored in the *Critical Entities Resilience* (CER) Directive, the EU's flagship legislation for protecting critical infrastructure against all hazards. Proposed in 2020 and in force since January 2023, the CER Directive aims to ensure the uninterrupted provision of services essential to vital societal functions and economic activities within the internal market. It establishes specific obligations for both Member States and critical entities.[88] By 17 January 2026, Member States must compile a list of critical entities operating across eleven designated sectors (see Table 2), guided by national resilience strategies and risk assessments covering both natural and man-

[82] European Commission, "Speech by President von der Leyen at the European Parliament Plenary on Russia's escalation of its war of aggression against Ukraine", *Speech*, Strasbourg, 5 October 2022. https://ec.europa.eu/commission/presscorner/detail/en/speech_22_5964. For instance, see below EU-NATO initiatives in the field, including the EU-NATO Dialogue on Resilience.

[83] Council Recommendation of 8 December 2022 on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure, *Official Journal of the European Union*, C, 20, 20 January 2023, point. 1.

[84] *Ibid*., points. 25(a) and 31.

[85] Council Recommendation of 25 June 2024 on a blueprint to coordinate a response at Union level to disruptions of critical infrastructure with significant cross-border relevance, *Official Journal of the European Union*, C, 2024/4371, 5 July 2024.

[86] *Ibid*., point 1 and Annex, Part I, point 1.

[87] *Ibid*., Annex, Part IV.

[88] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC, *Official Journal of the European Union*, L, 333, 27 December 2022, Art. 1(1).

made threats. [89] To support this process, a delegated act adopted in July 2023 provides a non-exhaustive list of essential services.[90]

Table 2: Sectors covered under the CER Directive and the NIS2 Directive

Sector	CER	NIS2	Sector	CER	NIS2
Energy	■	■	Transport	■	■
Banking	■	■	Financial market infrastructures	■	■
Health	■	■	Drinking water	■	■
Waste water	■	■	Digital infrastructure	■	■
ICT service management		■	Public administration	■	■
Space	■	■	Postal and courier services		■
Waste management		■	Manufacture, production and distribution of chemicals		■
Production, processing and distribution of food	■	■	Manufacturing		■
Digital providers		■	Research		■

Sources: NIS2 Directive, Annexes I and II; CER Directive, Annex.

The EP, in its INGE and subsequent ING2 Resolutions, recommended expanding the list of critical entities to include digital election infrastructure and education systems, recognizing their importance for long-term stability. It also called for flexibility in adding new strategic sectors.[91] At the Council level, the PROCIV CER Working Group monitors the implementation of measures under the CER Directive. As part of the European Preparedness Union Strategy, the European Commission and the High Representative have announced plans to work with Member States to identify sectors and services currently not covered by existing legislation. Based on this assessment, they will propose recommendations on minimum preparedness requirements, including a monitoring mechanism.[92] This strategy also includes the establishment of a Public-Private Preparedness Task Force and the development of public-private emergency protocols.[93]

[89] *Ibid*., Art. 6.

[90] Commission Delegated Regulation (EU) 2023/2450 of 25 July 2023 supplementing Directive (EU) 2022/2557 of the European Parliament and of the Council by establishing a list of essential services, *Official Journal of the European Union*, L, 2023/2450, 30 October 2023.

[91] European Parliament resolution of 9 March 2022 on foreign interference in all democratic processes in the European Union, including disinformation, *Official Journal of the European Union*, C, 347, 9 September 2022, para. 75; European Parliament resolution of 1 June 2023 on foreign interference in all democratic processes in the European Union, including disinformation, *Official Journal of the European Union*, C, 2023/1226, para. 61.

[92] European Commission and High Representative, *European Preparedness Union Strategy*, *cit*., p. 7.

[93] *Ibid*., p. 11.

In response to multiple incidents affecting seabed cables in the Baltic Sea,[94] the EU has launched a dedicated initiative to strengthen the resilience of submarine critical infrastructure. In February 2024, the European Commission issued a *Recommendation on Secure and Resilient Submarine Cable Infrastructures,* outlining measures for Member States to implement at both national and EU levels. These include EU-wide mapping of existing submarine cable infrastructure and the development of regular, consolidated assessments of risks, vulnerabilities, and dependencies. The ultimate goal is to produce a *Cable Security Toolbox* – a set of recommended mitigation actions.[95]

The Recommendation also calls for identifying strategic *Cable Projects of European Interest* (CPEIs), based on risk assessments conducted by the Submarine Cable Infrastructure Expert Group. [96] At the Group's fourth meeting, the Commission proposed: (i) publishing the mapping analysis and risk assessment – including stress test methodologies – in autumn 2025, aligned with a planned call under the DEP; and (ii) releasing the *Cable Security Toolbox* and the priority list of CPEIs by year-end.[97] Member States are expected to assess the impact of the Recommendation by December 2025, considering the Union-wide risk assessment.[98]

These measures complement broader efforts outlined in key EU policy documents. The revised *EU Maritime Security Strategy* (EUMSS), adopted in October 2023 alongside its Action Plan, includes actions to enhance the resilience of critical maritime infrastructure – such as improved information exchange, stress testing, risk assessments, and maritime exercises.[99] Progress is regularly reported to the EUMSS Working Party in the Council.

In its January 2024 Resolution on the security and defence implications of China's influence on EU critical infrastructure, the EP called on the European Commission to propose a legislative framework to address security risks from suppliers of undersea cable systems.[100] Looking ahead, the *Niinistö Report* – aligned with the White Paper *How to master Europe's digital infrastructure needs?* –

[94] In addition to the mentioned Nord Stream 1 and 2, other incidents in the Baltic Sea affected the Balticonnector gas pipeline in October 2023, the BCS East-West Interlink and C-Lion1 fibre-optic cables in November 2024, and the EastLink2 cable (December 2024), among others.

[95] Commission Recommendation (EU) 2024/779 of 26 February 2024 on Secure and Resilient Submarine Cable Infrastructures, *Official Journal of the European Union*, L, 2024/779, 8 March 2024, paras. 16-20.

[96] *Ibid*., paras. 24 ff.

[97] European Commission, *Minutes. 4th Meeting of the Submarine Cable Infrastructure Expert Group*, Brussels, 18 June 2025. According to the Action Plan on Cable Security (see below), the funding for preparedness testing/stress testing will be delivered within the framework of the Cyber Solidarity Act and through the Digital Europe Programme, where EUR 30 million are allocated for preparedness actions in critical sectors until 2027 (p. 3).

[98] Commission Recommendation (EU) 2024/779, *cit*., para. 34.

[99] Council of the European Union, *Council conclusions on the Revised EU Maritime Security Strategy (EUMSS) and its Action Plan*, 14280/23, Brussels, 24 October 2023, Annex II to the Annex, points 3.1.3, 4.2.1-4.2.9, 4.7.4.

[100] European Parliament resolution of 17 January 2024 on the security and defence implications of China's influence on critical infrastructure in the European Union, *Official Journal of the European Union*, C, 2024/5719, 17 October 2024, para. 27.

advocated for the establishment of an EU governance system to harmonize risk assessments and security requirements across Member States.[101]

In February 2025, the EU presented a dedicated *Action Plan on Cable Security* to consolidate existing and new efforts under a comprehensive "whole resilience cycle approach".[102] Under the "Prevention" pillar, key actions include implementing existing legislative frameworks – particularly the CER Directive and the NIS2 Directive – and prioritising investment in smart cable infrastructure, supported by the development of an EU Investment Framework for submarine Cable projects.[103]

The "Detection" pillar focuses on enhancing threat awareness and early warning capabilities. Core actions include the setup of an "Integrated Surveillance Mechanism for Submarine cables" tailored to each sea basin – on a voluntary basis and starting from a Nordic/Baltic Regional Hub – and the deployment of new technologies to ensure early threat detection.[104]

Under the "Response and Recovery" pillar, the Action Plan proposes strengthening existing repair capabilities advancing the creation of a fully-fledged "EU Cable multipurpose Vessels Reserve" for cable deployment and repair. It also highlights the importance of enhanced cooperation with NATO, particularly through the EU-NATO Structured Dialogue on Resilience.[105] A joint EU-NATO Task Force on Resilience of Critical Infrastructure, established in January 2023, issued its final report in June of that year.[106]

Finally, the "Deterrence" pillar suggests measures to raise the cost for perpetrators, including full use of the Hybrid toolbox, actions against the so-called "shadow fleet" and the promotion of a proactive cable diplomacy on the global stage.[107] As an initial follow-up, in May 2025 the European Commission and members of the Baltic Energy Market Interconnection Plan (BEMIP) High-Level Group signed a Memorandum of Understanding to strengthen regional energy cooperation.[108]

As for the defence dimension, the protection of critical infrastructure became a capability development priority with the approval of the Capability Development Plan in 2023. Some PESCO projects are aimed at developing capabilities in this area,[109] such as the Modular Seabed Vessel and the Critical Seabed Infrastructure Protection.

---

[101] Niinistö, S., *Safer Together. Strengthening Europe's Civilian and Military Preparedness and Readiness*, Brussels, 2024, p. 99 ss.

[102] European Commission and High Representative, *EU Action Plan on Cable Security*, *cit.*, p. 1.

[103] *Ibid.*, 2-9.

[104] *Ibid.*, 10-12.

[105] *Ibid.*, 12-14

[106] EU and NATO, *EU-NATO Task Force on Resilience of Critical Infrastructure. Final assessment report*, June 2023.

[107] *Ibid.*, 15-17.

[108] European Commission, "New Memorandum of Understanding to bolster energy cooperation in the Baltic Sea Region", 13 May 2025. https://energy.ec.europa.eu/news/new-memorandum-understanding-bolster-energy-cooperation-baltic-sea-region-2025-05-13_en

[109] European Commission and High Representative, *Joint Staff Working Document. Eighth progress report on the implementation of the 2016 Joint framework on countering hybrid threats and the 2018 Joint communication on*

Following recent multiple violations of the EU and NATO airspace by Russian aircrafts and drone incidents at European airports,[110] the EU has embarked on a process to secure European skies. Plans are reportedly underway to develop a "drone wall", to be possibly financed through the Security Action for Europe loans scheme.[111] Moreover, the Commission is currently developing capabilities to monitor radio interference and it is preparing a fully-fledged Galileo Signal Authentication Service to enhance protection against spoofing threats.[112] A Galileo Open Service Navigation Message Authentication has been operational since July 2025.[113]

2.3.1. Cybersecurity

In recent years, the EU's cybersecurity framework has been significantly strengthened to address an increasingly complex and challenging threat landscape. A key development in this regard is the Directive on measures for a high common level of cybersecurity across the Union (*NIS2 Directive*), adopted in December 2022. The NIS2 Directive establishes a broader and more coherent legal framework aimed at enhancing cybersecurity across the EU. Under the Directive, Member States are mandated to develop a national cybersecurity strategy – which must address the governance framework, supply chain security and cybersecurity awareness – and to establish a list of essential entities.[114] The NIS2 Directive also introduces cybersecurity risk-management measures and incident reporting obligations for essential entities in 18 critical sectors.[115]

The NIS2 Directive establishes a network of Computer Security Incident Response Teams (CSIRTs) tasked with monitoring, analysing and responding to cyber threats, vulnerabilities and incidents.[116] To ensure coordinated management and proper information exchange in case of large-scale cybersecurity incidents, the Directive also envisages a European Cyber crisis liaison organisation network (EU-CyCLONe).[117] Furthermore, a Cooperation Group supports the implementation of the Directive across

increasing resilience and bolstering capabilities to address hybrid threats, SWD(2024) 233 final, Brussels, 10 October 2024, p. 8.

[110] Cfr. NATO, "Statement by the North Atlantic Council on recent airspace violations by Russia", 23 September 2025. https://www.nato.int/cps/en/natohq/official_texts_237721.ht

[111] Bryant, M. and Rankin, J., "Talks on European 'drone wall' after Danish airport intrusions", *The Guardian*, 25 September 2025. https://www.theguardian.com/world/2025/sep/25/drones-aalborg-airport-denmark-closed-days-after-copenhagen-oslo

[112] Committee on Security and Defence (SEDE). Committee meeting. Russia's hybrid warfare against the European Union, cit.

[113] European Commission. "Galileo's OSNMA Authentication Service Now Operational", 25 August 2025. https://defence-industry-space.ec.europa.eu/galileos-osnma-authentication-service-now-operational-2025-08-25_en

[114] 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 (NIS 2 Directive), *Official Journal of the European Union*, L, 333, 27 December 2022, Arts. 3(3) and 7.

[115] *Ibid*., Annexes I and II. Entities classified as critical entities pursuant to the CER Directive also fall under the scope of the NIS2 Directive.

[116] NIS2 Directive, *cit*., Art. 15.

[117] *Ibid*., Art. 16.

the Union.[118] Significantly, the NIS2 Directive provides also for the setup of a European vulnerability database, which was launched by ENISA in May 2025.[119]

The provisions set out in the Directive have been further complemented by the *Regulation laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union*, adopted in December 2023. This Regulation establishes a minimum set of cybersecurity rules and standards applicable to EUIBAs. In March 2022, the European Court of Auditors had found that "the EUIBA community has not achieved a level of cyber preparedness commensurate with the threats", with significant shortfalls identified in cybersecurity practices, training and governance.[120] Specifically, the Regulation mandates the establishment of an internal cybersecurity risk-management, governance and control framework in each Union entity, provides for the creation of an Interinstitutional Cybersecurity Board (IICB) and broadens the mandate of the CERT-EU.[121] These new structures operate alongside ENISA, whose mandate is laid down in the Cybersecurity Act, and the European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC), the EU's framework promoting research, innovation and deployment in the area of cybersecurity.[122] Additionally, a Regulation on horizontal cybersecurity requirements for products with digital elements (*Cyber Resilience Act*), adopted in October 2024, introduces horizontal cybersecurity requirements for products with digital elements made available in the EU internal market.[123] These requirements will largely become applicable from 2027 onwards.

