European Parliament
2024-2029

Special committee on the European Democracy Shield

2025/2069(INI)

18.12.2025

DRAFT REPORT

on the findings and recommendations of the Special Committee on the European Democracy Shield
(2025/2069(INI))

Special Committee on the European Democracy Shield

Rapporteur: Tomas Tobé

CONTENTS

Page

MOTION FOR A EUROPEAN PARLIAMENT RESOLUTION

on the findings and recommendations of the Special Committee on the European Democracy Shield

(2025/2069(INI))

The European Parliament,

– having regard to its decision of 18 December 2024 on setting up a special committee on the European Democracy Shield, and defining its responsibilities, numerical strength and term of office[1],

– having regard to the joint communication from the Commission and the High Representative of the Union for Foreign Affairs and Security Policy of 12 November 2025 entitled 'European Democracy Shield: Empowering Strong and Resilient Democracies' (JOIN(2025)0791),

– having regard to the Treaty on European Union (TEU), and in particular to Article 2 thereof on the EU's founding values, Article 10 thereof on democratic life and Article 21 thereof on external action,

– having regard to the Treaty on the Functioning of the European Union, and in particular to Article 114 thereof on the internal market and Article 222 thereof on solidarity,

– having regard to the Charter of Fundamental Rights of the European Union,

– having regard to Regulation (EU, Euratom) 2025/2445 of the European Parliament and of the Council of 26 November 2025 on the statute and funding of European political parties and European political foundations[2],

– having regard to 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)[3],

– having regard to Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing[4],

– having regard to Regulation (EU) 2024/1083 of the European Parliament and of the Council of 11 April 2024 establishing a common framework for media services in the

[1] OJ C, C/2025/1981, 11.4.2025, ELI: http://data.europa.eu/eli/C/2025/1981/oj.
[2] OJ L, 2025/2445, 8.12.2025, ELI: http://data.europa.eu/eli/reg/2025/2445/oj.
[3] OJ L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj.
[4] OJ L, 2024/1624, 19.6.2024, ELI: http://data.europa.eu/eli/reg/2024/1624/oj.

internal market and amending Directive 2010/13/EU (European Media Freedom Act)[5],

– having regard to Directive (EU) 2024/1069 of the European Parliament and of the Council of 11 April 2024 on protecting persons who engage in public participation from manifestly unfounded claims or abusive court proceedings ('Strategic lawsuits against public participation')[6],

– having regard to Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on the transparency and targeting of political advertising[7],

– having regard to 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[8],

– having regard to Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937[9] (Markets in Crypto-Assets Regulation),

– having regard to 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[10],

– having regard to 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)[11],

– having regard to 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)[12] and to Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act)[13],

– having regard to Regulation (EU) 2021/692 of the European Parliament and of the Council of 28 April 2021 establishing the Citizens, Equality, Rights and Values Programme and repealing Regulation (EU) No 1381/2013 of the European Parliament and of the Council and Council Regulation (EU) No 390/2014[14],

---

[5] OJ L, 2024/1083, 17.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1083/oj.
[6] OJ L, 2024/1069, 16.4.2024, ELI: http://data.europa.eu/eli/dir/2024/1069/oj.
[7] OJ L, 2024/900, 20.3.2024, ELI: http://data.europa.eu/eli/reg/2024/900/oj.
[8] OJ L, 2023/2841, 18.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2841/oj.
[9] OJ L 150, 9.6.2023, p. 40, ELI: http://data.europa.eu/eli/reg/2023/1114/oj.
[10] OJ L 333, 27.12.2022, p. 164, ELI: http://data.europa.eu/eli/dir/2022/2557/oj.
[11] OJ L 333, 27.12.2022, p. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj.
[12] OJ L 277, 27.10.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/2065/oj.
[13] OJ L 265, 12.10.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/1925/oj.
[14] OJ L 156, 5.5.2021, p. 1, ELI: http://data.europa.eu/eli/reg/2021/692/oj.

– having regard to Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law[15],

– having regard to Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive)[16],

– having regard to Council Decision 2014/145/CFSP of 17 March 2014 concerning restrictive measures in respect of actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine[17], and to Council Regulation (EU) No 269/2014 of 17 March 2014 concerning restrictive measures in respect of actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine[18],

– having regard to Council Decision 2014/119/CFSP of 5 March 2014 concerning restrictive measures directed against certain persons, entities and bodies in view of the situation in Ukraine[19], and to Council Regulation (EU) No 208/2014 of 5 March 2014 concerning restrictive measures directed against certain persons, entities and bodies in view of the situation in Ukraine[20],

– having regard to Council Decision 2014/512/CFSP of 31 July 2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine[21], and to Council Regulation (EU) No 833/2014 of 31 July 2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine[22],

– having regard to Council Decision (CFSP) 2022/266 of 23 February 2022 concerning restrictive measures in response to the recognition of the non-government controlled areas of the Donetsk and Luhansk oblasts of Ukraine and the ordering of Russian armed forces into those areas[23], and to Council Regulation (EU) 2022/263 of 23 February 2022 concerning restrictive measures in response to the recognition of the non-government controlled areas of the Donetsk and Luhansk oblasts of Ukraine and the ordering of Russian armed forces into those areas[24],

– having regard to Council Decision 2012/642/CFSP of 15 October 2012 concerning restrictive measures against Belarus[25], and to Council Regulation (EC) No 765/2006 of

---

[15] OJ L 305, 26.11.2019, p. 17, ELI: http://data.europa.eu/eli/dir/2019/1937/oj.
[16] OJ L 95, 15.4.2010, p. 1, ELI: http://data.europa.eu/eli/dir/2010/13/oj.
[17] OJ L 78, 17.3.2014, p. 16, ELI: http://data.europa.eu/eli/dec/2014/145(1)/oj.
[18] OJ L 78, 17.3.2014, p. 6, ELI: http://data.europa.eu/eli/reg/2014/269/oj.
[19] OJ L 66, 6.3.2014, p. 26, ELI: http://data.europa.eu/eli/dec/2014/119(1)/oj.
[20] OJ L 66, 6.3.2014, p. 1, ELI: http://data.europa.eu/eli/reg/2014/208/oj.
[21] OJ L 229, 31.7.2014, p. 13, ELI: http://data.europa.eu/eli/dec/2014/512/oj.
[22] OJ L 229, 31.7.2014, p. 1, ELI: http://data.europa.eu/eli/reg/2014/833/oj.
[23] OJ L 42 I, 23.2.2022, p. 109, ELI: http://data.europa.eu/eli/dec/2022/266/oj.
[24] OJ L 42 I, 23.2.2022, p. 77, ELI: http://data.europa.eu/eli/reg/2022/263/oj.
[25] OJ L 285, 17.10.2012, p. 1, ELI: http://data.europa.eu/eli/dec/2012/642/oj.

18 May 2006 concerning restrictive measures against President Lukashenko and certain officials of Belarus[26],

– having regard to Council Decision (CFSP) 2023/1532 of 20 July 2023 concerning restrictive measures in view of Iran's military support to Russia's war of aggression against Ukraine[27], and to Council Regulation (EU) 2023/1529 of 20 July 2023 concerning restrictive measures in view of Iran's military support of Russia's war of aggression against Ukraine[28],

– having regard to Council Decision (CFSP) 2024/1603 of 31 May 2024 amending Decision (CFSP) 2016/849 concerning restrictive measures against the Democratic People's Republic of Korea[29], and to Council Implementing Regulation (EU) 2024/1602 of 31 May 2024 implementing Regulation (EU) 2017/1509 concerning restrictive measures against the Democratic People's Republic of Korea[30],

– having regard to the Commission proposal of 16 July 2025 for a Council regulation laying down the multiannual financial framework for the years 2028 to 2034 (COM(2025)0571),

– having regard to the amendments adopted by the European Parliament on 27 November 2025 on the 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)0637 – C9-0464/2023 – 2023/0463(COD))[31],

– having regard to its resolution of 9 October 2025 on a united response to recent Russian violations of the EU Member States' airspace and critical infrastructure[32],

– having regard to its resolution of 18 June 2025 on the Commission's 2024 Rule of Law Report[33],

– having regard to its resolution of 7 May 2025 on a revamped long-term budget for the Union in a changing world[34],

– having regard to its resolution of 13 July 2023 on recommendations for reform of European Parliament's rules on transparency, integrity, accountability and anti-corruption[35],

– having regard to its resolution of 1 June 2023 on foreign interference in all democratic processes in the European Union, including disinformation[36],

---

[26] OJ L 134, 20.5.2006, p. 1, ELI: http://data.europa.eu/eli/reg/2006/765/oj.
[27] OJ L 186, 25.7.2023, p. 20, ELI: http://data.europa.eu/eli/dec/2023/1532/oj.
[28] OJ L 186, 25.7.2023, p. 1, ELI: http://data.europa.eu/eli/reg/2023/1529/oj.
[29] OJ L, 2024/1603, 31.5.2024, ELI: http://data.europa.eu/eli/dec/2024/1603/oj.
[30] OJ L, 2024/1602, 31.5.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/1602/oj.
[31] Texts adopted, P10_TA(2025)0306.
[32] Texts adopted, P10_TA(2025)0230.
[33] OJ C, C/2025/6259, 19.12.2025, ELI: http://data.europa.eu/eli/C/2025/6259/oj.
[34] Texts adopted, P10_TA(2025)0090.
[35] OJ C, C/2024/4011, 17.7.2024, ELI: http://data.europa.eu/eli/C/2024/4011/oj.
[36] OJ C, C/2023/1226, 21.12.2023, ELI: http://data.europa.eu/eli/C/2023/1226/oj.