In addition to the above-mentioned developments, it is important to highlight three key initiatives, which were presented by the European Commission as part of a broader cybersecurity package unveiled in April 2023. The first of these is the *Cyber Solidarity Act*, which entered into force on 4 February 2025. The Act is designed to strengthen the EU's capacity to detect, prepare for and respond to cyber threats and incidents.[124] To this end, it provides for the establishment of a European

---

[118] *Ibid*., Art. 14.

[119] ENISA, "Consult the European Vulnerability Database to enhance your digital security!", *Press Release*, 13 May 2025. https://www.enisa.europa.eu/news/consult-the-european-vulnerability-database-to-enhance-your-digital-security

[120] European Court of Auditors, *Cybersecurity of EU institutions, bodies and agencies : Level of preparedness overall not commensurate with the threats*, Special Report 05/2022, 29 March 2022, pp. 4 ff.

[121] Regulation (EU, Euratom) 2023/2841 of the European Parliament and of the Council of 13 December 2023 laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union, *Official Journal of the European Union*, L, 2023/2841, 18 December 2023, spec. Arts. 1, 6, 10 and 13.

[122] Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres, *Official Journal of the European Union*, L, 202, 8 June 2021, Art. 4.

[123] Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act), *Official Journal of the European Union*, L, 2024/2847, 20 November 2024, Art. 1.

[124] Regulation (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694 (Cyber Solidarity Act), *Official Journal of the European Union*, L, 2025/38, 15 January 2025, Art. 1.

Cybersecurity Alert System, comprising both national and cross-border "Cyber Hubs".[125] Additionally, the Act sets out the setup of a Cybersecurity Emergency Mechanism supporting (i) preparedness actions, (ii) the creation of an EU Cybersecurity Reserve composed of trusted managed security service providers and (iii) assistance actions.[126] The Digital Europe Programme (DEP) allocates EUR 36 million for the creation of this Reserve, which is operated by ENISA.[127] The Act also foresees the creation of a European Cybersecurity Incident Review Mechanism to review and assess occurred incidents at the request of the European Commission or EU-CyCLONe.[128] Closely linked to these mechanisms is the revised *EU blueprint for cyber crisis management*, adopted in June 2025, which outlines the procedures rules for managing large-scale cybersecurity incidents and cyber crises.[129]

The second initiative under the April 2023 cybersecurity package is the creation of a *Cybersecurity Skills Academy*, aimed at addressing the cybersecurity talent gap across the EU, while the third initiative introduced a targeted amendment to the Cybersecurity Act enabling the future adoption of European certification schemes for "managed security services".[130] Looking ahead, the 2025 European Internal Security Strategy announced that the European Commission will table a revision of the *Cybersecurity Act* in 2025 and propose measures to ensure cybersecure use of Cloud services.[131] Lastly, particular attention has been given to the healthcare sector through the *Action Plan on the cybersecurity of hospitals and healthcare providers*, adopted by the European Commission in January 2025.[132]

As for the space domain, a proposal for a fully-fledged *EU Space Act* has been presented by the European Commission on 25 June 2025. It sets out rules to ensure the safety and sustainability of space activity, as well as the resilience of the EU's space infrastructure. Among its key provisions, the Act introduces cybersecurity rules applicable to space operators and assets of space infrastructure, serving as a sector-specific Union legal act with regard to the NIS2 Directive and complementing the CER Directive.[133] Global Navigation Satellite System (GNSS) services have increasingly come under scrutiny due to a growing number of incidents threatening their continued operation. In May 2025, several

[125] *Ibid*., spec. Arts. 3 and 4.

[126] *Ibid*., spec. Arts., 10 and 11.

[127] European Commission, *Annex to the Commission Implementing Decision on the financing of the Digital Europe Programme and the adoption of the multiannual work programme for 2025 – 2027*, C(2025) 1839 final, Brussels, 28 March 2025, pp. 104-105.

[128] Cyber Solidarity Act, *cit*., Art. 21.

[129] Council Recommendation of 6 June 2025 on an EU blueprint for cyber crisis management, *Official Journal of the European Union*, C, 2025/3445, 20 June 2025.

[130] European Commission, "Cyber: towards stronger EU capabilities for effective operational cooperation, solidarity and resilience", *Press release*, 18 April 2023. https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2243

[131] European Commission, *ProtectEU: a European Internal Security Strategy*, *cit*., p. 17.

[132] European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. European action plan on the cybersecurity of hospitals and healthcare providers*, COM(2025) 10 final, Brussels, 15 January 2025.

[133] European Commission, *Proposal for a Regulation of the European Parliament and of the Council on the safety, resilience and sustainability of space activities in the Union*, COM(2025) 335 final, Brussels, 25 June 2025, Art. 75.

Member States asked the European Commission to take stronger action to tackle GNSS interference across the EU.[134]

In the defence domain, the EU Policy on Cyber Defence was released in November 2022. Complementing existing initiatives, including the Cyber Diplomacy Toolbox, the Cyber Defence Policy builds on four pillars: (i) act together for a stronger cyber defence, (ii) secure the EU defence ecosystem, (iii) invest in cyber defence capabilities and (iv) partner to address common challenges.[135] An Annual Progress Report of the EU Cyber Defence Policy is issued on a yearly basis, called the "EU Cyber Census".

A final mention should also be devoted to measures enhancing the protection of 5G networks, notably the 5G Cybersecurity Toolbox, which "currently is insufficiently implemented by Member States",[136] raising concerns over the EU's digital infrastructure resilience.

[134] Council of the European Union, *Call for common actions in response to Global Satellite Navigation Systems (GNSS) jamming and spoofing threats*, 9188/1/25 REV 1, Brussels, 4 June 2025.

[135] European Commission and High Representative, Joint Communication to the European Parliament and the Council. EU Policy on Cyber Defence, JOIN(2022) 49 final, Brussels, 10 November 2022.

[136] European Commission, *ProtectEU: a European Internal Security Strategy, cit.*, 13.

Box 2: Protecting the EU's elections from cyber and hybrid threats

As part of the DoD package, the European Commission issued a Recommendation on inclusive and resilient electoral processes, urging Member States to implement measures enhancing resilience against cyber and other hybrid threats. In preparation for the 2024 EP elections, a Compendium of e-voting and other information and communication technology practices was developed under the ECNE framework. Building on the 2023 Commission Recommendation, the NIS Cooperation Group also published an updated Compendium on Elections Cybersecurity and Resilience, revising its 2018 version.

To stress-test cybersecurity capabilities, several table-top exercises have been organised, including ELEx23 ahead of the 2024 EP elections. In addition to relevant formations in the Council, platforms such as the ECNE and the Joint Mechanism for Electoral Resilience facilitated information exchange and coordination on mitigation strategies for election-related cybersecurity threats.

Regarding information-related threats, the European Commission issued Guidelines on recommended measures for VLOPs and VLOSEs in April 2024, aimed at mitigating systemic online risks for electoral processes. Stress tests were also conducted with VLOPs and VLOSEs to assess their preparedness. Online platform providers reported measures taken under the Code of Practice to safeguard election integrity. Based on this experience, the Commission published an Elections Toolkit for Digital Services Coordinators in February 2025, providing guidance on applying the Guidelines during electoral periods.

Swift situational awareness was ensured through mechanisms such as the RAS, the IPCR arrangements, and a 'Tripartite' cooperation format involving the EP, the Commission, and the EEAS. Awareness-raising and media literacy initiatives also contributed to societal resilience, including efforts by EUvsDisinfo, the EP's dedicated election website and educational videos.

Sources: European Commission, *Recommendation (EU) 2023/2829 of 12 December 2023 on inclusive and resilient electoral processes in the Union and enhancing the European nature and efficient conduct of the elections to the European Parliament, Official Journal of the European Union*, L, 2023/2829, Part VII; European Commission, *Compendium of e-voting and other ICT practices. Non-Paper from the Commission services*, Publications Office of the European Union, Luxembourg, 2023; NIS Cooperation Group, *Compendium on Elections Cybersecurity and Resilience*, 6 March 2024; European Commission, *Report on the 2024 elections to the European Parliament*, *cit.*, p. 15; European External Action Service, *2024 Report on EEAS Activities to Counter Foreign Information Manipulation and Interference*, Policy Planning and Strategic Communication, August 2025, p. 7; European Commission, Guidelines for providers of VLOP and VLOSE on the mitigation of systemic risks for electoral processes, *Official Journal of the European Union*, C, 2024/3014, 26 April 2024

2.4. EU's External Action

As outlined in the fourth pillar of the FIMI Toolbox, the EU has invested heavily in its external action and diplomacy to build international partnerships aimed at countering FIMI and ensuring accountability. This commitment is explicitly reflected in the *Strategic Compass for Security and Defence*,[137] and reinforced by the *International Digital Strategy for the EU*, adopted in June 2025.[138]

Three main strands of work can be identified. First, on the unilateral front, the EU increasingly relies on restrictive measures as a key instrument to raise the costs for perpetrators – most notably in response to Russia's war of aggression against Ukraine. The topic will be examined in detail in Chapter 3.

Second, at the bilateral level, the EU's *Security and Defence Partnerships* (SDP) with eight countries include specific FIMI-related commitments.[139] As of September 2025, these non-binding agreements have been concluded with Moldova, Norway, Japan, Republic of Korea, North Macedonia, Albania, United Kingdom and Canada. Negotiations are under way with Australia and Iceland,[140] while Switzerland and India have entered exploratory talks.[141] Enhanced cooperation on security and defence, including FIMI, is also foreseen in the recent Joint Statement on *Strengthening EEA Foreign and Security Policy Cooperation*.[142] Table 3 summarises the main FIMI-related commitments in the eight SDPs signed to date.

[137] Council of the European Union, *A Strategic Compass for Security and Defence*, *cit.*, p. 22.

[138] European Commission and High Representative, *Joint Communication to the European Parliament and the Council. An International Digital Strategy for the European Union*, JOIN(2025) 140 final, Brussels, 5 June 2025, p. 10; European Commission and High Representative, *Annex to the Joint Communication to the European Parliament and the Council. An International Digital Strategy for the European Union*, JOIN(2025) 140 final ANNEX, Brussels, 5 June 2025, p. 9.

[139] SDPs are non-binding instruments (NBIs) that provide an enhanced framework for cooperation between the EU and selected third partners in peace, security and defence.

[140] Council of the European Union, "Europe and Australia commit to security and defence partnership", 17 June 2025. https://www.consilium.europa.eu/en/press/press-releases/2025/06/17/australia-and-the-european-union-committing-to-security-and-defence-partnership/; European Commission, "Statement by President von der Leyen with Icelandic Prime Minister Kristrún Frostadóttir", 17 July 2025. https://ec.europa.eu/commission/presscorner/detail/en/statement_25_1872.

[141] Swiss Federal Department of Foreign Affairs, "Security and defence partnership: Federal Council to seek exploratory talks with the EU", 25 June 2025. https://www.europa.eda.admin.ch/en/newnsb/sHxHxYhqwno7. On 16 September 2025, the Swiss National Council backed the government's engagement with the EU regarding a possible SDP. Cfr. Swissinfo, "Parliament in favour of Swiss defence partnership with EU", 16 September 2025. https://www.swissinfo.ch/eng/swiss-diplomacy/national-council-supports-federal-council-in-armaments-cooperation-with-eu/90009872; European Commission and High Representative, Joint Communication to the European Parliament and the Council on a New Strategic EU-India Agenda, JOIN(2025) 50 final, Brussels, 17 September 2025.

[142] Joint Statement between the Foreign Ministers of Iceland, Liechtenstein and Norway and the High Representative of the Union for Foreign Affairs and Security Policy on "Strengthening EEA Foreign and Security Policy Cooperation", Brussels, 21 May 2025, para. 5.

Table 3: Commitments on FIMI under the EU's SDPs

Commitments	Countries							
	MD	NO	KR	JP	MK	AL	UK	CA
Information sharing								
(*proactively*) ***share information*** **on threat assessments** (through bilateral exchanges)								
Further reinforce information sharing, including on FIMI threat analysis, reporting and best practices								
Operational cooperation								
Explore (the possibility for) operation cooperation								
Expand towards more structured, operational (and impactful) cooperation								
Coordination								
Explore the possibility for coordination								
Coordinate approaches and systems to detect, analyse and respond to FIMI								
Cooperation and joint action								
Keep developing ongoing bilateral (and multilateral) exchanges								
Strengthen cooperation in detecting and responding to FIMI through bilateral exchanges								
Continue close cooperation on collectively responding to FIMI in relevant international platforms and multilateral for a, including the G7								
Consider joint action against FIMI perpetrators, either bilaterally or via relevant multilateral mechanisms, such as the G7 Rapid Response Mechanism								
Support capacities of the third country's institutions to counter FIMI and to increase the resilience of the population								

Source: SDPs[143]

[143] EU and Moldova, Security and Defence Partnership between the European Union and the Republic of Moldova, 21 May 2024; EU and Norway, Security and Defence Partnership between the European Union and Norway, 28 May 2024; EU and Japan, Security and Defence Partnership between the European Union and Japan, 1 November 2024; EU and the Republic of Korea, Security and Defence Partnership between the European Union and the Republic of Korea, 4 November 2024; EU and North Macedonia, Security and Defence Partnership between the European Union and the Republic of North Macedonia, 19 November 2024; EU and Albania, Security and Defence Partnership between the European Union and the Republic of Albania, 18 December 2024; EU and United Kingdom, Security and Defence Partnership between the European Union and the Kingdom of Great Britain and Northern Ireland, 19 May 2025; EU and Canada, Security and Defence Partnership between the European Union and Canada, 23 June 2025.

In the coming years, effective implementation of these instruments will be crucial – and appears already underway. For example, under the relevant SDP, the EU–Japan dialogue on FIMI was launched in July 2025 to "share information on threat assessment, methodologies and responses regarding FIMI, and explore opportunities for further coordination and operational cooperation".[144]

These SDPs complement broader EU external action initiatives addressing FIMI. One notable example is the *Reform and Growth Facility* for the Republic of Moldova, adopted in March 2025. This facility provides €520 million in non-repayable support and up to €1.5 billion in loans from NDICI – Global Europe, targeting multiple objectives,[145] including efforts to "mitigate challenges posed by Russia's war of aggression against Ukraine and attempts to destabilise Moldova, fight disinformation, hybrid threats, and FIMI, in particular by Russia, against Moldova's sovereignty, democratic processes and institutions, as well as against the Union and its values".[146]

Cooperation with Ukraine has also intensified at both bilateral and multilateral levels. In June 2024, the EU signed *Joint Security Commitments* with Ukraine, setting out enhanced cooperation in resilience, cyber and hybrid threats, and FIMI.[147] Moreover, the EU became a founding member of the *Ukraine Communications Group*, a multilateral forum aimed at strengthening coordination to expose Russian disinformation.[148]

Before turning to multilateral cooperation, it is worth noting that FIMI-related cooperation with the United States has declined. In recent years, the EU-US Trade and Technology Council (TTC) served as the main forum for cooperation, including through Working Group 6 on the "Misuse of Technology Threatening Security and Human Rights". Within this framework, the EU and the US agreed to establish a *Cooperation Framework on Information Integrity on a Crisis* at the second TTC Ministerial meeting in Paris, and later announced plans for a "common standard for exchanging structured threat information on FIMI" and the launch of capacity-building initiatives, including in third countries.[149] However, no further Ministerial meetings have been held since the new US administration took office in January 2025, and press reports suggest Washington may be stepping back from joint efforts with European partners.[150]

Third and last, on the multilateral side, the G7 has become a key platform for FIMI-related information sharing and coordinated action. The G7 Rapid Response Mechanism (RRM), launched at the 2018

[144] European Commission, "Joint statement following the EU-Japan Summit 2025", 23 June 2025, Attachment I, point I.d. https://ec.europa.eu/commission/presscorner/detail/en/statement_25_1890

[145] Regulation (EU) 2025/535 of the European Parliament and of the Council of 18 March 2025 establishing the Reform and Growth Facility for the Republic of Moldova, *Official Journal of the European Union,* L, 2025/535, 21 March 2025, Art. 6(1).

[146] *Ibid*., Art. 3(1)(c).

[147] *Joint security commitments between the European Union and Ukraine*, 27 June 2024, para. 4.

[148] European External Action Service, *2024 Report on EEAS Activities*, *cit.*, p. 12.

[149] *EU-U.S. Joint Statement of the Trade and Technology Council*, Paris-Saclay, 16 May 2022, p. 30; *Joint Statement EU-US Trade and Technology Council*, Luleå, 31 May 2023, point E; *Foreign information manipulation and interference in third countries*, Annex to the Joint Statement, Luleå, 31 May 2023.

[150] Mackinnon, A., "US ends international push to combat fake news from hostile states", *Financial Times*, 8 September 2025. https://www.ft.com/content/d31b56e3-aca9-4ee7-af5a-abec74830455

Charlevoix Summit, aims to "strengthen coordination to identify and respond to diverse and evolving threats to our democracies, including through sharing information and analysis, and identify opportunities for coordinated response".[151] The RRM brings together focal points from all G7 members and the EU (represented by the EEAS), with Australia, New Zealand, the Netherlands, Sweden, and NATO participating as observers. Over time, the RRM has set priorities and created working groups on capacity building, collective response, AI-enabled information threats, open-source analytics, subnational interference, and transnational repression.[152]

The EU has played a leading role in these efforts. Under the EEAS leadership, the G7 RRM Collective Response Framework (CRF) was finalised in the late 2024, as mandated by the Apulia G7 Leaders' Communiqué.[153] The CRF outlines collective response options, including public-facing actions, and has already been applied – for example, in joint statements on Russian influence campaigns and Hong Kong arrest warrants.[154] Additionally, under the G7 Italian Presidency, a Task Force on Monitoring Elections was created to enhance information exchange on FIMI in electoral contexts, launching a pilot initiative during the June 2024 EP elections.[155]

In recent years, the EU and NATO have deepened cooperation in this field. The first EU-NATO Joint Declaration in 2016 identified strategic communications and countering hybrid threats – including resilience-building – as key areas for strengthening the partnership.[156] The third Joint Declaration (2023) expanded this framework to explicitly include FIMI.[157]

Concrete steps to operationalise these commitments include staff-to-staff exchanges (notably through the RAS), mutual support for public diplomacy, and increased cooperation with the NATO Strategic Communications and the Hybrid Centre of Excellence.[158] A major development on NATO's side was the adoption of its *Approach to Counter Information Threats* in October 2024. Building on the

---

[151] Global Affairs Canada, "Charlevoix commitment on defending democracy from foreign threats", 9 June 2018. https://www.international.gc.ca/world-monde/international_relations-relations_internationales/g7/documents/2018-06-09-defending_democracy-defense_democratie.aspx?lang=eng

[152] Global Affairs Canada, "G7 Rapid Response Mechanism Annual Report 2024", 17 June 2025. https://www.international.gc.ca/transparency-transparence/rapid-response-mechanism-mecanisme-reponse-rapide/2024-annual-report-rapport-annuel.aspx?lang=eng

[153] Italian G7 Presidency, *Apulia G7 Leaders' Communiqué*, 15 June 2025. https://www.g7italy.it/wp-content/uploads/Apulia-G7-Leaders-Communique.pdf

[154] Global Affairs Canada, "G7 Rapid Response Mechanism (RRM) statement on Russian Influence Campaign", 17 January 2025. https://www.canada.ca/en/global-affairs/news/2025/01/g7-rapid-response-mechanism-rrm-statement-on-russian-influence-campaign.html; Global Affairs Canada, "G7 Rapid Response Mechanism (RRM) Statement on Hong Kong Arrest Warrants", 8 August 2025. https://www.canada.ca/en/global-affairs/news/2025/08/g7-rapid-response-mechanism-rrm-statement-on-hong-kong-arrest-warrants.html

[155] Global Affairs Canada, "G7 Rapid Response Mechanism Annual Report 2024", 17 June 2025. https://www.international.gc.ca/transparency-transparence/rapid-response-mechanism-mecanisme-reponse-rapide/2024-annual-report-rapport-annuel.aspx?lang=eng

[156] NATO and EU, *Joint Declaration*, 8 July 2016.

[157] NATO and EU, *Joint Declaration on EU-NATO Cooperation*, 10 January 2023.

[158] NATO and EU, *Tenth progress report on the implementation of the common set of proposals endorsed by EU and NATO Councils on 6 December 2016 and 5 December 2017*, 10 June 2025, p. 5.

existing NATO's Information Environment Assessment (IEA) capability,[159] this approach rests on four pillars: (a) understanding and (b) preventing information threats, (c) containing and mitigating incidents and (d) recovering from information campaigns.[160]

Additionally, NATO established the Rapid Response Group (NRRG) in 2024 to monitor emerging information trends and share best practices.[161] Despite these advances, recent media reports suggest internal restructuring within NATO – possibly including the closure of the Public Diplomacy Division – raising uncertainty about the future trajectory of EU–NATO cooperation in this domain.[162]

In recent years, the Organization for Economic Co-Operation and Development (OECD) has launched several initiatives to address these challenges, primarily under the *Reinforcing Democracy Initiative* (RDI). Rooted in the 2021 and 2022 OECD Ministerial Council Statements and Members' long-term vision,[163] the RDI is structured around five pillars: (i) public governance to combat mis- and dis-information, (ii) enhancing representation, participation and openness in public life, (iii) strengthening resilience to foreign undue influence, (iv) governing green, and (v) transforming governance for digital democracy.[164] A key milestone was the adoption in November 2022 of the *Declaration on Building Trust and Reinforcing Democracy*, to which the EU also adhered. The Declaration welcomed the release of three OECD Action Plans, including one on combating mis- and disinformation;[165] the creation of the OECD Global Forum on Building Trust; and the launch of the OECD DIS/MIS Information Resource Hub, now evolved into the Hub on Information Integrity.[166]

Most notably, on 17 December 2024, the OECD adopted the *Recommendation on Information Integrity*,[167] building on the report *Facts not Fakes: Tackling Disinformation, Strengthening Information Integrity*.[168] While non-binding, OECD recommendations carry significant political weight. This

[159] NATO's IEA capability is composed of "people, process and technology to analyse the information environment and to provide actionable insights". Cf. NATO, *NATO's approach to counter information threats*, 18 October 2024, para. 12. https://www.nato.int/cps/en/natohq/official_texts_231905.htm

[160] *Ibid*., para. 21.

[161] Government of Canada, "G7 Rapid Response Mechanism Annual Report 2024", 17 June 2025. https://www.international.gc.ca/transparency-transparence/rapid-response-mechanism-mecanisme-reponse-rapide/2024-annual-report-rapport-annuel.aspx?lang=eng

[162] Starcevic, S., "Mark Rutte DOGEs NATO with dozens of job cuts", *Politico*, 19 June 2025. https://www.politico.eu/article/mark-rutte-doge-nato-staff-warn-cuts-us-ukraine-iran-defense-donald-trump-budget/; Schultz, T., "NATO ex-employees accuse the alliance of going DOGE", *Deutsche Welle*, 30 July 2025. https://www.dw.com/en/nato-ex-employees-accuse-the-alliance-of-going-doge/a-73442195

[163] OECD, *Building Trust and Reinforcing Democracy: Preparing the Ground for Government Action*, OECD Public Governance Reviews, OECD Publishing, Paris, 2022, p. 3.

[164] OECD, "Reinforcing Democracy Initiative". https://www.oecd.org/en/about/programmes/reinforcing-democracy-initiative.html

[165] OECD, *Action Plan on public governance for combating mis- and disinformation*, GOV/PGC(2022)27/REV1, 5 October 2022.

[166] OECD, *Declaration on Building Trust and Reinforcing Democracy*, OECD/LEGAL/0484, 18 November 2022.

[167] OECD, *Recommendation of the Council on Information Integrity*, OECD/LEGAL/0505, 17 December 2024.

[168] OECD, *Facts not Fakes: Tackling Disinformation, Strengthening Information Integrity*, 4 March 2024.

Recommendation sets out broad commitments to promote information integrity across multiple policy areas, including societal resilience, transparency, accountability, plurality of information sources, and institutional frameworks to uphold these principles.

In the European context, the Council of Europe (CoE) has increasingly addressed the challenges of disinformation, particularly its interaction with freedom of expression under the European Convention on Human Rights (ECHR). The Committee of Ministers has adopted several relevant recommendations, including on media pluralism and ownership transparency, the role of internet intermediaries, the human rights impact of algorithmic systems, quality journalism, and the effects of digital technologies on freedom of expression. Other CoE bodies, such as the Parliamentary Assembly (PACE) and the Venice Commission, have also been active. In April 2025, PACE adopted a *Resolution on Foreign interference: a threat to democratic security in Europe*, condemning such interference and recommending measures ranging from strengthening democratic institutions to promoting media literacy.[169] A landmark development came on 22 July 2025, when the European Court of Human Rights (ECtHR) issued its judgment in *Bradshaw and Others v. the United Kingdom*, clarifying obligations under Article 3 of Protocol No. 1 ("Right to free elections") in the context of Russian interference in UK democratic processes.[170]

As for EU-CoE cooperation, the EU priorities for 2025-2026 state that both organisations "will cooperate to counter foreign information manipulation and interference, including disinformation campaigns and distortion of history".[171] Building on the 2023 Reykjavík Declaration, the CoE has launched a process to establish a *New Democratic Pact for Europe*.[172] Structured around three pillars – (i) learning and practising democracy, (ii) protecting democracy from internal and external threats, including disinformation and (iii) innovating for democracy[173] – the process will culminate at the CoE Summit of Heads of State and Government in 2026.[174] In a recent speech, the Secretary General of the CoE Alain Berset has unveiled that "[t]he pact is already taking shape with a proposed convention on disinformation and foreign influence".[175]

At the international level, the United Nations (UN) has stepped up efforts to safeguard information integrity, particularly in the digital sphere, across its agencies and bodies. On 24 June 2024, the UN

[169] Parliamentary Assembly of the Council of Europe, *Foreign interference: a threat to democratic security in Europe*, Resolution 2593 (2025), 8 April 2025.

[170] European Court of Human Rights, *Bradshaw and Others V. The United Kingdom*, app. no. 15653/22, Judgement of 22 July 2025. https://hudoc.echr.coe.int/?i=001-244218

[171] Council of the European Union, *Council conclusions on EU priorities for cooperation with the Council of Europe in 2025-2026*, 17028/24, Brussels, 17 December 2024, para. 41.