– having regard to its resolution of 15 December 2022 on suspicions of corruption from Qatar and the broader need for transparency and accountability in the European institutions[37],

– having regard to its resolution of 23 November 2022 on recognising the Russian Federation as a state sponsor of terrorism[38],

– having regard to its resolution of 9 March 2022 on foreign interference in all democratic processes in the European Union, including disinformation[39],

– having regard to its resolution of 8 March 2022 on the shrinking space for civil society in Europe[40],

– having regard to its resolution of 20 October 2021 on Europe's Media in the Digital Decade: an Action Plan to Support Recovery and Transformation[41],

– having regard to its resolution of 23 November 2016 on EU strategic communication to counteract propaganda against it by third parties[42],

– having regard to its 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[43],

– having regard to its recommendation of 23 November 2022 to the Council, the Commission and the Vice-President of the Commission / High Representative of the Union for Foreign Affairs and Security Policy concerning the new EU strategy for enlargement[44],

– having regard to its recommendation of 13 March 2019 to the Council and the Vice-President of the Commission / High Representative of the Union for Foreign Affairs and Security Policy concerning taking stock of the follow-up taken by the EEAS two years after the European Parliament report on EU strategic communication to counteract propaganda against it by third parties[45],

– having regard to the Commission's follow-up to Parliament's recommendations in its resolutions,

– having regard to the Commission communication of 12 November 2025 entitled 'EU Strategy for Civil Society' (COM(2025)0790),

---

[37] OJ C 177, 17.5.2023, p 109.
[38] OJ C 167, 11.5.2023, p. 18.
[39] OJ C 347, 9.9.2022, p. 61.
[40] OJ C 347, 9.9.2022, p. 2.
[41] OJ C 184, 5.5.2022, p. 71.
[42] OJ C 224, 27.6.2018, p. 58.
[43] OJ C, C/2024/494, 23.1.2024, ELI: http://data.europa.eu/eli/C/2024/494/oj.
[44] OJ C 167, 11.5.2023, p. 105.
[45] OJ C 23, 21.1.2021, p. 152.

– having regard to the Commission communication of 1 April 2025 on ProtectEU: a European Internal Security Strategy (COM(2025)0148),

– having regard to the Commission communication of 24 July 2024 entitled ‘2024 Rule of Law Report – The rule of law situation in the European Union’ (COM(2024)0800),

– having regard to the Commission communication of 8 July 2025 entitled ‘2025 Rule of Law Report – The rule of law situation in the European Union’ (COM(2025)0900),

– having regard to the Commission communication of 12 December 2023 on Defence of Democracy (COM(2023)0630),

– having regard to the Commission communication of 3 December 2020 on the European democracy action plan (COM(2020)0790),

– having regard to the joint communications from the Commission and the High Representative of the Union for Foreign Affairs and Security Policy of 5 December 2018 entitled ‘Action Plan against Disinformation’ (JOIN(2018)0036) and of 14 June 2019 entitled ‘Report on the implementation of the Action Plan Against Disinformation’ (JOIN(2019)0012),

– having regard to the Security and Defence Partnership between the European Union and the United Kingdom of Great Britain and Northern Ireland, established on 19 May 2025,

– having regard to the political guidelines for the 2024-2029 Commission term, presented by Commission President Ursula von der Leyen on 18 July 2024, entitled ‘Europe’s Choice’,

– having regard to the Commission Implementing Decision of 28 March 2025 on the financing of the Digital Europe Programme and the adoption of the multiannual work programme 2025-2027 (C(2025)1839),

– having regard to the Code of Conduct on Disinformation,

– having regard to the report by the Network and Information Systems Cooperation Group of 23 January 2020 entitled ‘Cybersecurity of 5G networks – EU Toolbox of risk mitigating measures’,

– having regard to the report of 30 October 2024 by Sauli Niinistö, former President of the Republic of Finland, in his capacity as Special Adviser to the President of the European Commission, entitled ‘Safer Together – Strengthening Europe’s Civilian and Military Preparedness and Readiness’,

– having regard to 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[46],

[46] OJ L, 2023/2829, 20.12.2023, ELI: http://data.europa.eu/eli/reco/2023/2829/oj.

– having regard to 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[47],

– having regard to the establishment of the European Cooperation Network on Elections (ECNE) in 2019 by the Commission,

– having regard to the Commission press release of 13 November 2025 on its opening of an investigation into a potential Digital Markets Act breach by Google in demoting media publishers' content in search results,

– having regard to the Council conclusions of 21 May 2024 on the Future of Cybersecurity: implement and protect together,

– having regard to the Council conclusions of 17 October 2022 on ICT supply chain security,

– having regard to the Council Recommendation of 8 December 2022 on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure[48],

– having regard to Council Decision (CFSP) 2023/855 of 24 April 2023 on a European Union Partnership Mission in Moldova (EUPM Moldova)[49],

– having regard to the action plan entitled 'Strategic Compass for Security and Defence – For a European Union that protects its citizens, values and interests and contributes to international peace and security', approved by the Council on 21 March 2022 and endorsed by the European Council on 25 March 2022,

– having regard to the information from Lithuania, Denmark, Estonia, Finland, Germany, Latvia, Slovenia and Spain for the meeting of the Transport, Telecommunications and Energy Council on 6 June 2025 calling for common actions in response to Global Satellite Navigation Systems (GNSS) jamming and spoofing threats,

– having regard to the Interinstitutional Agreement of 20 May 2021 between the European Parliament, the Council of the European Union and the European Commission on a mandatory transparency register[50],

– having regard to special report 05/2022 of the European Court of Auditors of 29 March 2022 entitled 'Cybersecurity of EU institutions, bodies and agencies – Level of preparedness overall not commensurate with the threats',

– having regard to the UN Global Principles for Information Integrity – Recommendations for Multi-stakeholder Action, published on 24 June 2024,

– having regard to the International Covenant on Civil and Political Rights, in particular Article 20 thereof,

[47] OJ L, 2023/2836, 20.12.2023, ELI: http://data.europa.eu/eli/reco/2023/2836/oj.
[48] OJ C 20, 20.1.2023, p. 1.
[49] OJ L 110, 25.4.2023, p. 30, ELI: http://data.europa.eu/eli/dec/2023/855/oj.
[50] OJ L 207, 11.6.2021, p. 1, ELI: http://data.europa.eu/eli/agree_interinstit/2021/611/oj.

– having regard to the UN Convention on the Law of the Sea of 10 December 1982, which entered into force on 16 November 1994,

– having regard to the Articles on Responsibility of States for Internationally Wrongful Acts, adopted in November 2001,

– having regard to the Reykjavik Declaration, adopted at the 4th Summit of Heads of State and Government of the Council of Europe, held from 16 to 17 May 2023,

– having regard to the G7 Rapid Response Mechanism, established at the G7 Summit in Charlevoix, held from 8 to 9 June 2018,

– having regard to the working paper presented on 13 June 2025 to the International Civil Aviation Organization by Estonia, Finland, Latvia, Lithuania, Poland and Sweden on the recurring GNSS radio frequency interference in the Baltic, eastern and northern European regions and its implications on the safety and security of international civil aviation,

– having regard to the report on the final outcome of the Conference on the Future of Europe, published on 9 May 2022, and, in particular, to proposals 27 and 37 thereof,

– having regard to the study requested by Parliament's Special Committee on the European Democracy Shield entitled 'Strengthening Resilience – Towards the European Democracy Shield', published by its Directorate-General for Citizens' Rights, Justice and Institutional Affairs in October 2025[51],

– having regard to the 1st, 2nd and 3rd reports by the European External Action Service (EEAS) on Foreign Information Manipulation and Interference Threats,

– having regard to the report by the European Union Agency for Cybersecurity (ENISA) of 1 October 2025 entitled 'ENISA Threat Landscape 2025',

– having regard to the report by Europol entitled 'EU Serious and Organised Crime Threat Assessment – The changing DNA of serious and organised crime', published in 2025,

– having regard to the report of the Dutch data protection authority's Department for the Coordination of Algorithmic Oversight of October 2025 entitled 'AI chatbots as voting aid',

– having regard to the measures adopted by Italy's communications regulatory authority (AGCOM) on 3 September 2025 regarding influencers,

– having regard to the Code of Conduct for Influencer Advertising, adopted by AUTOCONTROL in Spain on 7 July 2025,

– having regard to the warning issued by Czechia's National Cyber and Information Security Agency (NÚKIB) on 3 September 2025 regarding cybersecurity threats

[51] Study – 'Strengthening Resilience – Towards the European Democracy Shield', European Parliament, Directorate-General for Citizens' Rights, Justice and Institutional Affairs, Policy Department for Justice, Civil Liberties and Institutional Affairs, October 2025.

associated with the transfer of data to and remote administration from the People's Republic of China and its special administrative regions,

– having regard to the report entitled 'Manipulation d'algorithmes et instrumentalisation d'influenceurs: enseignements de l'élection présidentielle en Roumanie & risques pour la France', published by the French Government's Service for Vigilance and Protection against Foreign Digital Interference (VIGINUM) in February 2025,

– having regard to the Influencer Handbook, produced by Finland's Mediapooli in 2020,