[172] Council of Europe, *Reykjavík Declaration. United around our values*, 17 May 2023, para. 7.

[173] Council of Europe, *Roadmap Towards a New Democratic Pact for Europe. Building a resilient, inclusive and agile democracy*, SG/Inf(2025)14, 29 April 2025, pp. 3-4.

[174] Council of Europe, *The New Democratic Pact for Europe – What is it?*. https://rm.coe.int/2pager-new-democratic-pact-for-europe/1680b650f2

[175] Alain Berset. *Speech*, 25 September 2025. New York, Columbia University. https://worldleaders.columbia.edu/content/alain-berset-secretary-general-council-europe

Secretary-General launched the *UN Global Principles for Information Integrity*, providing "a holistic framework to guide multi-stakeholder action for a healthier information ecosystem".[176] Building on the UN Policy Brief 8 on information integrity on digital platforms, these principles focus on (i) societal trust and resilience, (ii) healthy incentives, (iii) public empowerment, (iv) independent, free, and pluralistic media, and (v) transparency and research.

The EU supports these principles. The 2025 Council Conclusions on EU priorities at the 80th UN General Assembly reaffirm the EU's support and its pledge to "work with partners towards a global strategy for countering foreign information manipulation and interference".[177] They also stress the EU and Member States' commitment to protecting democracy, including elections, from such threats. This shared commitment was also enshrined in the *Global Digital Compact*, adopted at the 2024 Summit of the Future, which calls for joint action to protect information integrity and democratic processes.[178] In parallel, the UN is addressing information integrity during electoral periods. In this context, the United Nations Development Programme (UNDP) leads an *Action Coalition on Information Integrity in Elections* to advance this work.[179] Beyond the Euro-Atlantic Area, the EU has intensified cooperation on strategic communication and countering FIMI in several regions, such as Latin America and Indo-Pacific partners.[180]

Any analysis of the EU's external action against FIMI must also consider its CSDP missions and operations. The civilian EU Partnership Mission in the Republic of Moldova (EUPM Moldova), established on 24 March 2023, is particularly relevant. Its mandate includes "enhancing the resilience of the security sector of the Republic of Moldova in the areas of crisis management and hybrid threats, including cybersecurity and countering foreign information manipulation and interference".[181] The mission has supported the setup of Strategic Communications and Countering Disinformation Centre and the development of methodologies for detecting and responding to disinformation.[182] In April–May 2025, the Hybrid Rapid Response Teams were also deployed to provide short-term targeted assistance.[183] Under the 2022 Strategic Compass, the EU committed to ensuring that "by 2024, all CSDP missions and operations will be fully equipped with capabilities and resources to deploy relevant instruments of this toolbox".[184] According to the *Common Foreign and Security Policy Report - Our*

[176] United Nations, *United Nations Global Principles for Information Integrity. Recommendations for Multi-stakeholder Action*, 2024, p. 5. https://www.un.org/sites/un2.un.org/files/un-global-principles-for-information-integrity-en.pdf

[177] Council of the European Union, *Council Conclusions on EU priorities at the United Nations during the 80th session of the United Nations General Assembly, September 2025 – September 2026*, 10491/25, Brussels, 23 June 2025, para. 34.

[178] United Nations, *Summit of the Future Outcome Documents. Pact for the Future, Global Digital Compact and Declaration on Future Generations*, September 2024, p. 45.

[179] Bentzen, N., *Information integrity online and the European democracy shield*, *cit*., December 2024, pp. 4-5.

[180] European External Action Service, *2024 Report on EEAS activities*, *cit*., p. 12.

[181] Council Decision (CFSP) 2023/855 of 24 April 2023 on a European Union Partnership Mission in Moldova (EUPM Moldova), *Official Journal of the European Union*, L 110, 25 April 2023, Art. 2(1).

[182] European External Action Service, *Our Priorities in 2025*, *cit*., p. 8.

[183] *Ibid*., p. 9.

[184] Council of the European Union, *A Strategic Compass for Security and Defence*, 7371/22, Brussels, 21 March 2022, p. 22.

priorities in 2025, this goal has been achieved. The report notes that, "[i]n addition to analytical support and dedicated trainings, the EEAS has strengthened strategic communications capabilities of CSDP missions and operations and started to provide dedicated support during crisis".[185]

[185] Council of the European Union, *Our priorities in 2025"*, 11306/25, Brussels, 9 July 2025, p. 36.

2.5. Countering FIMI and disinformation at the national level

While this Study focuses primarily on EU-level actions, it is equally important to consider measures adopted by Member States, which bear the "primary responsibility for countering FIMI, including in the context of broader hybrid campaigns", as noted in the July 2022 Council Conclusions on FIMI.[186] Reflecting their diverse organisational and constitutional cultures, EU Member States have adopted different institutional structures and policy approaches.[187]

First, several countries have published – or are developing – national strategies on disinformation. Ireland adopted a *National Counter Disinformation Strategy* in April 2025.[188] Italy's *2022-2026 National Cybersecurity Strategy* includes a commitment to coordinate national efforts against online disinformation,[189] while Spain has recently initiated work on a national strategy.[190]

Second, some Member States have established interministerial units to coordinate responses. Examples include Germany's Task Force on disinformation, operating within the interministerial working group on hybrid threats, and the Central Office for the Detection of Foreign Information Manipulation (ZEAM),[191] Denmark's Inter-Departmental Task Force to counter Foreign Influence,[192] Spain's National Commission against Disinformation,[193] and Czechia's Government Strategic Communications Coordinator.[194]

Third, some Member States have established dedicated agencies to address threats in the information space. Two notable examples are France and Sweden. In France, *the Vigilance and Protection Service against Foreign Digital Interference* (VIGINUM) was created in 2021 under the General Secretariat for Defence and National Security (SGDSN). VIGINUM is responsible for detecting and analysing foreign information manipulation that may affect national interests, particularly during election periods, by

[186] Council of the European Union, "Council conclusions on Foreign Information Manipulation and Interference (FIMI)", 11429/22, Brussels, 18 July 2022, para. 3.

[187] The analysis only focuses on the most significant developments, rather than providing a comprehensive review.

[188] Government of Ireland, *National Counter Disinformation Strategy*, Department of Tourism, Culture, Arts, Gaeltacht, Sport and Media, Dublin, 2025.

[189] Italian National Cybersecurity Agency, *Strategia nazionale di cybersicurezza*, Rome, 2022, p. 19.

[190] Orden PJC/248/2025, *Boletín Oficial del Estado*, 64, BOE-A-2025-5151, 13 March 2025.

[191] German Federal Ministry of the Interior, "Protecting the Bundestag elections from hybrid threats, including disinformation". https://www.bmi.bund.de/SharedDocs/faqs/EN/topics/disinformation/bt_wahl_2025/faq_liste.html; German Federal Ministry of the Interior, "Central Office for the Detection of Foreign Information Manipulation (ZEAM)". https://www.bmi.bund.de/SharedDocs/schwerpunkte/EN/disinformation-election/zeam-artikel-en.html

[192] Danish Ministry of Defence, "Strengthened safeguards against foreign influence on Danish elections and democracy", 7 September 2018. https://www.fmn.dk/en/news/english/strengthened-safeguards-against-foreign-influence-on-danish-elections-and-democracy/

[193] Orden PCM/1030/2020, *Boletín Oficial del Estado*, 292, 5 November 2020.

[194] Gongala, P., Fridrichovský, J. and Havránek, O., *Disinformation landscape in Czech Republic*, EU DisinfoLab, December 2020, p. 8.

monitoring publicly available online content.[195] It also supports SGDSN in coordinating interministerial responses, contributes to European and international initiatives, and ensures operational and technical coordination with foreign counterparts.[196] A recent development is the launch of "French Response", an X account managed by the Foreign Ministry to counter FIMI targeting France.

In Sweden, the *Psychological Defence Agency* was established in 2022 under the Ministry of Defence. Its mandate includes identifying, analysing, and supporting efforts to counter foreign malign influence and other misleading information targeting Sweden or its interests.[197] The agency also plays a preventive role by strengthening societal preparedness, fostering inter-agency cooperation, conducting training activities, and promoting research in its field.[198]

New platforms have also emerged to bolster societal resilience against disinformation and FIMI. For example, Poland created a *Council for Resilience*, bringing together 22 experts from NGOs and academia to facilitate cooperation between public authorities and civil society.[199]

Beyond the EU, in the United Kingdom a *Defending Democracy Taskforce* coordinates cross-government responses to threats to democracy.[200] Among other measures, the UK revoked Russia Today's broadcast licence in 2022 and imposed sanctions on social media platforms and individuals spreading disinformation about Russia's war of aggression against Ukraine.[201] Under UK law, social media services must take "reasonable steps" to prevent content dissemination by designated individuals.[202] The *Online Safety Act 2023* is a key instrument in this context, notably for classifying foreign interference as a priority offence and introducing media literacy provisions.[203] Some commentators have called for the creation of a National Disinformation Agency to ensure cognitive security.[204]

---

195 *Décret n° 2021-922 du 13 juillet 2021 portant création, auprès du secrétaire général de la défense et de la sécurité nationale, d'un service à compétence nationale dénommé « service de vigilance et de protection contre les ingérences numériques étrangères*, *Journal Officiel de la République Française*, 0162, 13 July 2021, Art. 3(1).

196 *Ibid*., Art. 3(2)-(4).

197 Förordning (2021:936) med instruktion för Myndigheten för psykologiskt försvar, *Svensk författningssamling*, 936, 15 October 2021, Art. 2(1).

198 *Ibid*., Art. 2(2)-(5).

199 Polish Ministry of Foreign Affairs, "Council for Resilience, joint initiative by MFA and civil society organisations against international disinformation, begins operation", 3 April 2025. https://www.gov.pl/web/diplomacy/council-for-resilience-joint-initiative-by-mfa-and-civil-society-organisations-against-international-disinformation-begins-operation

200 British Ministry of Housing, Communities and Local Government, "Restoring trust in our democracy: Our strategy for modern and secure elections", *Policy Paper*, 17 July 2025, para. 69.

201 Mills, C., "Sanctions against Russia (February 2022 to January 2025)", *Research briefing*, Number 9481, House of Commons Library, 21 January 2025, p. 35.

202 *Ibid*., p. 36.

203 Cfr. Library specialists, "Countering Russian influence in the UK", *Research briefing*, Number 9472, House of Commons Library, 13 March 2025, pp. 34-36.

204 Dixon, W., "Why the UK Now Needs a National Disinformation Agency", RUSI, 5 September 2025. https://www.rusi.org/explore-our-research/publications/commentary/why-uk-now-needs-national-disinformation-agency

3. THE WORK AHEAD

3.1. Concluding outstanding legislation

KEY FINDINGS

- Completing pending legislation is critical, notably the recast Regulation on European Political Parties, the Directive on Interest Representation on behalf of Third Countries, and the revised FDI screening framework.
- Implementation gaps undermine the effectiveness of existing legislation, such as the DSA, the EMFA, and the NIS2 Directive, requiring stronger enforcement and support for Member States.
- The EU has recently broadened the use of sanctions against hybrid threats, but enforcement inconsistencies and cross-border challenges limit their impact.
- The EU must invest in resilience through the next Multiannual Financial Framework, ensuring adequate funding for media literacy, cybersecurity, and critical infrastructure protection.

Protecting the EU and its Member States from foreign interference requires preventing foreign funding from undermining democratic processes or threatening critical infrastructure. In recent years, the EU has intensified efforts to close regulatory gaps in this area. The pending legislative proposals discussed in this section reflect this approach, and their adoption will be key to mitigating risks posed by foreign funding and investment.

On 25 November 2021, the European Commission proposed a *recast of the Regulation on European Political Parties and Political Foundations*,[205] as outlined in the EDAP. Among the issues that the recast regulation aims at addressing are the risk of foreign interference through foreign funding and participation in the Europarties' internal decision-making processes, as well as the need to ensure that their party members uphold EU values. After extensive negotiations, a provisional inter-institutional agreement was reached on 17 June 2025. The compromise permits Europarties to maintain institutional relationships with third country parties through an 'associate membership' status.[206] However, these associated parties cannot make financial contributions, have only limited decision-making powers and must respect EU values under Article 2 TEU.[207] Entities subject to sanctions are explicitly barred from joining.[208] The new rules also mandate European political parties and foundations to collect identifying

[205] European Commission, *Proposal for a Regulation of the European Parliament and of the Council on the statute and funding of European political parties and European political foundations (recast)*, COM(2021) 734 final, Brussels, 25 November 2021.

[206] Council of the European Union, *Proposal for a Regulation of the European Parliament and of the Council on the statute and funding of European political parties and European political foundations (recast) - Offer letter sent to the Chair of the European Parliament's Committee on Constitutional Affairs*, 11684/25, Brussels, 16 July 2025, Art. (2)(1a).

[207] *Ibid*., Arts. 3(1)(e) and 4(2a).

[208] *Ibid*., Art. 3(1)(ea).

information from donors contributing more than €3,000.[209] These measures reflect a broader trend toward tightening controls on foreign funding of European political parties and foundations.[210]

The proposed *Directive on Interest Representation on behalf of Third Countries* is intended to harmonise rules for interest representation services carried out in the internal market for remuneration and on behalf of a third country entity.[211] Notably, the rules would not apply to diplomatic or consular activities of third countries nor to entities that merely receive funding from abroad. A key feature of the proposal is the creation of one or more national registers for entities engaged in interest representation, to be established and created by the Member States.[212] Upon registration, each entity would be assigned a European interest representation number ('EIRN').[213] Discussions in the EP are ongoing within the IMCO Committee. In parallel, work continues in the Council, particularly in the Working Party on General Affairs.[214] Both the Polish and Danish Presidencies have listed this file among their priorities for their six-month terms.[215] Negotiations will need to address concerns raised by stakeholders, especially the potential risk of stigmatisation for entities receiving foreign funding. To mitigate this, stronger safeguards could be introduced – for instance, requiring public disclosure of foreign donations only above a certain threshold.[216]

Finally, the revision process of the *Foreign Direct Investment (FDI) Regulation* deserves close attention. Adopted on 24 January 2024 as part of the 'Economic security' package,[217] the proposal seeks to modernise the EU's framework for assessing and, where necessary, restricting FDIs that may threaten security or public order in the EU or its Member States.[218] Under the proposed rules, Member States would be required to establish national FDI screening mechanisms that comply with harmonised minimum standards.[219] This aims to ensure consistent implementation across the Union and prevent regulatory arbitrage. The sectoral scope of the regulation would also expand. In addition to investments

[209] *Ibid*., Art. 23(5).

[210] Bressanelli, E., *Towards a revision of the Regulation on the statute and funding of European political parties and foundations*, PE 729.741, Policy Department for Citizens' Rights and Constitutional Affairs, March 2022, pp. 43-45.

[211] European Commission, *Proposal for a Directive of the European Parliament and of the Council establishing harmonised requirements in the internal market on transparency of interest representation carried out on behalf of third countries and amending Directive (EU) 2019/1937*, COM(2023) 637 final, Strasbourg, 12 December 2023, Art. 1.

[212] European Commission, *Proposal for a Directive of the European Parliament and of the Council establishing harmonised requirements*, *cit*., Art. 9.

[213] *Ibid*., Art. 11.

[214] Council of the European Union, *Proposal for a Directive on Transparency of Interest Representation on behalf of Third Countries – Progress report*, 10134/25, Brussels, 16 June 2025.

[215] Polish Presidency of the Council, *Programme of the Polish Presidency of the Council of the European Union*, 2024, p. 10.

[216] Bressanelli, E. and Bernardi, S., *Resilience of Democracy*, *cit*., 50-53.

[217] 'Economic security' has become an important component of the broader security strategy of the Union.

[218] 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, *Official Journal of the European Union*, L 79I, 21 March 2019.

[219] European Commission, *Proposal for a Regulation of the European Parliament and of the Council on the screening of foreign investments in the Union and repealing Regulation (EU) 2019/452 of the European Parliament and of the Council*, COM(2024) 23 final, Brussels, 24 January 2024, Arts. 3-4.

linked to projects or programmes of Union interest, it would cover entities active in specific areas listed in Annex II, including ten critical technology sectors relevant to the EU's economic security.[220] The proposal would also extend to intra-EU investments involving foreign control.[221] Moreover, the criteria for assessing potential risks to public order or security would be updated. Notably, the assessment would include the possible impact on "online platforms that can be used for large-scale disinformation or criminal activities".[222] As regards the cooperation mechanism, the proposal foresees a stronger coordinating and decision-making role of the European Commission – a point questioned by the Council. The EP adopted its first reading position on 8 May 2025, while the Council endorsed its negotiating mandate on 11 June 2025. Interinstitutional negotiations began on 17 June 2025 and will need to strike a balance between safeguarding EU's security interests and maintaining openness to investment.

3.2. Monitoring enforcement and implementation

Before the end of the 2019-2024 legislative cycle, several important legislative dossiers were concluded. However, in some cases, the entry into force of significant provisions was postponed. Their transposition, implementation, and enforcement should now be pursued swiftly, and carefully assessed. According to the Commission's report on the 2024 EP elections, this is "essential".[223] Indeed, if implementation is lacking or delayed, key EU legislation will fail to produce tangible effects.

The following sections focus selectively on the implementation of key legislation aimed at strengthening resilience of the information space – the DSA and the EMFA – and enhancing the cybersecurity of critical sectors – the NIS2 Directive. This list is not exhaustive, but highlights some of the most pressing and, in various ways, challenging regulations.

The *DSA* was concluded in 2022 and its rules have fully applied since 17 February 2024. On 1 July 2025, the Code of Practice on Disinformation was incorporated in the regulation, thus becoming a "Code of Conduct", according to the DSA. Both the DSA and the Code of Practice have been affected by limited compliance and enforcement at the national level.[224]

Several Member States have delayed the implementation of the DSA, by failing to designate and/or empower their Digital Service Coordinator, (DSCs) overseeing the monitoring and the enforcement of the obligations of the DSA at the national level. The Commission sent letters of formal notice to the Czech Republic, Cyprus, Estonia, Poland, Portugal and Slovakia in April, and to Belgium, Croatia, Luxemburg, Netherlands, Spain and Sweden in July 2024. Reasoned opinions were subsequently sent

[220] *Ibid*., Art. 4(4) and Annex II. The critical technology areas are (i) advanced semiconductors technologies, (ii) artificial intelligence technologies, (iii) quantum technologies, (iv) biotechnologies, (v) advanced connectivity, navigation and digital technologies, (vi) advanced sensing technologies, (vii) space & propulsion technologies, (viii) energy technologies, (ix) robotics and autonomous systems, (x) advanced materials, manufacturing and recycling technologies.

[221] *Ibid*., Art. 2(1).

[222] *Ibid*., Art. 13(3)(e).

[223] European Commission. *Report on the 2024 Elections to the European Parliament*, *cit*., p. 21.

[224] European Parliament, *Working Document on Protecting European democracy and our* values, Special Committee on the Democratic Shield, 29 April 2025, pp. 4-5.

to the Czech Republic, Cyprus and Portugal in October, and to Belgium, Netherlands, Poland and Spain in December 2024. On 7 May 2025, the Commission decided to refer the Czech Republic, Spain, Cyprus, Portugal and Poland to the CJEU.[225] In addition, Member States are behind schedule in the appointment of "trusted flaggers" – organisations responsible for detecting potentially illegal content and alerting online platforms – with only thirteen of them having such entities in place.[226] Beyond delays, recent research also shows that the DSCs are often not sufficiently shielded from political interference, safeguards against 'revolving doors' are absent, and the involvement of civil society remains weak.[227]

The DSA puts forward specific measures for providers of Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs).[228] They are asked to assess at least yearly "systems risks" originating from the provision of their services and adopt mitigation measures. Twice a year, they should submit transparency reports. Overall, their compliance with the Code of Practice – and, prospectively, the DSA – is disappointing. According to a recent report by the EDMO, based on a triangulation of different sources (i.e., the platforms' own transparency reports, fact-checkers' independent assessments and a survey with stakeholders), the analysis of the actions of seven very large platforms or search engines – Meta (Facebook and Instagram), Google (Search and YouTube), Microsoft (Bing and LinkedIn) and TikTok – reveals a "consistent trend of partial implementation, with uneven progress across key areas". [229] The overall assessment is bleak, with the report stating that, in the absence of stronger enforcement, "the implementation of the Code risks remaining performative rather than impactful".[230]

Since the entry into force of the DSA, the Commission has sent several requests for information to most platforms and has started formal infringement proceedings against X, Tik Tok, Ali Express, Meta Platforms (Facebook and Instagram), Temu and platforms offering pornographic content. Platforms are variously accused of failing to effectively curb illegal content, deceptive advertising and political content, protect minors and provide data access to researchers.

Another issue concerns the methodology for determining the number of users – crucial to register providers of online services as "very large" and therefore make them subject to stricter obligations – particularly as it regards Telegram.[231] As part of the Digital Omnibus package, the Commission plans to

[225] Bulgaria received a letter of formal notice in December 2024 and a reasoned opinion in May 2025.

[226] Agence Europe, *Europe Daily Bulletin* No. 13676, point 15. See the updated list in European Commission, "Shaping Europe's Digital Future. The cooperation framework under the DSA", 9 July 2025. https://digital-strategy.ec.europa.eu/en/policies/trusted-flaggers-under-dsa

[227] Civil Liberties Union for Europe (Liberties), *Monitoring the implementation of the Digital Services Act. The independence of Digital Services Coordinators*, January 2025.

[228] According to Art. 33(1) of the DSA, VLOPs and VLOSEs have "a number of average monthly active recipients of the service in the Union equal to or higher than 45 million".

[229] Botan, M. and Meyer, T., *Implementing the EU Code of Practice on Disinformation. An evaluation of VLOPSE Compliance and Effectiveness (Jan – Jun 2024)*, European Digital Media Observatory, June 2025.

[230] *Ibid.*, p. 36.

[231] European Parliament, *Parliamentary question – E-001293/2025(ASW). Answer given by Executive Vice-President Virkkunen on behalf of the European Commission*, 19 May 2025.

release a report on the interplay of the DSA with a number of pieces of legislation.[232] Existing provisions mandate the Commission to issue this document and to evaluate and report on the application of Article 33 – laying down the designation thresholds and process for VLOPs and VLOSEs – by 17 November 2025.[233] According to press reports, more than 45 legislative texts are reportedly under assessment by the Commission in this process, including the GDPR, the AVMSD, the Regulation on the transparency and targeting of political advertising and the NIS2 Directive.[234] It is paramount that simplification efforts lead to targeted amendments and not to a broader de-regulation.

The *EMFA* was concluded in April 2024 and its rules fully apply as of 8 August 2025. It introduces minimum standards related to media freedom, pluralism and editorial independence, complementing the DSA and the Digital Markets Act (DMA). While its "full implementation" [235] is regarded as important to strengthen information integrity, concerns about national laws attempting to restrict media freedom and the editorial independence of public service media have been mounting.[236]

Based on the EMFA, the European Board for Media Services (the "Media Board") – an independent advisory body – was established in February 2025 to, among other things, support the consistent and effective implementation of the EMFA across the Union. The Media Board, in its input on the EDS, stressed the importance of "effective implementation of existing legislation across the Member States and industry players",[237] which requires sufficient powers, operational capabilities and resources for National Regulatory Authorities. Newly established collaboration mechanisms necessitate streamlined communication channels and the willingness by the actors to share experiences, best practices and knowledge about the implementation of the regulatory framework.

Speaking before the EP plenary, the European Commission confirmed that it "is working closely with the Member States to ensure that the implementation of EMFA is on track". The Commission also informed MEPs that earlier in the year it had sent a questionnaire to the Member States asking about national legislation and implementation efforts, followed by bilateral meetings. In the ensuing debate, MEPs signalled problems in several Member States, with national legislation (approved or being proposed) with provisions clashing with the EMFA.[238]

The *NIS2 Directive* was concluded in November 2022 and entered into force on 16 January 2023. Transposition by the Member States had to be ensured by 17 October 2024, but a "low level of

[232] European Parliament, *Committee on Civil Liberties, Justice and Home Affairs Ordinary meeting*, 22 September 2025.

[233] DSA, Art. 91(1).

[234] Agence Europe, Europe Daily Bulletin No. 13717, 26 September 2025.

[235] EUDS, *Working Document, cit.,* p. 5. A Working Group on the implementation of the EMFA, composed by members of the CULT committee, has been set up in January 2025.

[236] Pion, C., *As EMFA's implementation grows closer, why concerns over its effectiveness remain*, Analysis, Public Media Alliance, 27 February 2025.

[237] Media Board, *Input into the call for evidence on the European Democracy Shield*, 2025, p. 2.

[238] European Parliament, *State of play of implementation of the European Media Freedom Act in the Member States*, Plenary Debate, 2025/2785(RSP), 8 July 2025. See also Agence Europe, *Europe Daily Bulletin* No. 13676, *cit*., p. 4.

transposition" has been observed.[239] This has serious security implications, as the "cybersecurity threat level" is "substantial".[240] On 28 November 2024, the Commission opened infringement procedures by sending a letter of formal notice to 23 Member States (all Members except Belgium, Italy, Lithuania and Spain). In May 2025, the Commission followed it with reasoned opinions to 19 Member States (Greece, Malta, Romania and Slovakia had in the meanwhile transposed the directive). The delay in the transposition of the NIS2 Directive was further aggravated by the missing transposition of the Resilience of Critical Entities (CER) Directive. In this case, a letter of formal notice was sent to 24 Member States in late November. Among the key factors for the delays are the complexity of the transposition process, the need to adopt several cybersecurity policies at the same time, the significant impact on companies and domestic politics. According to stakeholders, significant variation in the implementation of the directive across Member States poses a challenge for transnational operators.[241]

3.3. Beyond legislation: Sanctions

The EU has recently broadened the use of restrictive measures to fight hybrid threats. In December 2024, the Council imposed – for the first time – sanctions on 16 individuals and 3 entities behind Russia's interferences abroad.[242] This followed the creation of a new horizontal sanctions framework in October 2024, targeting individuals and entities engaged in actions and policies attributable to the Government of the Russian Federation in order to destabilise the EU, its Member States and/or international partners. The sanctions regime covers a wide array of hybrid activities, including those undermining democratic processes, public order, safety, economic activities, and services of public interest or critical infrastructure – also through cyberattacks or sabotage.[243] Coordinated information manipulation and interference are explicitly sanctionable.[244]

On 20 May 2025, as part of the EU's 17th sanctions package against Russia, new listings were added, and the scope of the sanction regime was expanded. The updated provisions now allow targeting of tangible assets – such as vessels, aircraft, real estate, and elements of digital and communication networks – as well as financial institutions, crypto service providers, and entities offering technical or operational assistance linked to Russia's destabilising activities.[245] The Council also gained the power

[239] EUDS, *Working Document, cit.,* p. 8.