– having regard to the report by the US Department of State of August 2020 entitled 'Pillars of Russia's Disinformation and Propaganda Ecosystem',

– having regard to the joint cybersecurity advisory by the US Cybersecurity and Infrastructure Security Agency, the US National Security Agency, the FBI and international partners of August 2025 entitled 'Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage Systems',

– having regard to the report by Reporters Without Borders of 25 September 2025 entitled 'The Propaganda Monitor: The Russian Edition',

– having regard to the article published by the Centre for Media Pluralism and Media Freedom at the having regard to the article published by the Centre for Media Pluralism and Media Freedom at the European University Institute on 1 November 2025 entitled 'Influencers as news creators: implications for media regulation',

– having regard to the article published by the AlgoSoc Consortium on 28 October 2025 entitled '1 in 10 Dutch citizens are likely to ask AI for election advice. This is why they shouldn't',

– having regard to the report by What to Fix of June 2025 entitled 'Bankrolling Sanctioned Entities: How Meta Platforms Ireland Ltd. May Have Violated EU Sanctions and Channeled Money To RT, Sputnik and Other EU-Sanctioned Entities via Facebook's Revenue Redistribution Programs',

– having regard to the special report by NewsGuard of 6 March 2025 entitled 'A Well-funded Moscow-based Global "News" Network has Infected Western Artificial Intelligence with Russian Propaganda',

– having regard to the report by Media Freedom Rapid Response entitled 'Mapping Media Freedom – Monitoring Report 2024', published in February 2025,

– having regard to the report by the World Economic Forum of January 2025 entitled 'Global Cybersecurity Outlook 2025',

– having regard to the investigative report published by VSquare, Delfi Estonia and partner media organisations on 26 February 2024 entitled 'Kremlin Leaks: Secret Files Reveal How Putin Pre-Rigged his Reelection',

– having regard to the Ethical Code of Conduct for Social Media Influencers and Content Creators, published by the Aspen Institute Germany in 2024,

– having regard to the article published by Debunk.org on 4 May 2023 entitled ‘Kremlin spent 1.9 billion USD on propaganda last year, the budget exceeded by a quarter’,

– having regard to the statement by the Russian Federation’s Ministry of Foreign Affairs of 28 December 2024 on measures in response to the EU’s 15th sanctions package against Russia, in which it announced the expansion of the list of EU officials and citizens prohibited from entering the country,

– having regard to the article by the Russian News Agency TASS of 28 December 2024 entitled ‘Russia substantially expands blacklist of EU officials in response to sanctions – MFA’,

– having regard to the statement by TikTok of December 2024 on continuing to protect the integrity of TikTok during Romanian elections,

– having regard to the statement issued by the European Solar Manufacturing Council on 30 April 2025 entitled ‘Restrict Remote Access of PV Inverters from High-Risk Vendors’, in which it warned of the risks to Europe’s energy sovereignty due to unregulated and remote-control capabilities of PV inverters from high-risk, non-European manufacturers,

– having regard to Rule 55 of its Rules of Procedure,

– having regard to the report of the Special Committee on the European Democracy Shield (A10-0000/2025),

A. whereas on 12 November 2025, the Commission and the High Representative of the Union for Foreign Affairs and Security Policy presented a joint communication on the establishment of the European Democracy Shield, setting out a series of measures to empower, protect and promote strong and resilient democracies across the EU;

B. whereas the European Centre for Democratic Resilience constitutes the centrepiece of the European Democracy Shield; whereas both Parliament’s Special Committees on Foreign Interference in all Democratic Processes in the European Union, including Disinformation (INGE and INGE 2), had already called for the establishment of an EU structure to counter foreign information manipulation and interference (FIMI);

C. whereas recent EEAS reports on FIMI threats demonstrate an increasingly granular understanding of malicious actor methodologies, technical infrastructure and intended narratives, yet this situational awareness has not been translated into sustained operational mechanisms that enable the EU to take timely, coordinated countermeasures; whereas the EU’s institutional nexus is a principal focus of hostile information manipulation campaigns; whereas the EU is suffering from a fragmented approach to countering FIMI and disinformation, with significant variations in Member States’ capacities and no overarching strategic framework linking operational response to threat intelligence;

D. whereas the ECNE, the Rapid Alert System (RAS) and the European Digital Media Observatory (EDMO) are valuable components of the EU’s overall resilience to FIMI and disinformation, yet their effectiveness is substantially limited by the absence of a dedicated EU operational structure with the authority to coordinate resilience-building

activities and rapid response and escalation mechanisms connecting national operational capacities to EU-level coordination;

E. whereas the threats posed by FIMI and disinformation extend beyond individual Member States, to an attack on the very essence of the European project; whereas FIMI operations systematically target the core democratic values of Article 2 TEU and the principle of open, transparent decision-making processes enshrined in Article 1 TEU, in a manner that adversely affects the interests of the EU;

F. whereas individual Member States that have invested in dedicated operational structures, with clear statutes and mandates, as well as sufficient funding and staffing, demonstrate what is achievable, most notably in the cases of France's VIGINUM and Sweden's Psychological Defence Agency;

G. whereas the rapid advancement of artificial intelligence (AI) and deepfake technologies is outpacing the adaptive capacity of fragmented national institutions; whereas without coordinated EU responses and clear operational capabilities, the technological advantage will increasingly favour attackers over defenders;

H. whereas the concurrence of the early stages of the implementation of the Digital Services Act (DSA), the Digital Markets Act (DMA), the Artificial Intelligence Act (AI Act) and the European Media Freedom Act (EMFA) establishes a window of opportunity to build comprehensive FIMI defences;

I. whereas democratic societies in the EU are increasingly being targeted by hybrid threats, disinformation and FIMI, with a particular intensity in the digital sphere; whereas the online space enables the proliferation of new manipulation techniques, including: (a) the inauthentic use of social media through automated software programmes, fake social media accounts and the use of troll factories, bot-driven amplification and engagement, (b) the use of astroturfing and flooding techniques to influence online public debate, (c) the personalisation, tracking and micro-targeting of individuals, (d) websites designed to mimic official sources, (e) the artificial amplification of divisive content, (f) the use of synthetic content, such as deepfakes and other AI-generated content, and (g) recommender systems purposefully designed to drive engagement through polarisation;

J. whereas online platforms, when deciding on whether or not to promote content in a user's feed, use their insights into the preferences and vulnerabilities of each individual user, making them more influential than traditional publishers;

K. whereas the EU has recently adopted a set of comprehensive legislative acts to establish a safe and transparent online space, including the DSA, the regulation on the transparency and targeting of political advertising, and the AI Act; whereas these laws represent an important step forward in holding digital platforms accountable and protecting democratic processes, increasing transparency and safeguarding freedom of expression; whereas, at the same time, their enforcement remains a challenge;

L. whereas the use of AI presents new opportunities for strengthening election management and oversight, such as through detecting unusual online activity and coordinated manipulative behaviour; whereas the use of AI, including generative models and deepfakes, also presents significant challenges for information integrity and

electoral processes; whereas credible reports have exposed the operations of a Moscow-based disinformation network known as ‘Pravda’, which has deliberately targeted and infiltrated large language models (LLMs) with pro-Kremlin narratives designed to mimic neutral and fact-based outputs; whereas such tactics represent a dangerous evolution of FIMI, as they exploit the opacity and scalability of AI systems to subtly disseminate false or misleading geopolitical messaging under the guise of authoritative language; whereas this form of algorithmic manipulation threatens to erode public trust in AI technologies, distort democratic discourse, and exacerbate disinformation risks across the EU and globally; whereas this underlines the need for strengthened AI literacy in education, work and society at large;

M. whereas online influencers can play an important role in strengthening the digital resilience of our societies, when raising awareness about media literacy, democratic procedures or contributing to a healthy political debate;

N. whereas the autumn 2024 presidential elections in Romania exposed significant vulnerabilities in the online information environment, with credible reports indicating the widespread use of fake accounts, bots and algorithmically amplified content to promote specific political narratives; whereas TikTok, one of the most widely used platforms among young voters, claimed to have blocked over 116 000 spam accounts from being created and removed 59 000 fake accounts in a post-election clean-up; whereas the use of influencers, including nano- and micro-influencers, by foreign actors further highlights the fact that low-cost, low-visibility actors can be weaponised to evade detection and influence public opinion, in breach of democratic norms;

O. whereas Telegram, a messaging platform with a growing user base in the EU, has increasingly been flagged as a conduit for disinformation, foreign interference and illicit activities, including the spread of extremist content and untraceable political propaganda; whereas its origins in Russia and lack of meaningful content moderation have raised persistent concerns regarding its role in undermining democratic discourse; whereas Telegram has become a primary channel for recruiting ‘disposable agents’ and conducting hybrid operations; whereas malicious state actors have been found to exploit the technological skills, financial needs and naivety of Telegram users, especially young people, to conduct espionage and sabotage operations at minimal cost, while maintaining plausible deniability; whereas reports suggest that Telegram meets the user threshold for it to be classified as a Very Large Online Platform (VLOP) under the DSA, making it subject to stricter regulatory obligations and risk-mitigation requirements;

P. whereas the growing influence of non-European technology companies – particularly those based in the United States and China – has highlighted the EU’s strategic dependencies in critical areas such as data infrastructure, cloud services and social media platforms; whereas fostering home-grown innovation, supporting European start-ups and investing in sovereign digital infrastructure are essential steps towards building a competitive, secure and resilient EU digital ecosystem; whereas aligning digital innovation with democratic values and fundamental rights offers the EU an opportunity to become a global leader in responsible and human-centred technology;