[240] ENISA, 2024 Report on the State of Cybersecurity in the Union, *cit.*, p. 7.

[241] European Cyber Security Organisation (ECSO), *NIS2 Implementation: Challenges and priorities*, January 2025, pp. 15–16.

[242] Council Implementing Regulation (EU) 2024/3188 of 16 December 2024 implementing Regulation (EU) 2024/2642 concerning restrictive measures in view of Russia's destabilizing activities, *Official journal of the European Union*, L, 2024/3188, 16 December 2024, Art. 1; Council Decision (CFSP) 2024/3174 of 16 December 2024 amending Decision (CFSP) 2024/2643 concerning restrictive measures in view of Russia's destabilising activities, *Official Journal of the European Union*, L, 2024/3174, 16 December 2024, Art. 1.

[243] Council Regulation (EU) 2024/2642 of 8 October 2024 concerning restrictive measures in view of Russia's destabilizing activities, *Official Journal of the European Union*, L, 2024/2642, 9 October 2024, Art. 2(3)(a)(i) and (v), as amended; Council Decision (CFSP) 2024/2643 of 8 October 2024 concerning restrictive measures in view of Russia's destabilising activities, *Official Journal of the European Union*, L, 2024/2643, 9 October 2024, Art. 1(a)(i) and (iv), as amended.

[244] Council Regulation (EU) 2024/2642, *cit.*, Art. 2(3)(a)(iv); Council Decision (CFSP) 2024/2643, *cit.*, Art. 1(a)(iv).

[245] Council Regulation (EU) 2025/964 of 20 May 2025 amending Regulation (EU) 2024/2642 concerning restrictive measures in view of Russia's destabilizing activities, *Official Journal of the European Union*, L, 2025/964, 20 May 2025, Art. 1(2);

to suspend broadcasting licences of media outlets controlled by Russian leadership listed in Annex IV, and prohibited the advertising of products or services in any content produced or broadcast by sanctioned entities.[246] In its Conclusions of 26 June 2025, the European Council welcomed "the adoption of additional listings [...] and the broadened scope of this regime", signalling strong political endorsement.[247] This appears to be a unique sanctions framework globally, although countries such as Canada and the UK have also sanctioned Russian actors involved in disinformation and hybrid activities.[248]

As of 26 September 2025, 47 individuals and 15 entities are listed under this sanctions framework (Annex I). However, no entries have yet been made in Annex II (tangible assets), Annex III (entities providing technical or operational assistance), or Annex IV (media outlets).[249] In line with standard EU practice, those listed in Annex I are subject to an asset freeze, a ban on providing funds or economic resources, and – when natural persons are concerned – a travel ban.[250] Notably, the current framework does not restrict the broadcasting or transmission of content attributable to listed individuals or entities within the EU, even when their designation cites involvement in coordinated information manipulation and interference.

Separately, on 28 April 2023, at the request of the Moldovan authorities, the Council adopted a dedicated sanctions framework to address Russia's destabilising activities in the country. As of 26 September 2025, 23 individuals and 5 legal entities are listed under this framework.[251] Compared to the broader regime, its scope is narrower, focusing mainly on undermining democratic processes, violent demonstrations, and serious financial misconduct in Moldova.[252] However, this does not pose a legal or practical obstacle, as the broader framework can address activities beyond the Moldova-specific regime. It may therefore be worth considering whether the latter should be integrated into the broader regime, given its wider applicability.

Council Decision (CFSP) 2025/963 of 20 May 2025 amending Decision (CFSP) 2024/2643 concerning restrictive measures in view of Russia's destabilising activities, *Official Journal of the European Union*, L, 2025/963, 20 May 2025, Art. 1(2).

246 *Ibid*.

247 European Council, *Conclusions*, EUCO 12/25, Brussels, 26 June 2025, p. 13.

248 Government of Canada, "Canadian Sanctions Related to Russia". https://www.international.gc.ca/world-monde/international_relations-relations_internationales/sanctions/russia-russie.aspx?lang=eng; Foreign, Commonwealth and Development Office, "UK sanctions Putin's interference actors", Press release, 28 October 2024. https://www.gov.uk/government/news/uk-sanctions-putins-interference-actors

249 In Regulation (EU) 2024/2642, Annexes II, III and IV are Annexes III, IV and V, respectively.

250 Council Regulation (EU) 2024/2642, *cit*., Arts. 1 and 2. Council Decision (CFSP) 2024/2643, *cit.*, Arts. 1 and 2.

251 Council Decision (CFSP) 2023/891 of 28 April 2023 concerning restrictive measures in view of actions destabilising the Republic of Moldova, *Official Journal of the European Union*, L, 114, 2 May 2023, Annex, as amended; Council Regulation (EU) 2023/888 of 28 April 2023 concerning restrictive measures in view of actions destabilising the Republic of Moldova, *Official Journal of the European Union*, L, 114, 2 May 2023, Annex I, as amended.

252 Council Decision (CFSP) 2023/891, *cit*., Art. 1(1), as amended; Council Regulation (EU) 2023/888, *cit*., Art. 2(3).

Another key element of the EU's sanctions toolkit is the so-called "broadcasting" ban targeting selected Russian media outlets.[253] In response to Russia's war of aggression against Ukraine, the Council amended Decision 2014/512/CFSP and Regulation (EU) 833/2014 to address Russia's "systematic, international campaign of media manipulation and distortion of facts", deemed a "significant and direct threat to the Union's public order and security".[254] These measures prohibit operators within the Union from broadcasting or contributing to broadcast content from designated media outlets under Russian state control, which also face suspension of their broadcasting licences within the EU.[255]

In June 2022, a further amendment introduced a ban on advertising "products or services in any content produced or broadcast" by the sanctioned entities,[256] mirroring provisions later included in the EU's hybrid sanctions regime. As with the Moldova-specific framework, it may be worth exploring synergies – or even integration – between the "broadcasting ban" and the broader regime.

The "broadcasting ban" was challenged before the General Court but was ultimately upheld.[257] As of 26 September 2025, these restrictions apply to 32 media outlets.[258] While some countries – such as the UK – have adopted similar measures, others – including Switzerland and Norway – have opted not to align with the EU's approach.

In addition, other EU sanctions regimes – particularly the one targeting actions undermining Ukraine's territorial integrity – have been used to counter foreign information manipulation and interference. For example, in July 2023, the Council sanctioned seven Russian individuals and five entities responsible for the "Recent Reliable News" campaign, which used fake websites and social media accounts to impersonate national media and government sources in support of Russia's war of aggression.[259]

---

253 *RT France v. Council*, Judgement of the General Court (Grand Chamber), T-125/22, 27 July 2022, ECLI:EU:T:2022:483, para. 68.

254 Council Regulation (EU) 2022/350 of 1 March 2022 amending Regulation (EU) No 833/2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine, *Official Journal of the European Union*, L 65, 2 March 2022, recitals 6 and 8; Council Decision (CFSP) 2022/351 of 1 March 2022 amending Decision 2014/512/CFSP concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine, *Official Journal of the European Union*, L 65, 2 March 2022, recitals 6 and 8.

255 Council Regulation (EU) 2022/350, *cit*., Art. 1(1); Council Decision (CFSP) 2022/351, *cit*., Art. 1(1).

256 Council Decision (CFSP) 2022/884 of 3 June 2022 amending Decision 2014/512/CFSP concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine, *Official Journal of the European Union*, L 153, 3 June 2022, Art. 1(10); Council Regulation (EU) 2022/879 of 3 June 2022 amending Regulation (EU) No 833/2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine, *Official Journal of the European Union*, L, 153, 3 June 2022, Art. 1(10).

257 RT France v. Council, cit; *A2B Connect BV and Others v Council*, Judgement of the General Court (First Chamber, extended composition), T-307/22, 26 March 2025, ECLI:EU:T:2025:331.

258 Regulation (EU) No 833/2014, Annex XV, as amended; Decision 2014/512/CFSP, Annex IX, as amended.

259 Council Implementing Regulation (EU) 2023/1563 of 28 July 2023 implementing Regulation (EU) No 269/2014 concerning restrictive measures in respect of actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine, *Official Journal of the European Union*, L, 190I, 28 July 2023, Art. 1; Council Decision (CFSP) 2023/1566 of 28 July 2023 amending Decision 2014/145/CFSP concerning restrictive measures in respect of actions

The EU's framework for restrictive measures against cyber-attacks, introduced in May 2019 under the Cyber Diplomacy Toolbox, remains a key component of its response to hybrid threats. Cyber-attacks are broadly defined to include (i) access to information systems, (ii) interference with systems or data, and (iii) data interception, posing threats to both the Union and its Member States.[260] The framework also recognises that such attacks may target (a) critical infrastructure, (b) essential services, (c) critical state functions, (d) classified information systems, or (e) government emergency response teams.[261] Restrictive measures can also be applied in response to cyber-attacks against third States or international organisations, where necessary to achieve CFSP objectives.[262] Currently, these measures apply to 17 individuals and four entities.[263] Similar regimes exist in other jurisdictions, including the US and the UK.

Implementation challenges can undermine the effectiveness of sanctions. For example, the enforcement of the "broadcasting ban" – introduced in the EU's third sanctions package and later extended to other outlets – involves national audiovisual regulators. Notably, in March 2022, the European Regulators Group for Audiovisual Services (ERGA) – now European Board for Digital Services (EBDS) – pledged to ensure "the swift and effective implementation".[264] Under the DSA, VLOPs and VLOSEs must also assess systemic risks, including the spread of illegal content, and adopt mitigation measures.[265]

However, enforcement remains uneven. A study by the Institute for Strategic Dialogue found inconsistent blocking of domains linked to sanctioned Russian media across major Internet Service Providers (ISPs) in six Member States, with circumvention possible via third-party resolvers.[266] While most official accounts of sanctioned outlets are restricted in the EU, posts linking to banned domains still circulate widely on platforms like X.[267] Research by Okholm, Ebrahimi Fard and ten Thij (2024) shows that geo-blocking reduced the sharing of Russian propaganda among fringe communities

undermining or threatening the territorial integrity, sovereignty and independence of Ukraine, *Official Journal of the European Union*, L, 190I, 28 July 2023, Art. 1.

[260] Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, *Official Journal of the European Union*, L, 129I, 17 May 2019, Art. 1(3), as amended; Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, *Official Journal of the European Union*, L, 129I, 17 May 2019, Art. 1(3), as amended.

[261] Council Regulation (EU) 2019/796, *cit.*, Art. 1(4); Council Decision (CFSP) 2019/797, *cit.*, Art. 1(4).

[262] Council Regulation (EU) 2019/796, *cit.*, Art. 1(5); Council Decision (CFSP) 2019/797, *cit.*, Art. 1(5).

[263] Council Regulation (EU) 2019/796, *cit.*, Annex I; Council Decision (CFSP) 2019/797, *cit.*, Annex.

[264] European Regulators Group for Audiovisual Services, "ERGA's united response to foreign disinformation and information manipulation: European media regulators strengthen their cooperation", *Press release*, 10 February 2022.

[265] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), *Official Journal of the European Union*, L, 277, 27 October 2022, Art. 34-35.

[266] Maristany de las Casas, P., "Investigation | Holding the line: Auditing the EU's ban of Russian state media 3 years on", *Institute for Strategic Studies*, 5 August 2025. https://www.isdglobal.org/digital_dispatches/investigation-holding-the-line-auditing-the-eus-ban-of-russian-state-media-3-years-on/

[267] *Ibid*.

without boosting other Russian content, but it did increase pro-Russian activity on alternative platforms.[268]

Cross-border challenges persist. For instance, a Swiss media outlet recently republished a German translation of an RT article. Since Switzerland has not aligned itself with the EU sanctions mentioned above, whether this violated EU rules could be debated. The case illustrates the difficulty of enforcing measures nationally against transnational issues.[269]

To address these gaps, experts suggest creating a comprehensive, regularly updated list of domains linked to sanctioned entities as a reference for national implementation, and using intergovernmental forums – such as RAS – to share information on these domains and their mirror versions. [270] The RAS and EBDS (Working Group 4) could also facilitate discussions on enforcement practices. Finally, timely transposition of Directive (EU) 2024/1226 on criminal offences and penalties for violating EU sanctions will be essential for harmonised enforcement across Member States.[271]

3.4. Investing Money for Democracy: The Multiannual Financial Framework

On 16 July 2025, the European Commission presented its proposal for the 2028-2034 Multiannual Financial Framework (MFF), complemented by seven sectoral legal acts on 3 September 2025.[272] While the final shape of MFF will depend on inter-institutional negotiations, analysing the proposed components is essential to assess how measures to counter FIMI and protect critical infrastructure could be financed during this period.

Within the proposed MFF, several instruments are relevant to countering FIMI. Chief among them is the *AgoraEU* programme, which builds on Creative Europe and Citizens, Equality, Rights and Values (CERV). With a total proposed budget of €8.5 billion,[273] AgoraEU is structured around three strands: "Creative Europe – Culture", "MEDIA+" and "Democracy, Citizens, Equality, Rights and Values" (CERV+).[274]

---

[268] Santos Okholm, C., Fard, A. E., ten Thij, M., "Blocking the information war? Testing the effectiveness of the EU's censorship of Russian state propaganda among the fringe communities of Western Europe", *Internet Policy Review*, Vol. 13, No. 3 (2024), p. 1.

[269] Gyimesi, B., *Defending Democracy: Sanctions on Disinformation*, Royal United Services Institute, 12 June 2025.