Q. whereas research shows a concerning trend in the revenue redistribution programmes of online platforms, revealing that media outlets that are subject to sanctions, such as

Sputnik and Russia Today, remained listed as ‘partner-publishers’ on Facebook months after the launch of EU sanctions against Russia – raising questions about whether they have continued to benefit financially; whereas such opaque monetisation mechanisms enable foreign state-affiliated actors to profit from sharing disinformation, and continue to destabilise EU information spaces despite regulatory measures;

R. whereas in a survey held in the run-up to the 2025 parliamentary elections in the Netherlands, 1 in 10 respondents declared that they would be likely to ask AI for voting advice, while another 13 % declared they would maybe use it; whereas in the Netherlands, the combined ratio for the youngest voters amounts to more than one third of the voters; whereas this trend is consistent with findings across the Member States and globally; whereas a recent study by the Dutch data protection authority demonstrates that voting recommendations generated by AI chatbots often present a highly distorted and polarised view of the political landscape;

S. whereas the fundamental right to freedom of expression and information, as enshrined in Article 11 of the Charter of Fundamental Rights of the European Union and Article 10 of the European Convention on Human Rights, is a cornerstone of democracy; whereas the EU’s commitment to freedom of expression represents a coherent and principled counter-FIMI strategy, in clear contrast with the restrictions that authoritarian actors systematically impose on their populations; whereas the freedom and pluralism of the media, and the existence of a vibrant civic space, empower societies to detect, expose and reject manipulative narratives through democratic deliberation;

T. whereas freedom of expression and information is a fundamental right designed to protect humans, not machines, bots and AI;

U. whereas FIMI actors exploit technologies to orchestrate coordinated inauthentic disinformation campaigns; whereas these technologies, notably bots and AI-based software programmes, are capable of exhibiting autonomous behaviour, and subsequently distort and destroy genuine public discourse, flooding the expressions of real persons with inauthentic content;

V. whereas the freedom and pluralism of the media are cornerstones of the European way of life, embedded in Article 11(2) of the Charter of Fundamental Rights of the European Union; whereas editorially independent, high-quality journalism is a powerful antidote to FIMI and disinformation;

W. whereas under the DMA, app developers distributing their apps via app stores should be able to inform customers, free of charge, of alternative offers outside of the app store; whereas the Commission has opened an investigation into a potential breach of the DMA by Google in demoting media publishers’ content in search results; whereas the Commission launched its first review of the DMA on 3 July 2025;

X. whereas the Audiovisual Media Services Directive requires the Member States to take measures to develop media literacy skills and report their efforts every three years;

Y. whereas the Media Freedom Rapid Response documented 1 548 press freedom violations in 2024, ranging from legal, physical and psychological threats to forms of censorship, targeting 2 567 media-related persons or entities in 35 European countries, an alarming increase compared to the 1 153 violations recorded in 2023;

Z. whereas Parliament and Council negotiators reached a provisional agreement on the proposed regulation on the screening of foreign investments in the Union on 11 December 2025;

AA. whereas the work of Radio Free Europe/Radio Liberty (RFE/RL) is of strategic interest to the EU; whereas the EU has approved EUR 5.5 million in emergency funding for this work, in the aftermath of the reform of the United States' foreign aid policy; whereas a sustainable funding solution for RFE/RL needs to be developed;

AB. whereas new technologies, such as AI, can improve journalistic working conditions and methods, but can also expose journalists to new threats, such as quick and cheap impersonations of existing media, the mass creation of disinformation outlets and coordinated attacks against journalists;

AC. whereas the ongoing Russian war of aggression against Ukraine illustrates the vital role that civil society plays when communities are in crisis situations, particularly when it comes to providing humanitarian aid, securing basic needs and ensuring the continuation of the everyday lives of affected populations;

AD. whereas civil society also plays an essential role in contributing to policymaking, delivering social and community services, raising awareness of important social issues, representing diverse groups in vulnerable situations, and promoting and protecting the fundamental rights of citizens;

AE. whereas the Commission has published its EU Strategy for Civil Society, which is said to complement the actions set out in the joint communication on the European Democracy Shield; whereas the EU Strategy for Civil Society confirms that the Civil Society Platform, which the Commission has announced will be established as part of the implementation of the strategy, will aim to provide a regular and structured framework for the protection and promotion of EU values and the streamlining and strengthening of engagement on fundamental rights, democracy, equality and the rule of law, and will become operational in 2026; whereas the strategy also includes the creation of an online Knowledge Hub on Civic Space, which should document existing civic-space monitoring initiatives, reports and protection resources, at national, EU and international level, in cooperation with the EU Agency for Fundamental Rights;

AF. whereas the AgoraEU programme, proposed by the Commission for the 2028–2034 multiannual financial framework (MFF), constitutes an important step forward in strengthening EU support for culture, media and civil society, with an anticipated budget of EUR 9 billion;

AG. whereas hybrid attacks targeting critical infrastructure in the EU have become more frequent than ever, with incidents linked to the same malicious actors such as Russia and China, but also Iran and North Korea; whereas these attacks often target essential systems, networks, and facilities that are vital for a society's functioning, including public safety, security, and economic stability; whereas such attacks take various shapes and forms, such as physical sabotage, arson attacks, espionage and signal jamming, as well as cyberattacks and other grey zone activities, all of which demonstrate a coordinated effort to test, disrupt and undermine the EU's security and societal resilience;

AH. whereas the Baltic Sea has witnessed an unprecedented rise in the number of disruptions to submarine cables, which are vital for internet connectivity and power supply in the whole Baltic and Nordic region; whereas, since 2023, at least 11 incidents of cable damage have been recorded, suggesting coordinated sabotage;

AI. whereas in recent months multiple airspace violations and unauthorised drone incursions have been reported over several EU Member States and neighbouring NATO allies, including Poland, the Baltic States, Romania, Denmark, Sweden, Germany, Belgium and Norway; whereas a number of these incidents have been clearly attributed to Russian military aircraft and drones, while other incidents, involving unidentified aerial objects, remain under investigation but are widely suspected to form part of the same pattern of hybrid intimidation and destabilisation directed against Europe;

AJ. whereas several European countries, including France, Estonia, Germany, Czechia and Norway, have recently faced major cyberattacks targeting government systems, critical infrastructure and private enterprises, attributed to Russia's military intelligence services and Chinese state-linked actors, all of which underline the urgent need to strengthen the EU's collective cyber-resilience and cyber attribution capabilities;

AK. whereas the EU's dependence on foreign actors and foreign-made technologies in critical infrastructure and supply chains remains of major concern, and is one of the EU's most significant vulnerabilities; whereas this is particularly prevalent in the tech and digital sectors, posing a key challenge for cybersecurity;

AL. whereas criminal law tools can contribute to the European Democracy Shield to the extent that the activities concerned constitute criminal offences;

AM. whereas judicial and police cooperation mechanisms and cross-border information exchange tools need to be adjusted and strengthened, in light of the growing challenges posed by foreign interference to the EU's internal security;

AN. whereas the EU Agency for Law Enforcement Cooperation (Europol) has warned, in its latest EU Serious and Organised Crime Threat Assessment report (EU-SOCTA), published in March 2025, about the involvement of criminal organisations in hybrid campaigns; whereas the Commission communication on ProtectEU acknowledges that various factors prevent Europol from fully reaching its operational potential in supporting activities to counter cross-border crime, including gaps in the agency's mandate as regards new security threats, notably sabotage, hybrid threats and information manipulation;

AO. whereas the Commission has committed to launching a reform that will make Europol a truly operational police agency; whereas police officers are key partners in safeguarding democratic institutions; whereas this should be more clearly recognised in relevant policies;

AP. whereas the EU Agency for Criminal Justice Cooperation (Eurojust) may be requested by Member States to assist national authorities in dealing with any type of illegal conduct under their jurisdiction; whereas judicial cooperation can prove especially challenging when expanding to new criminal areas, requiring a modernised legal toolbox;

AQ. whereas EU agencies with responsibilities in the area of borders, migration and asylum management, i.e. the European Border and Coast Guard Agency (Frontex) and the EU Agency for Asylum, have a key role to play, in cooperation with national authorities, in establishing and maintaining common situational awareness of risks related to the exploitation of migratory flows for political purposes and in assisting frontline Member States crisis situations; whereas the Commission has included the strengthening of Frontex in its flagship initiatives for the 2024-2029 legislative term;

AR. whereas candidate countries and EU neighbours, notably Ukraine, Moldova and the Western Balkans, remain acutely targeted by FIMI and hybrid threats, and require EU support to build civic and institutional resilience;

AS. whereas Russia's war of aggression against Ukraine and China's assertive geopolitical posture have intensified the use of disinformation, economic coercion and strategic influence, targeting not only the EU, but also vulnerable regions such as the Western Balkans, Eastern Partner countries and the Global South; whereas various sources reveal that Russia's budget for spreading disinformation and propaganda amounts to between USD 1 billion and USD 2 billion per year; whereas elections and political events across Europe demonstrate persistent, targeted and sophisticated full-scale offensive hybrid warfare perpetrated by Russia, aiming to destabilise trust in our political systems and institutions, and to create constant confusion between facts and false information; whereas such warfare requires an appropriate response and a shift from a mere defensive strategy to an offensive one;

AT. whereas the EU Partnership Mission in the Republic of Moldova (EUPM Moldova) was established on 24 April 2023 with the explicit purpose of supporting the Moldovan authorities in combating FIMI;

AU. whereas the reduction in US support for international democracy has created a substantial global gap in funding for countering disinformation and authoritarian influence;

AV. whereas international initiatives, including those by the UN, the Organisation for Economic Co-operation and Development, and the G7, have begun to outline principles and frameworks for safeguarding information integrity, anchored in democratic values, media pluralism and human rights;

AW. whereas FIMI constitutes a growing challenge to the EU's democratic resilience; whereas certain forms of manipulative information activities may also arise from actors operating within the EU; whereas the phenomenon of information manipulation and interference in the domestic context should be further examined and understood, particularly in its interaction with FIMI; whereas the measures presented to combat FIMI also contribute to increasing the overall resilience of societies in the domestic context, particularly with regard to enhancing situational awareness, increasing transparency and pluralism, and strengthening media and digital literacy levels across all age groups;

AX. whereas the Commission's recommendations on inclusive and resilient electoral processes in the Union, published in December 2023, have yet to be fully implemented across all of the Member States, including the provisions aimed at strengthening

cooperation between national authorities during and ahead of electoral processes through the establishment of national election networks;

AY. whereas the ECNE has played an increasingly important role in recent years, but currently lacks the resources and capacity needed to elevate its activities to the next level;

AZ. whereas candidate countries have been invited to participate in meetings of the ECNE; whereas in addition to such participation, there is still significant potential for further enhancing cooperation with these countries within the context of the network's activities, to learn from each other's experiences when encountering threats, and to exchange best practices in fighting these threats;

BA. whereas there is a clear need to strengthen the protection of the electoral infrastructure and that of national political parties that have also been a target of cyberattacks, not least in light of the large-scale cyberattacks targeting the Romanian electoral authorities in autumn 2024;

BB. whereas the covert funding of political parties and movements in the EU by non-EU countries poses a threat to the legitimacy of the democratic process;

BC. whereas judicial independence is an indispensable structural component of electoral integrity; whereas electoral integrity depends on the existence of accessible and effective remedies against violations of voting rights and electoral procedures, insulated from political and executive pressure;

BD. whereas, between 2022 and 2025, the EU imposed a total of 19 packages of extensive and unprecedented sanctions in response to Russia's military aggression against Ukraine, substantially increasing pressure on the Russian war economy, targeting key sectors such as energy, finance and the defence industry, special economic zones, and enablers and profiteers of its war of aggression, and ending the EU's dependency on fossil fuel imports from Russia; whereas the EU has also adopted sanctions against Belarus, Iran and North Korea in response to their support for Russia's military aggression against Ukraine;

BE. whereas, since 8 October 2024, the EU sanctions framework has enabled the targeting of a broad range of hybrid activities carried out by Russia, including the undermining of electoral processes and the functioning of democratic institutions, threats against and the sabotaging of economic activities, services of public interest and critical infrastructure, the use of coordinated disinformation and FIMI, malicious cyber activities, the instrumentalisation of migrants and other destabilising activities; whereas this framework has already led to the sanctioning of tens of individuals and entities, including Russian oligarchs, propagandists, military intelligence operatives, media outlets and companies, for spreading pro-Kremlin narratives, conducting sabotage and undermining democratic processes; whereas related measures now allow the EU to include asset freezes, travel bans and the suspension of broadcasting licences, and to prohibit financial and crypto-asset transactions linked to hybrid activities;

BF. whereas on 28 December 2024, the Russian Government announced that it had 'significantly expanded' its blacklist of EU citizens and officials, including representatives of EU institutions, national governments, law-enforcement agencies and

commercial organisations; whereas this blacklist, targeting those who promote democratic values and oppose Russian aggression in Ukraine, seeks to intimidate and silence voices through opaque and arbitrary restrictions, often without any formal notification, justification or right of appeal;

BG. whereas hybrid threats, foreign interference and disinformation campaigns have evolved into complex, full-scale and cross-sectoral crises with detrimental effects on safety and security, the well-being of citizens, and the functioning of society and the economy as a whole, constituting a key challenge to the EU's internal affairs and destabilising democratic institutions across the Member States, as has been seen throughout Russia's aggression against Ukraine;

BH. whereas effective civilian and defence preparedness requires a comprehensive, whole-of-society, whole-of-government and all-hazards approach that integrates the national authorities of the Member States with EU institutions, bodies, offices and agencies, as well as businesses, academia, civil society and individual citizens; whereas this effort needs to be accompanied by long-term investment, strategic foresight and the embedding of resilience into policymaking, infrastructure development, education systems and supply chains;

BI. whereas empowering citizens is key to societal resilience, and preparedness must include practical tools such as an EU-wide crisis alert app, a household preparedness booklet, and wide-reaching awareness campaigns promoting self-sufficiency and crisis readiness;

BJ. whereas civil-military cooperation, dual-use capabilities and the integration of preparedness into educational programmes are essential for enhancing defence readiness through targeted training not only for workers in critical sectors, such as firefighters, healthcare workers and public servants, but also civil society actors and the public at large;

BK. whereas technological sovereignty and secure digital ecosystems, including projects such as IRIS² and the European Critical Communication System, are key to maintaining control over essential communication channels and strengthening critical infrastructure;

BL. whereas preparedness depends on seamless cooperation between EU institutions, agencies, Member States and international partners, supported by joint exercises and training, shared situational awareness platforms and rapid information exchange;

BM. whereas building credible resilience and achieving a sufficient level of civilian and defence preparedness requires massive investment, boosting Europe's technological and industrial base and reducing strategic dependencies; whereas this effort requires the exploration of new targeted funding mechanisms;

Introduction

1. Welcomes the joint communication from the Commission and the High Representative of the Union for Foreign Affairs and Security Policy on the establishment of a European Democracy Shield and the continued efforts to build on the work already undertaken under the European democracy action plan and the Defence of Democracy package; is of the view that the core mission of the European Democracy Shield should be to

protect European democracy from external threats, and ultimately contribute to safeguarding the European way of life, the rule of law and the values enshrined in Article 2 TEU;

2. Notes with concern the increasingly complex and evolving threat landscape faced by the EU and its Member States, characterised by FIMI, hybrid attacks and disinformation campaigns conducted by malicious third-country actors; stresses that these are hostile actions that undermine the democratic foundations of the EU by fomenting division, diminishing public trust in institutions and exploiting societal vulnerabilities, frequently leveraging advanced digital technologies;

3. Considers Russia as the primary external threat to Europe's democratic integrity; reiterates its view that Russia is a state sponsor of terrorism; underlines the urgent need for a comprehensive, coherent and forward-looking strategy to effectively address these challenges and safeguard European democracy;

4. Reiterates its conviction that the key policy priorities outlined in the European Democracy Shield initiative – including combating FIMI and hybrid threats, strengthening electoral resilience, enhancing cybersecurity, supporting civil society and promoting independent and investigative journalism – must be firmly embedded and sufficiently funded within the upcoming MFF;

European Centre for Democratic Resilience

5. Welcomes the Commission's proposal for a European Centre for Democratic Resilience (the Centre) as a necessary and logical step towards enhanced coordination of efforts to withstand evolving common threats, in particular FIMI and disinformation; notes its approach of a gradual phasing-in of functions and operations, including a gradual increase in Member State participation; welcomes the Commission's assurance that it is already working on setting up the Centre under the leadership of the Commissioner for Democracy, Justice, the Rule of Law and Consumer Protection, with the express aim of ensuring that it is operational in the course of 2026; welcomes the Commission's commitment to regularly update and involve Parliament in the process of implementing the European Democracy Shield and the Centre;

6. Recalls however, that the proposal lacks sufficient operational detail, clear budgetary allocations, a specific governance structure, a concrete mandate and a timeline; notes that the joint communication on the European Democracy Shield does not explicitly link the centre to any of the actions outlined therein, which remain in different administrative frameworks within the Commission and the EEAS; expresses concern that if the Centre remains only another hub, network, platform or framework among others this could further reduce the EU's capacity to make efficient use of the full spectrum of tools available at present, and add to the shortcomings identified in the joint communication, including reduced reactiveness, fragmentation and stretched budgets;

7. Welcomes the fact that the joint communication provides an extensive mapping of existing counter-FIMI and disinformation and resilience frameworks, structures, tools, initiatives and programmes, and a list of the actions which the Commission and the EEAS have committed to undertake; calls on the Commission and the EEAS to propose a clear timeline for their gradual phasing-in and integration within the Centre, with 2026 to be set as the deadline for such integration; calls for this integration to include relevant

DSA supervisory and enforcement mechanisms, especially with a view to identifying and minimising systemic risk, coordinating efforts to counter information manipulation campaigns, ensuring operational responsibility for an enhanced Rapid Alert System (RAS) and the maintenance and operation of a unified FIMI intelligence database, and developing the EUvsDisinfo resource, the ECNE, and the Commission's Task Force on Disinformation and Strategic Communication, among others;

8. Welcomes the Commission's recognition of the need to engage with the Member States and Parliament on the Centre's mandate, structure and working methods, and calls on the Commission to initiate the process by proposing, by Q1 2027, a legal basis for establishing the Centre as an EU entity with a clear institutional statute and positioning, governance structure and parliamentary oversight mechanisms; emphasises that institutional clarity is essential to enable the Centre to act decisively while remaining accountable;