[270] Maristany de las Casas, P., "Investigation | Holding the line: Auditing the EU's ban of Russian state media 3 years on", *cit*.

[271] Directive (EU) 2024/1226 of the European Parliament and of the Council of 24 April 2024 on the definition of criminal offences and penalties for the violation of Union restrictive measures and amending Directive (EU) 2018/1673, *Official Journal of the European Union*, L, 2024/1226, 29 April 2024.

[272] European Commission, "An ambitious budget for a stronger Europe: 2028-2034", *Press release*, 16 July 2025. https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1847; European Commission, "Commission completes proposal for the 2028-2034 EU long-term budget", *Press release*, 3 September 2025. https://ec.europa.eu/commission/presscorner/detail/en/ip_25_2011

[273] Figures in this paragraph are in current prices and refer to the total financial allocation, unless otherwise specified.

[274] European Commission, *Proposal for a Regulation of the European Parliament and of the Council establishing the 'AgoraEU' programme for the period 2028-2034, and repealing Regulations (EU) 2021/692 and (EU) 2021/818*, COM(2025) 550 final, Brussels, 16 July 2025, Arts. 3 and 11(1).

Under the "MEDIA+" strand (€3.194 billion), the "News" objective is expected to support actions such as monitoring and safeguarding the online information space, detecting and combating disinformation and FIMI, protecting news media and journalists, and promoting digital and media literacy. [275] The "CERV+" strand (€3.593 billion) includes a specific objective on "democratic participation and rule of law", aimed at fostering citizen engagement and ensuring free, fair, and resilient electoral processes.[276] More broadly, AgoraEU identifies the "protection of the integrity of public discourse, bolstering democratic resilience, societal preparedness, and civic engagement" as a cross-cutting priority.[277]

Other instruments in the proposed MFF are also relevant. Under Pillar II "Competitiveness and Society", the *Horizon Europe* programme (proposed budget: €7.6 billion) will support bottom-up research to "strengthen democratic values and foundations [...] by fostering resilient, pluralistic societies, and the integrity of the information and media space, while countering polarisation, disinformation, hate speech, discrimination, and xenophobia".[278] The *Erasmus+* programme (€40.8 billion) will contribute to societal resilience and democratic participation by equipping citizens with key skills and competences.[279] In addition, the draft *European Fund for economic, social and territorial cohesion, agriculture and rural, fisheries and maritime, prosperity and security* includes among its general objectives the protection and the strengthening of "fundamental rights, democracy, the rule of law", including through media pluralism and information integrity.[280] Finally, the *Justice* programme (€0.8 billion) aims to support the consistent and effective implementation of relevant EU legal instruments, explicitly referencing the DSA.[281]

For cybersecurity and critical infrastructure protection, the proposed *European Competitiveness Fund* will be a key financing instrument. Its objectives include developing cross-border and critical infrastructure in energy, transport, digital, security, defence, space, and related data and services.[282]

---

[275] *Ibid*., Art. 6(a), (d) and (e).

[276] *Ibid*., Art. 9 (a) and (b).

[277] *Ibid*., Art. 10(a).

[278] European Commission, *Proposal for a Council Decision on establishing the Specific Programme implementing Horizon Europe – the Framework Programme for Research and Innovation for the period 2028-2034, laying down the rules for participation and dissemination under that Programme, and repealing Decision (EU) 2021/764, COM(2025) 544 final*, Brussels, 16 July 2025, Art. 11(b)(i), first indent.

[279] European Commission, *Proposal for a Regulation of the European Parliament and of the Council establishing the Erasmus+ programme for the period 2028-2034, and repealing Regulations (EU) 2021/817 and (EU) 2021/888*, 16 July 2025, p. 2 and Art. 9.

[280] European Commission, *Proposal for a Regulation of the European Parliament and of the Council establishing the European Fund for economic, social and territorial cohesion, agriculture and rural, fisheries and maritime, prosperity and security for the period 2028-2034 and amending Regulation (EU) 2023/955 and Regulation (EU, Euratom) 2024/2509*, COM(2025) 565 final, Brussels, 16 July 2025, Art. 3(e)(II).

[281] European Commission, *Regulation of the European Parliament and of the Council establishing the Justice programme for the period 2028-2034 and repealing Regulation (EU) 2021/693*, COM(2025) 463 final, Brussels, 3 September 2025, p. 5 and Art. 3(2)(b).

[282] European Commission, *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, repealing provisions of*

With a total budget of approximately €51.5 billion, the "Digital Leadership" policy window will support Europe's digital sector through measures such as "ensuring a high level of cybersecurity in the Union" and securing critical infrastructures and digital supply chains. [283] The "Resilience and Security, Defence Industry and Space" window (€125.2 billion) will strengthen supply chain resilience and civil industrial security, including for critical and dual-use infrastructures.[284] These allocations will be complemented by *Horizon Europe* top-ups of €16.8 billion and €6.4 billion, respectively.[285]

Additional support will come from the *Connecting Europe Facility, national and partnership plans,* and *the Union Civil Protection Mechanism*.[286] Furthermore, the *Union support for internal security* will strengthen "the Union's and Member States' capabilities in relation to preventing and combating serious and organised crime [...] and hybrid threats" as well as enhance resilience of critical entities against hostile acts and improve the management of security-related incidents, risks, and crises, including through interoperable critical communication systems. [287] The financial envelope for this instrument amounts to €6.843 billion.[288]

Another relevant component of the proposed MFF is the *Global Europe* programme. Under its "Europe" pillar (€43.174 billion), one specific objective regarding cooperation with candidate and potential candidate countries focuses on "enhancing capacities for strategic communication [...] while addressing foreign information manipulation and interference and disinformation".[289] Within the broader goal of building "mutually beneficial partnerships with the Union's partners," this pillar also aims to mitigate challenges posed by Russia's war of aggression and destabilisation attempts, fight disinformation, hybrid threats, and FIMI – particularly by Russia – and reduce strategic dependencies of both the Union and partner countries.[290] References to combating FIMI, hybrid, and cyber threats also appear under the "Middle East, North Africa and the Gulf" pillar (€42.934 billion). Additionally, the "Global" pillar will fund measures to address "threats to democracy, including foreign information manipulation and interference and disinformation", support free and independent media, and tackle global threats such

Regulations (EU) 2021/696, (EU) 2023/588, and amending Regulation (EU) [EDIP], COM(2025) 555 final, Brussels, 16 July 2025, Art. 3(1)(f).

283 European Commission, *Proposal for a Regulation of the European Parliament and of the Council on establishing the European Competitiveness Fund ('ECF')*, COM(2025) 555 final, Brussels, 16 July 2025, Art. 39(3).

284 *Ibid*., Art. 3(2)(d).

285 European Commission, European Commission, *Proposal for a Regulation of the European Parliament and of the Council establishing Horizon Europe, cit*., Art. 6(5)(b).

286 European Commission, *Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions. A dynamic EU Budget for the priorities of the future – The Multiannual Financial Framework 2028-2034*, COM(2025) 570 final, Brussels, 16 July 2025, pp. 10, 19.

287 European Commission, *Proposal for a Regulation of the European Parliament and of the Council establishing the Union support for internal security for the period from 2028 to 2034*, COM(2025) 542 final, Brussels, 16 July 2025, Art. 3(1)(a) and (b).

288 *Ibid*., Art. 4(1).

289 European Commission, *Proposal for a Regulation of the European Parliament and of the Council establishing Global Europe*, COM(2025) 551 final, Brussels, 16 July 2025, Annex II.A(1)(j).

290 *Ibid*., Annex II.A(2)(g) and (t).

as hybrid, space, and cyber risks, while promoting maritime and aviation security. Improving the productive and export capacity of critical raw materials is a recurring priority across all regions.[291]

As these examples show, funding relevant to the priorities likely to feature in the forthcoming EDS is dispersed across multiple instruments. It is therefore essential that interinstitutional negotiations ensure that these work strands are backed by adequate financing in the next MFF.

[291] *Ibid*., Annex II.B(2)(e) and (3)(b), Annex II.F(3)(c) and (4)(b).

4. RECOMMENDATIONS

General matters

1. The objective of protecting democracy cuts across multiple policy areas and often involves **trade-offs**. While legislation may curb foreign interference, it can also unintentionally make democratic engagement harder. **Safeguards** should ensure that protecting democracy does not come at the expense of participation and civic involvement.[292]
2. The horizontal and cross-cutting nature of policy initiatives to protect democracy requires effective **coordination both within, across and beyond EU institutions**. Initiatives such as the Commissioners' Project Group on Democracy and the EP's **Special Committee on the EDS** are steps in the right direction. The **six-months extension** of the latter's mandate **is welcome** to complete pending work. In the medium term, the EP should consider establishing a permanent committee or sub-committee to continue exercising parliamentary oversight and influence the EU's agenda, building on the experience gathered through the INGE, ING2 and EUDS Special Committees.
3. The rapidly changing geopolitical context poses major challenges. Learning from past crises, such as Brexit, **the EU should avoid allowing its regulatory framework to be cherry picked or moulded by third country pressures**. For instance, while the DSA may require adjustments to remain fit for the purpose, the EU should not bow to pressure from third countries to deregulate social platforms or dilute its provisions.
4. Over the past decade, the EU has expanded the number of structures involved in protecting EU democracy. The EDS offers an opportunity to **clarify mandates and streamline governance**. **New structures** should only be created where they provide a clear added value compared to the existing institutional setup.

The EU Agenda on Democratic Protection

5. The 'shield' should protect EU democracy from external hybrid threats while also addressing internal democratic challenges. It should therefore combine both an **outward-looking** and an **inward-looking dimension.**
6. Every five years, the EU should issue a **Hybrid Strategy** alongside a Cybersecurity Strategy. Building on previous action plans, this strategy should cover the full spectrum of hybrid threats – including FIMI and disinformation – and be accompanied by an action plan with concrete measures,

[292] The trade-off is well illustrated by the reform of the regulation on Europarties (cf. also above). They are mainly funded through the EU budget, but they also receive contributions (from members) and donations. While the current regulation prohibits donations from abroad, member political parties from 'third countries' have financially contributed to their budgets. Following a ruling of the General Court in 2020, membership from third country parties was no longer possible. Such a ban, however, undermines the democratic and political role that the Europarties could play in accession and candidate countries.

timelines, and financial resources. This process should align with the revision of the Strategic Compass, informed by the new threat analysis due in 2025.

Elections, disinformation and FIMI

7. To improve information sharing and situational awareness – especially given advances in generative AI – the EU should continue refining its **methodology** for identifying, tracking and exposing FIMI incidents, building on existing efforts.
8. Develop an **EU FIMI Protocol** to define actors, roles and processes for responding to FIMI, calibrated through the existing FIMI Toolbox. This would complement the EU Playbook for Hybrid Threats and the Hybrid Toolbox, as well as the Critical Infrastructure Blueprint.
9. Establish an **EU FIMI Reserve**, inspired by the EU Cybersecurity Reserve under the EU Cyber Solidarity Act. This reserve should consist of trusted managed security service providers to enhance situational awareness before, during, and after major events.
10. Continue strengthening the EU external action on FIMI at both bilateral and multilateral levels. Selected EU Delegations could host dedicated "**Hybrid" or "FIMI" attachés** to deepen engagement with international partners.
11. Building on the existing **Tripartite** format – a high-level dialogue between the Commission, the EP, and the EEAS on electoral resilience – expand participation to include the rotating Council Presidency, ENISA, and other relevant entities as needed. This would improve coordination, risk management, and proactive measures ahead of European elections.

Societal resilience, preparedness and media literacy

12. The EU should consider establishing a **pan-European e-learning initiative on digital and media literacy**, specifically targeting young people. The programme should build on existing guidelines and material and be a joint effort between the EU Institutions and Member States. It could be developed as a Massive Online Open Course (MOOC), which could be easily shared in educational settings. Accordingly, it should be translated in all EU official languages. Appropriate funding for this initiative should be envisaged under the next MFF.
13. The European architecture for ensuring information integrity has recently been enriched by national agencies specifically dedicated to ensuring protection against foreign digital interference – such as the Psychological Defence Agency in Sweden or VIGINUM in France. In this logic, **institutional developments in other Member States should be encouraged**, with the aim of further improving – also in cooperation with other structures already existing at national level – situational awareness, responses to FIMI incidents and their effectiveness.

Critical infrastructure and cybersecurity

14. **Electoral infrastructure** should be treated as "critical" in the *EU acquis* – formally included among the critical entities under the CER Directive and explicitly covered as essential/important entities under the NIS2 Directive.

Citizens' participation and civil society's engagement

15. The "whole of society" approach is commendable and should be pursued further. Yet, a thorough assessment and review of the impact of the **key initiatives of deliberative democracy to enhance citizens' involvement** should be made. Such initiatives **should not become a bureaucratic exercise or, worse, a form of "citizen washing"**.[293]

Implementation

16. The toolbox to protect democracy has massively expanded in the last decade, but **relevant legislation still must be properly implemented**. The case of the DSA, the EMFA and the NIS2 Directive are among the most prominent. To minimise delays and enhance the consistency of the EU regulatory framework, **the Commission should provide full support to the Member States**. In turn, formal proceedings should start without delays against laggards in case of non-compliance.

Funding

17. The EP should ensure that, under the current MFF, adequate financial resources are allocated to support the priorities outlined in the EDS. Furthermore, in the context of ongoing negotiations for the **2028-2034 MFF**, clear and dedicated budget lines should be established to fund the various work strands aimed at strengthening the resilience of EU democracy.