9. Calls on the Commission to endow the Centre with a clear mandate and decision-making mechanisms, thus allowing it to function as an independent centre of excellence for detecting and analysing FIMI and disinformation operations, as a capability-building platform establishing common definitions, standards, training and technical tools across the EU, and as an operational backbone providing real-time coordination of technical support in countering active information manipulation campaigns;

10. Calls on the Commission to ensure that the Centre is mandated with the responsibility to safeguard the integrity of democratic processes at EU level; reaffirms that the Member States' operational structures constitute a first line of defence; stresses, however, that their primary responsibility does not exhaust the EU's legitimate interests with regard to countering FIMI and disinformation; calls on the Commission to clarify that the Centre must serve dual and mutually-reinforcing objectives, namely to coordinate the activities of the Member States in this area and enhance their operational capacity, and to protect the democratic interests of the EU;

11. Calls on Member States that lack dedicated operational structures to establish or substantially strengthen dedicated national FIMI and disinformation detection and response institutions with the Centre's support; calls on the Commission to establish a roadmap for Member State capacity development;

12. Calls on the Commission to assess the feasibility of empowering the Centre to administer and allocate dedicated EU grants under relevant EU programmes, including the Digital Europe Programme, the Connecting Europe Facility, Horizon Europe, the Citizens, Equality, Rights and Values (CERV) programme, and the proposed AgoraEU programme, and to authorise it to issue calls for proposals and to select, oversee and evaluate projects in areas within its mandate, in particular the EDMO, media literacy initiatives and other relevant European, regional and cross-border initiatives devoted to countering FIMI, strengthening democratic resilience and promoting information integrity;

13. Calls on the Commission to provide a dedicated EU budget line for the Centre's operations, with a clear separation between operational funding and general coordination costs; calls on the Commission to secure sufficient human resources and

bridge funding from existing budgets to enable preparatory work before the 2028-2034 MFF;

14. Calls on the Commission to assess the feasibility of establishing a financing mechanism to complement the dedicated budget line for the Centre's operations, based on contributions from VLOPs; recalls that the banking sector funds banking resolution mechanisms, pharmaceutical companies support safety monitoring, and polluting industries bear environmental costs; calls for a mechanism whereby social media platforms contribute proportionally to the infrastructure required to counter negative external influences and systemic risks related to their services, both as regards FIMI and disinformation and building resilience; underlines that such contributions would not only be in line with established European principles of responsibility and accountability but would also ensure that the costs of protecting democratic discourse are shared by those who profit most from the digital information ecosystem;

Digital resilience

15. Calls for the full implementation of key legislation in the digital space, such as the DSA, the regulation on transparency and targeting of political advertising and the AI Act, across all Member States; takes the position that the continued implementation of digital legislation should have a strengthened focus on countering online disinformation, ensuring information integrity and protecting democratic discourse in election periods; expresses concern, in this regard, that delayed guidelines and technical standards pose an obstacle to the timely implementation of the AI Act; welcomes the fact that in its proposed Digital Omnibus to simplify AI legislation the Commission seeks to address this by linking the implementation timeline for rules on high-risk AI systems to the availability of standards or other support tools;

16. Welcomes the official integration of the voluntary Code of Practice on Disinformation into the framework of the DSA; considers the inauthentic use of social media, e.g. through bots, fake accounts, polarising algorithms and artificial engagement and amplification, to be among the most serious risks to free and open discourse online, particularly in election periods; calls urgently on all VLOPs and very large online search engines (VLOSEs) operating in the EU to fully adhere to the Code, and urges the platform X to rejoin it;

17. Welcomes the Commission's commitment to draw up a DSA incidents and crisis protocol to further address major incidents and interference in the information environment; considers that this protocol should address, among other things, electoral interference through coordinated inauthentic behaviour in the online space, particularly through bot-driven amplification and engagement that effectively distort genuine public discourse;

18. Notes the Commission's finalisation of its investigation into the platform X's breach of transparency obligations under the DSA, followed by the imposition of a fine of EUR 120 million; urges the Commission to accelerate remaining investigations into suspected breaches of EU digital legislation, including those involving election interference, algorithmic opacity, or the proliferation of fake accounts and bots; calls, in particular, on the Commission to swiftly conclude investigations into TikTok's

compliance with the DSA in the context of the 2024 Romanian presidential elections, including its obligation to mitigate systemic risks to democratic processes;

19. Calls on the Commission and relevant regulatory authorities to investigate and publicly expose covert disinformation campaigns aimed at exploiting generative AI systems, such as the activities of the Moscow-based ‘Pravda’ network; urges providers of AI systems to duly address and mitigate this phenomenon through their AI risk management systems; calls, furthermore, for the setting of security standards for large language model (LLM) providers to be coordinated at international level, ensuring improved transparency with regard to the training of data sources;

20. Calls on the Commission to urgently complete its assessment of Telegram’s user base and functionality with a view to determining its classification as a VLOP under the DSA; urges the Commission and relevant authorities to investigate Telegram’s potential role in facilitating criminal activity, election interference and the dissemination of disinformation within the EU; furthermore, strongly encourages the platform to join the voluntary Code of Practice on Disinformation and comply fully with EU transparency, content moderation and data access requirements to ensure a level playing field and uphold citizens’ trust in the digital information space;

21. Recommends further examining the role of influencers, including nano- and micro-influencers, in shaping public discourse and influencing elections, both those countering and those contributing to foreign disinformation campaigns, whether knowingly or unknowingly; stresses, in this regard, the need for robust standards on transparency and information integrity for online political content creators, especially influencers operating in a grey area between commercial promotion and political messaging; welcomes existing codes of conduct, training and other initiatives that have been developed to make social media and influencers more responsible and transparent;

22. Considers an EU digital infrastructure, including secure local data centres and sovereign EU cloud and edge computing capacities, to be a strategic pillar of digital resilience, ensuring that Europeans’ sensitive data is not stored in foreign data centres; calls on the Commission to propose a definition of sovereign cloud and its scope of application in the planned Cloud and AI Development Act; calls on the Commission to reflect on the unsuccessful discussion on the EU cybersecurity certification scheme for cloud services and to propose a tangible solution in the revision of the Cybersecurity Act, taking into account the cybersecurity and sovereignty concerns related to a concentration of power; urges the development of regulatory sandboxes and funding mechanisms to support innovation by EU tech start-ups, particularly in sectors with critical dependencies; further supports the long-term vision of EU social media platforms designed in accordance with EU values of transparency, data protection, freedom of expression and democratic accountability;

23. Calls on the Commission, EU digital regulators and online platforms to ensure transparency in revenue redistribution programmes that could allow FIMI actors or even sanctions-listed entities to earn income; considers that the monetisation of FIMI activities under such programmes should be addressed as part of the risk assessment and mitigation obligations under the DSA;

24. Notes with concern the findings of the Dutch data protection authority indicating that AI chatbots may provide biased and unreliable voting advice, thereby posing risks to electoral integrity; calls on the Commission to deliver on its commitment to prepare guidance on the use of AI in electoral processes in order to ensure the responsible use of AI;

Freedom of speech

25. Underlines that the European Democracy Shield must protect and uphold freedom of expression and information as a fundamental right applicable to both offline and online spaces; highlights that human rights protections in the EU are among the strongest worldwide, and that companies wishing to operate in the EU environment and attract European customers have a shared responsibility to safeguard those protections; stresses, however, that the freedoms of expression and information have been designed to protect human beings, not machines or software that exhibit inauthentic behaviour, such as AI and bot-driven amplification and engagements, and automated software programmes performing repetitive tasks over a network with the aim of imitating real users;

26. Recognises the importance of effective safeguards for users when exercising their democratic rights, including the ability to challenge platforms' content moderation decisions and platforms' obligations to inform users when their content gets removed or restricted; recalls the obligation under the DSA for platforms to provide a separate complaint-handling mechanism for this purpose; highlights that safeguarding the fundamental rights of individual users also involves conducting thorough assessments and mitigating systemic risks affecting the integrity of the information space;

Media and information integrity

27. Takes the view that measures to promote free and editorially independent media are a central part of achieving the objectives set by the European Democracy Shield; welcomes, in this regard, the ground-breaking common minimum standards on media freedom and pluralism established through the adoption of the EMFA; underlines, however, that the regulation's significance can only be assessed on the basis of its implementation in practice and therefore stresses the importance of strict enforcement; welcomes the new commitments announced on media support via the Media Resilience Programme and calls on matching long-term commitments in the upcoming MFF;

28. Emphasises the need to carefully assess the potential impact of EU legislation on journalism and editorial media, with particular regard to safeguarding the sustainability and viability of media companies' business models;

29. Underlines, in the context of media companies selling subscriptions via apps, the importance of full implementation of the DMA; notes in this regard the Commission's non-compliance decision of 23 April 2025 with regard to Apple and Meta; notes the Commission's investigations into a potential breach of the DMA by Google in demoting media publishers' content in search results;

30. Welcomes the fact that the joint communication includes new support actions on promoting digital and media literacy, such as the Media Resilience Programme, the Basic Skills Support Scheme for schools, and the strengthening of the media literacy

expert group, including the setting up of a new expert network for media literacy, and updated guidelines for teachers and educators; underlines that the upcoming revision of the Audiovisual Media Services Directive should strengthen the provisions on minimum requirements for Member States' work on media literacy;