[293] As the former ombudsman warned: "I know that public consultations are a frequent source of frustration [...] this tool has risked becoming a tick-box exercise, a task to be completed by officials [...] the basic reflex suggests a bureaucratic mind-set that prizes process over genuine conversation". O'Reilly, E., *Speech at the event "Unmasking citizenwashing: the dos and don'ts of participation*", 14 November 2023.

REFERENCES

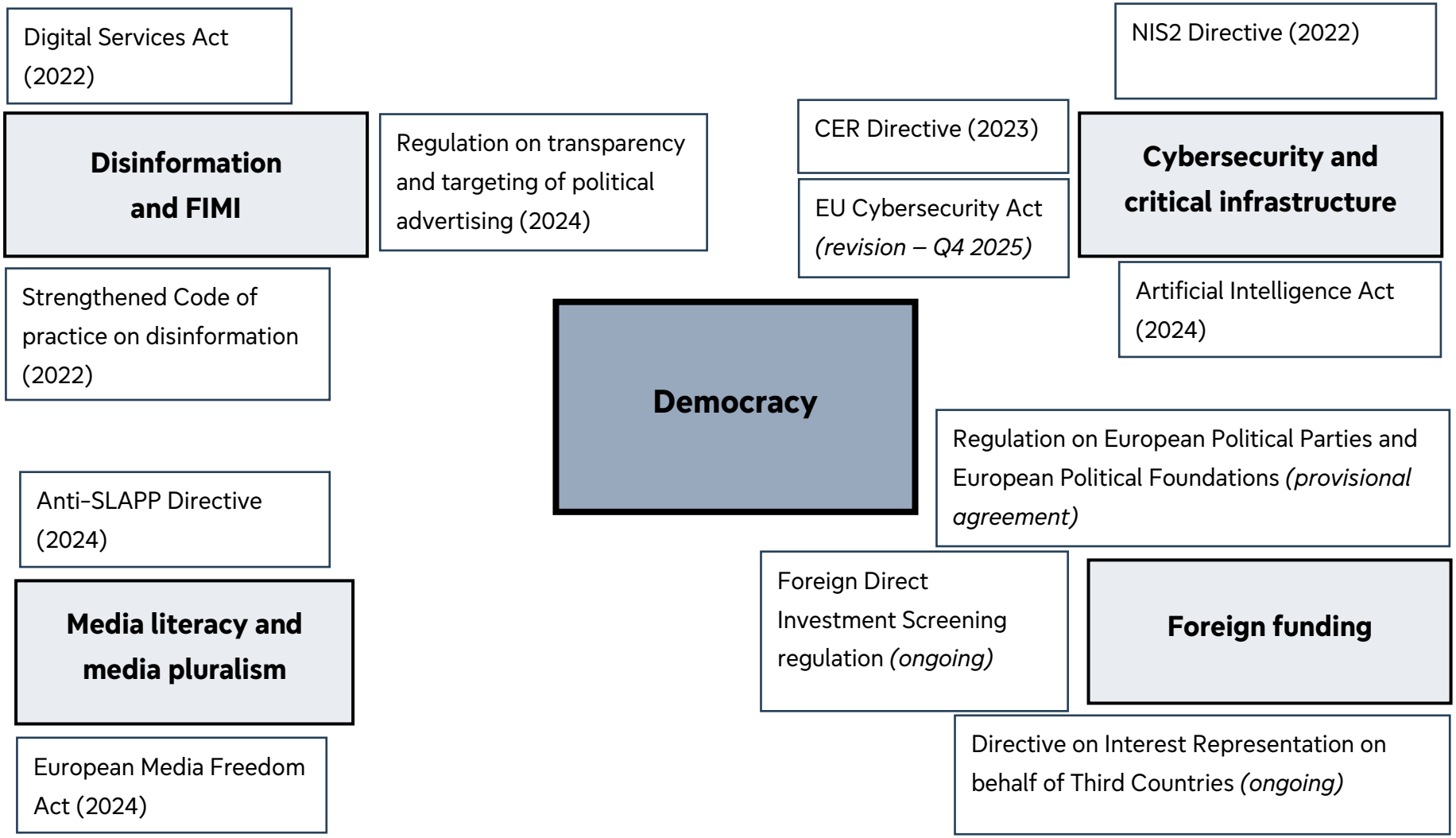
- Alliance for Security Democracy (ASD), *Authoritarian Interference Tracker,* German Marshall Fund of the United States. https://securingdemocracy.gmfus.org/toolbox/authoritarian-interference-tracker/?fwp_date_range=2024-01-01%2C2025-06-19
- Bentzen, N., *Information integrity online and the European democracy shield*, PE 767.153, European Parliamentary Research Service, Brussels, 2024.
- Borràs, J*., Disinformation in enlargement countries: Sowing instability, Distorting EU's perception*, CIDOB Briefing, Barcelona, December 2024.
- Botan, M. and Meyer, T., *Implementing the EU Code of Practice on Disinformation. An evaluation of VLOPSE Compliance and Effectiveness (Jan – Jun 2024)*, European Digital Media Observatory, June 2025.
- Bressanelli, E., *Towards a revision of the Regulation on the statute and funding of European political parties and foundations*, PE 729.741, Policy Department for Citizens' Rights and Constitutional Affairs, March 2022.
- Bressanelli, E. and Bernardi, S., *Resilience of Democracy and European Elections against New Challenges*, PE 761.471, Policy Department for Citizens' Rights and Constitutional Affairs, Brussels, April 2024.
- Bressanelli, E. and Natali, D., "Tested by the polycrisis? Reforming or Transforming the EU?", *Politics and Governance*, Vol. 11, No. 4 (2023), 246-251. doi.org/10.17645/pag.v11i4.7894.
- Brownlee, J. and Miao, K., "Why democracies survive", *Journal of Democracy*, Vol. 33, No. 4 (2022), 133-149.
- Bryant, M. and Rankin, J., "Talks on European 'drone wall' after Danish airport intrusions", *The Guardian*, 25 September 2025. https://www.theguardian.com/world/2025/sep/25/drones-aalborg-airport-denmark-closed-days-after-copenhagen-oslo
- Casero-Ripollés, A., Alonso-Muñoz, L., and Moret-Soler, D., "Spreading false content in political campaigns: Disinformation in the 2024 European Parliament elections", *Media and Communication*, Vol. 13 (2025), 1-20. doi.org/10.17645/mac.9525.
- Civil Liberties Union for Europe (Liberties), *Monitoring the implementation of the Digital Services Act. The independence of Digital Services Coordinators*, January 2025.
- Dixon, W., "Why the UK Now Needs a National Disinformation Agency", RUSI, 5 September 2025. https://www.rusi.org/explore-our-research/publications/commentary/why-uk-now-needs-national-disinformation-agency
- Economist Intelligence Unit (EIU), Democracy Index 2024. What's wrong with representative democracy?, 2025.
- European Digital Media Observatory, *Final Report – Outputs and outcomes of a community-wide effort,* 2025.

- European Fact Checking Standards Network, Elections24Check, database.
- Freedom House, *Freedom in the World 2025. The Uphill Battle to Safeguard Rights*, February 2025.
- Gongala, P., Fridrichovský, J. and Havránek, O., *Disinformation landscape in Czech Republic*, EU DisinfoLab, December 2020.
- Gyimesi, B., *Defending Democracy: Sanctions on Disinformation*, Royal United Services Institute, 12 June 2025.
- Gwyn Jones, M., "Online disinformation intensifies ahead of Moldovan parliamentary elections", *Euronews*, 3 September 2025. https://www.euronews.com/my-europe/2025/09/03/online-disinformation-intensifies-ahead-of-moldovan-parliamentary-elections
- Hallahan, K., Holtzhausen, D., van Ruler, B., Verčič, D. and Sriramesh K., "Defining Strategic Communication", *International Journal of Strategic Communication*, vol. 1, no. 1 (2007), 3–35. doi.org/10.1080/15531180701285244.
- International IDEA, *Review of the 2024 super-cycle year of elections. Trends, challenges and opportunities*, Stockholm, June 2025.
- International IDEA, *The Global State of Democracy Report 2025. Democracy on the Move*, September 2025.
- Institute for Strategic Dialogue, *Monitoring Influence and Disinformation Campaigns in the Western Balkans* (MEDIWEB), Berlin, 18 December 2024.
- Library specialists, "Countering Russian influence in the UK", *Research briefing*, Number 9472, House of Commons Library, 13 March 2025.
- Kops, M., Schittenhelm, C. and Wachs, S., "Young people and false information: A scoping review of responses, influential factors, consequences, and prevention programs", *Computers in Human Behavior*, Vol. 169 (2025). doi.org/10.1016/j.chb.2025.108650.
- Kovalčíková, N., De Agostini, L. and Catena, B., *Strengthening Resilience in the East*, Brief 15, European Union Institute for Security Studies, Paris, April 2025.
- Mackinnon, A., "US ends international push to combat fake news from hostile states", *Financial Times*, 8 September 2025. https://www.ft.com/content/d31b56e3-aca9-4ee7-af5a-abec74830455
- Maristany de las Casas, P., "Investigation | Holding the line: Auditing the EU's ban of Russian state media 3 years on", *Institute for Strategic Studies*, 5 August 2025. https://www.isdglobal.org/digital_dispatches/investigation-holding-the-line-auditing-the-eus-ban-of-russian-state-media-3-years-on/
- Marta, E., Damia-Martinez, S. and Riva, G. (eds), Alfabetizzazione digitale e fake news, Istituto Toniolo, Osservatorio giovani, 2025.
- Mills, C., "Sanctions against Russia (February 2022 to January 2025)", *Research briefing*, Number 9481, House of Commons Library, 21 January 2025.

- Media Board, *Input into the call for evidence on the European Democracy Shield*, 2025.
- Olari, V., Calmis, D. and Gigitashvili. G., "Malign interference in Moldova ahead of presidential elections and European referendum", DFRLab, 18 October 2024. https://dfrlab.org/2024/10/18/malign-interference-moldova/
- Our Rule of Law, *Our Democracy Report*, September 2025.
- Pion, C., *As EMFA's implementation grows closer, why concerns over its effectiveness remain*, Analysis, Public Media Alliance, 27 February 2025.
- Plattner, M. F., "Is Democracy in decline?", *Journal of Democracy*, Vol. 26, No. 1 (2015), 5–10.
- Radu, R., "TikTok, Telegram and Trust: Urgent Lessons from Romania's Election", *TechPolicy.Press*, 25 June 2025. https://www.techpolicy.press/tiktok-telegram-and-trust-urgent-lessons-from-romanias-election/
- Santos Okholm, C., Fard, A. E., ten Thij, M., "Blocking the information war? Testing the effectiveness of the EU's censorship of Russian state propaganda among the fringe communities of Western Europe", *Internet Policy Review*, Vol. 13, No. 3 (2024), 1–21. doi.org/10.14763/2024.3.1788.
- Schultz, T., "NATO ex-employees accuse the alliance of going DOGE", *Deutsche Welle*, 30 July 2025. https://www.dw.com/en/nato-ex-employees-accuse-the-alliance-of-going-doge/a-73442195
- Starcevic, S., "Mark Rutte DOGEs NATO with dozens of job cuts", *Politico*, 19 June 2025. https://www.politico.eu/article/mark-rutte-doge-nato-staff-warn-cuts-us-ukraine-iran-defense-donald-trump-budget/
- The Insider, "Russian bots from the "Matryoshka" network target EU summit in Moldova with fake videos impersonating The Insider and other media", 24 June 2025. https://theins.ru/en/news/282450
- Tui Stiftung and YouGov Institute, *Jugendstudie 2025*, Berlin, 3 July 2025.
- Varieties of Democracy (V-Dem), *Democracy Report 2025. 25 Years of Autocratization – Democracy Trumped?*, University of Gothenburg, V-Dem Institute, March 2025.
- Waldner, D. and Lust, E., "Unwelcome Change: Coming to Terms with Democratic Backsliding", *Annual Review of Political Science*, Vol. 21 (2018), 93–113. doi.org/10.1146/annurev-polisci-050517-114628.
- World Economic Forum, The Global Risks Report 2025. 20th edition, Cologny/Geneva, January 2025.
- Youngs, R., Riedl, R. B., McCoy, J., Roberts, K., Friesen, P., Cheeseman, N., Cianetti, L., Carothers, T., Carrier, M., D'Alessandra, F., Leininger, J., Lindberg, S. I., Godfrey, K., Way, L. A., "A New Dynamic of Democratic Resilience?", Carnegie Europe, European Democracy Hub, 29 April 2025. https://europeandemocracyhub.epd.eu/a-new-dynamic-of-democratic-resilience/
- Zakaria, F., "The Rise of Illiberal Democracy", *Foreign Affairs*, Vol. 76, No. 6 (1997), 22–43.

ANNEX

Mapping key legislation on the protection of democracy



This study reviews the current framework to protect democracy in the EU in view of the forthcoming European Democracy Shield. It provides a comprehensive map of the existing instruments, while identifying and assessing outstanding policy challenges, regulatory gaps and implementation issues. The study also formulates recommendations to strengthen democratic resilience.

The study was commissioned by the European Parliament's Policy Department for Justice, Civil Liberties and Institutional Affairs at the request of the EUDS Special Committee.

PE 777.917
IUST/2025/B/EUDS/IC/015

Print ISBN 978-92-848-3055-8| doi: 10.2861/ 8422610 | QA-01-25-213-EN-C
PDF ISBN 978-92-848-3054-1 | doi: 10.2861/ 0943148 | QA-01-25-213-EN-N