31. Welcomes the announced update of the Commission recommendation on the safety of journalists[52] and the forthcoming review of the Anti-SLAPP recommendation[53]; underlines that these updates and reviews must take into account how threats, violence, sabotage and other actions aimed at hindering journalistic work impact the protection, safety and empowerment of journalists and other media professionals in the EU;

32. Stresses the importance of protecting journalists from abusive lawsuits; welcomes, in this regard, the adoption of the Anti-SLAPP Directive[54] and the announced update of the mandate and composition of the expert group against SLAPPs; calls on the Member States to be ambitious in the ongoing implementation process and on the Commission to keep providing support; calls on the Commission to draft a comprehensive evaluation report on the effectiveness of the implementation;

33. Welcomes the provisional agreement on the Foreign Direct Investment Regulation[55], in particular the provisions that include the media sector as a factor to be considered when determining whether an investment is likely to negatively affect security or public order; regrets, however, that the media sector is not listed within the mandatory scope in the Annex to the Regulation;

34. Calls on the Commission and the Member States to carefully analyse the consequences of the US administration's shift in aid policy in the context of media pluralism and independent journalism and, if necessary, to act to fill the void left in media markets both within the EU and in the bordering regions; welcomes the EU emergency funding provided to RFE/RL; calls for the development of a solution to provide RFE/RL with stable, long-term funding;

35. Underlines that society-based fact-checking networks can play a role in detecting and combating disinformation campaigns and provide valuable insights for DSA risk assessments; notes that independent fact-checking organisations need stable conditions in which to operate; considers that the European Network of Fact-Checkers, announced by the Commission in 2025, could be a tool for achieving this; stresses that, to be

---

[52] Commission Recommendation (EU) 2021/1534 of 16 September 2021 on ensuring the protection, safety and empowerment of journalists and other media professionals in the European Union (OJ L 331, 20.9.2021, p. 8, ELI: http://data.europa.eu/eli/reco/2021/1534/oj).

[53] Commission Recommendation (EU) 2022/758 of 27 April 2022 on protecting journalists and human rights defenders who engage in public participation from manifestly unfounded or abusive court proceedings ('Strategic lawsuits against public participation') (OJ L 138, 17.5.2022, p. 30, ELI: http://data.europa.eu/eli/reco/2022/758/oj).

[54] Directive (EU) 2024/1069 of the European Parliament and of the Council of 11 April 2024 on protecting persons who engage in public participation from manifestly unfounded claims or abusive court proceedings ('Strategic lawsuits against public participation') (OJ L, 2024/1069, 16.4.2024, ELI: http://data.europa.eu/eli/dir/2024/1069/oj).

[55] 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 (OJ L 79I, 21.3.2019, p. 1, ELI: http://data.europa.eu/eli/reg/2019/452/oj).

credible and effective, fact-checking organisations must uphold strict standards of political neutrality, independence and methodological objectivity;

Civil society

36. Stresses the crucial role that civil society plays in defending our democracy, not only in acting as a watchdog by exposing and actively combating foreign attempts to interfere with democratic processes, but also in serving as a fundamental force in the long-term effort to build stronger and more resilient societies; underlines, in particular, the important role of civil society in upholding the values enshrined in Article 2 TEU;

37. Welcomes the Commission's EU Strategy for Civil Society, published alongside the communication on the European Democracy Shield; welcomes the Commission's approach of linking this strategy to its work on the Shield, as a tool to further bolster civic engagement;

38. Calls on the Commission to strengthen its work on civil dialogue and to establish new tools for this purpose; welcomes, in this context, the Commission's commitment to establishing an operational Civil Society Platform by 2026 to support a more systematic approach that will be used to strengthen dialogue in line with the EU's values; considers that the announced online Knowledge Hub on Civic Space may contribute to the coordination of the activities of civil society organisations in the area of protecting democracy and countering hybrid threats and FIMI, and improve situational awareness;

39. Stresses the importance of concrete funding programmes such as the CERV programme; welcomes the Commission's idea of maintaining the CERV programme and incorporating it into the new AgoraEU programme for 2028-2034; calls on the Commission to ensure that the funding for this strand of AgoraEU meets the needs of civil society organisations and is implemented under the direct management of the Commission;

40. Underlines the need for increased financial transparency regarding the funding of civil society organisations in general, and in the context of support from non-EU countries in particular; recalls that civil society organisations can be, and have been, used as tools by malicious non-EU-country actors to illegitimately influence democratic processes in the EU and its Member States; stresses that as an institution Parliament has a special responsibility to contribute to reforms in this area, in the light of the so-called Qatargate scandal; highlights, however, that measures to address this issue should be designed in a way that prevents them from being misused to stigmatise the legitimate activities of civil society as such;

41. Welcomes the Commission's proposed directive on interest representation carried out on behalf of third countries as an important part of the Defence of Democracy package, aiming to lay down harmonised requirements for economic activities relating to interest representation carried out on behalf of a third-country entity; stresses that common rules in this regard would constitute an important building block in terms of transparency regarding non-EU-country influence; calls on the co-legislators to finalise the legislative process without delay;

42. Underlines the importance of citizens' engagement in democratic processes; urges the Commission to ensure, in cooperation with the Member States, the clear and effective

communication of the initiatives it develops to promote and enhance the use of its citizen engagement tools; welcomes the Commission's strengthening of such tools, notably the European Citizens' Initiative, the European Citizens' Panels and the Citizens' Engagement Platform, and the proposal to strengthen the network of national authorities on citizen participation;

Protecting critical infrastructure

43. Takes the position that protecting the EU and its Member States from both physical and digital acts of sabotage targeting critical infrastructure is a vital element in safeguarding democratic resilience; calls for robust preventive measures, strengthened cross-border cooperation and enhanced EU capacity to detect, deter and respond to such hostile activities;

44. Strongly condemns escalatory drone and other airborne incursions targeting and interfering with critical infrastructure, including civil airports, military bases and energy facilities across the EU, in particular as perpetrated by Russia and Belarus; calls on the Member States to respond in a coordinated, unified and appropriate manner to any breach of their airspace, including through shooting down aircraft, drones and other airborne threats;

45. Stresses that a range of hybrid activities which Russia has undertaken against the EU amount to state-sponsored terrorism, even if they fall under the threshold of an armed attack; underlines, therefore, the need to apply all available legal frameworks for combating terrorism to Russia's hostile activities, which violate EU Member States' territorial sovereignty, undermine the integrity of their institutions and directly threaten the safety of the civilian population; underlines that the EU must urgently transition from defence mode to active deterrence; urges the Member States to evaluate the legal and operational frameworks for proportionate offensive measures targeting the logistical and digital infrastructure behind Moscow's destabilisation activities;

46. Calls on the Commission and the Member States to establish a joint EU interpretation of the United Nations Convention on the Law of the Sea (UNCLOS), in order to ensure coordinated action against hybrid activities and sabotage in the EU's maritime areas, notably in the Baltic Sea; considers that cross-border coordination can be further improved both at the operational and the financial level; stresses the need for the EU to step up its response to hybrid threats in maritime areas, including those posed by the Russian 'shadow fleet'; underlines that addressing these challenges requires dedicated and sufficient EU funding;

47. Notes with concern the existing structural dependencies, through market concentration and foreign control, in the EU's digital infrastructure, including operating systems, data centres, semiconductors, AI, cybersecurity, cloud computing and various digital platforms and services, all of which pose a high risk to democracy, freedom and security within the EU, and to the EU's competitiveness; calls on the Commission and the Member States to establish, as a foundational layer, a sovereign EU digital infrastructure with privacy-preserving technologies and an EU application programming interface (API) ecosystem through ambitious, targeted policies that enhance investment in and the market share of EU companies, leveraging the European supply of clean energy in the development of data centres and cloud infrastructure, including through

market-driven initiatives such as joint ventures or federated networks in areas such as AI gigafactories or cloud services;

48. Highlights the need to ensure greater integration between digital infrastructure, cybersecurity and defence policy to advance the strategic autonomy of the EU, and the need to leverage dual-use infrastructure, such as resilient data centres scattered across the EU, to ensure operational continuity in the face of hybrid or wartime threats; highlights, further, the need to increase investments in military mobility and secure communications, including the urgent and prioritised deployment of space-based capabilities such as IRIS², to provide encrypted services for public and defence use;

49. Stresses that cybersecurity frameworks such as the NIS2 Directive, the Cyber Resilience Act[56] and the Cyber Solidarity Act[57] must work in alignment to support secure-by-design standards and avoid regulatory fragmentation; calls, in this context, for a revision of relevant legislation in the field of cybersecurity, and underlines the need to strengthen existing structures, such as ENISA and the European Cybersecurity Competence Centre;

50. Recalls the low level of transposition of the NIS2 Directive; regrets that following the deadline of 17 October 2024, the Commission had to send letters of formal notice to as many as 23 Member States for failing to fully transpose the Directive; urgently calls on the Member States to finalise the transposition of the Directive as soon as possible, given that, at the end of 2025, more than one year after the deadline, the Directive was yet to be transposed by 10 Member States; welcomes, in this regard, the Commission's pledge to work closely with the Member States to ensure the swift and coherent implementation of the horizontal cybersecurity framework set out in the NIS2 Directive, as well as the Cyber Resilience Act and the Cyber Solidarity Act, as stipulated in the ProtectEU internal security strategy;

Cooperation in the area of justice and home affairs

51. Takes the view that all criminal law tools available at Member State and EU level should be applied and, where appropriate, further developed to prevent and counter illegal conduct aimed at undermining democratic institutions and processes; supports, in particular, the Commission's commitment to an ambitious overhaul of Europol's mandate, with a view to turning it into a truly operational police agency that better supports the Member States;

52. Welcomes the fact that the joint communication acknowledges the positive contribution of criminal justice and law enforcement cooperation to countering FIMI and disinformation activities; calls on the Commission, when preparing the planned revision of the mandates of Europol and Eurojust, to carefully assess the legal gaps which

[56] 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) (OJ L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

[57] 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) (OJ L, 2025/38, 15.1.2025, ELI: http://data.europa.eu/eli/reg/2025/38/oj).

currently prevent those agencies from providing their full assistance to the Member States confronted with hybrid threats, and to explore ways to overcome them;

53. Notes with concern the increasing examples of how malicious non-EU-country actors use crime as a service and criminal organisations as proxies within the EU to target individuals and entities identified as political adversaries, posing a grave threat to the EU's internal security; stresses that such practices constitute an intolerable act of foreign interference, with potentially destabilising effects on our societies; underlines, in this context, the need to further reinforce EU-level coordination in the field of criminal justice and law enforcement;

54. Strongly condemns the weaponisation and instrumentalisation of migration against the EU; takes the position that this phenomenon represents an unacceptable attempt by malign non-EU countries to exercise political pressure on frontline Member States and on the EU; welcomes the specific provisions on the instrumentalisation of migration recently included in key pieces of EU legislation on border management and migration; stresses that the Member States affected by such threats should be able to rely on support from specialised EU agencies; calls for Frontex's mandate to be strengthened so that the agency has the legal basis and the human, financial and technical resources it needs to properly assist the Member States in dealing with such hybrid threats; stresses, in this context, the need to further enhance the EU's capacity to contribute to Member States' border protection efforts through sufficient investment under the 2028-2034 MFF;

External dimension

55. Underlines the need for the European Democracy Shield to have a robust external dimension; welcomes the inclusion in the joint communication of specific actions aimed at supporting countries beyond EU borders, in particular by facilitating capacity-building to improve candidate and potential candidate countries' resilience to FIMI and hybrid interference, and by supporting independent media and journalism, and increasing their ability to monitor disinformation on social media before and during elections;

56. Supports the idea of leveraging diplomatic channels to strengthen capacity in priority regions; considers the role of EU Delegations and EU Member States' embassies to be key, in terms of gaining a better understanding of local circumstances that may lead to foreign interference, and of delivering a tailored response; notes the possibility for EU Delegations and Member States' embassies to support the organisation of awareness-raising campaigns in host countries; highlights the importance of involving common security and defence policy (CSDP) missions and operations in the actions envisaged in the joint communication; calls on the Member States and the EEAS to integrate capacity-building activities and training on hybrid threats into the individual mandates of missions and operations, in order to increase the preparedness of national counterparts;

57. Calls for the development of a comprehensive strategy whereby EU Delegations and CSDP missions and operations, in close coordination with the diplomatic missions of the EU Member States, can serve more effectively as a first line of defence against hybrid attacks, including cyber and FIMI operations; considers that enhanced strategic

communication and public diplomacy capacities within EU Delegations – with a focus on promoting fact-based narratives, civic engagement and trust-building, particularly among young people and educators – are of vital importance; calls on the Vice-President of the Commission / High Representative of the Union for Foreign Affairs and Security Policy and the Council to include disinformation monitoring and response teams within CSDP missions, ensure FIMI training for all mission staff, and strengthen coordination between civilian and military operations to counter hybrid influence;

58. Welcomes the strengthened commitment in the joint communication to developing an offensive information operations capacity; notes that such a commitment requires dedicated resources and long-term planning; stresses that the objective should include the EU's strengthening, in its neighbourhood, of proactive information measures to counter Russia's destabilising efforts; highlights the need to disseminate factual and trustworthy information to the populations living in authoritarian regimes, notably Russia, in order to reveal their rulers' destructive governance practices, which pose danger to freedom and peace not only in neighbouring countries, but primarily inside their own country; calls for every possible use of the digital and cyber space and its borderless nature to achieve this goal;

59. Recognises that the EU's immediate neighbours, including the Western Balkans, Moldova and Ukraine, face serious foreign interference; calls for the funding of regional coordination hubs for countering FIMI, boosting support for investigative journalism and media regulators and scaling up fact-based strategic communications via EU Delegations to counter anti-EU disinformation; underlines the need for a specific focus on election integrity assistance in the countries that are candidates for EU membership;

60. Calls on the Commission to make media literacy programmes a permanent part of pre-accession assistance and the European Neighbourhood Instrument, with dedicated EU grants for supporting investigative journalism in vulnerable regions;

61. Calls for strengthening current EU efforts to support partner countries in its neighbourhood, as well as in priority countries in sub-Saharan Africa, the Asia-Pacific region and Latin America, in building resilience to FIMI, strengthening democratic processes, and ensuring electoral integrity; underlines, in particular, the need to continue developing the flagship project EUvsDisinfo;

62. Acknowledges the establishment of EUPM Moldova as a successful example of how the EU can play a decisive role in supporting a partner country's crisis management structures and enhancing its resilience against hybrid, cyber and FIMI threats; considers that EUPM Moldova should serve as a model for including the countering of hybrid threats in the mandate of existing missions, or the establishment of similar missions in other partner countries; takes note of the parliamentary election held in Moldova on 28 September 2025 and the strong victory of the pro-European Party of Action and Solidarity (PAS);

63. Welcomes the deployment of EU Hybrid Rapid Response Teams, as illustrated by the recent example of Moldova, as a useful instrument in building capacity and resilience in countries targeted by hybrid, cyber and FIMI attacks, on the basis of the specific know-how and expertise of the EU and its Member States;

64. Underlines the importance of prioritising the principles and objectives of the European Democracy Shield in international cooperation with like-minded partners, such as the G7, NATO, the UN, the Organization for Security and Co-operation in Europe and the Council of Europe; welcomes the steps already taken within the framework of bilateral and multilateral engagement, notably the UN Code of Conduct for Information Integrity on Digital Platforms, the commitment of Council of Europe member states in the Reykjavik Declaration to safeguard electoral systems against foreign interference, the Security and Defence Partnerships and the continued efforts of the G7 Rapid Response Mechanism to foresee and develop collective responses to FIMI;

65. Welcomes the establishment of a Security and Defence Partnership between the EU and the UK in May 2025; welcomes its focus on, among other things, cooperation in countering cyber issues, hybrid threats and FIMI, and on protecting critical infrastructure;

Election systems and electoral resilience

66. Underlines that a core objective of the European Democracy Shield should be to protect the integrity of elections at local, regional, national and EU levels; calls on the Commission and the Member States to work together, with full respect for the principle of subsidiarity, to implement reforms aimed at strengthening the resilience of electoral processes in Europe, with a particular focus on measures to prevent foreign interference;

67. Calls on the Member States to step up efforts to implement the Commission's recommendations on inclusive, robust and resilient electoral processes within the EU; underlines, in particular, the importance of establishing national election networks to help national authorities and expert bodies to work in synergy;

68. Calls on the Member States to ensure that election authorities or equivalent bodies in charge of well-functioning, free and fair elections are sufficiently funded and equipped with the proper tools to allow them to carry out their functions, be this in terms of providing personnel training and the necessary digital tools, or in terms of ensuring sufficient investment in electoral bodies and election infrastructure;

69. Considers that hate campaigns and violence that make it difficult for candidates to participate in the public debate, or interact with voters, constitute a threat to democracy; underlines that such threats can be fuelled by non-EU countries' attempts to destabilise the EU; welcomes, in this regard, the Commission's commitment to presenting recommendations on safety in politics; calls on the Member States to step up their efforts to protect candidates standing for election and elected representatives;

70. Underlines the key role of the ECNE in ensuring the exchange of best practices with regard to electoral resilience in the EU and its Member States; notes, however, the current limitations of its activities; welcomes the Commission's commitment to strengthening the ECNE, including reforms such as putting in place a repository of common references and standards for electoral processes;

71. Calls on the Commission to raise its level of ambition with regard to reforming the ECNE, including by reviewing its resources and permanent staff and by further developing the joint mechanism for electoral resilience; stresses the importance of implementing concrete measures to strengthen the involvement of candidate countries in

the ECNE's operations; calls on the Commission, within the framework of the ECNE, to establish a permanent monitoring group responsible for overseeing the implementation of the Commission's recommendations on inclusive and resilient electoral processes in the EU, and the forthcoming recommendations on the safety of political actors; considers that such a monitoring group should also be mandated to develop proposals for future updates of these recommendations;

72. Calls on the Commission to include Parliament and the Authority for European Political Parties and European Political Foundations (APPF) as permanent partners in all meetings of the ECNE;

73. Welcomes the Commission's objective of strengthening the protection of election-related infrastructure through existing legislation and tools; calls on the Commission to complement these efforts with a targeted revision of the Resilience of Critical Entities Directive, with a view to including electoral infrastructure in the Directive's list of essential public administration services;

74. Calls on the Commission and the Member States to address the issue of foreign actors' involvement in the party political landscape in Europe; notes with concern various examples of non-EU-country funding of extremist movements within the EU; considers that financial transparency is an important tool for shedding light on this issue and calls for enhanced exchange between private and public entities in this regard; stresses, in particular, the need to combat covert political communication, including opaque funding structures and hidden sponsors, in order to safeguard democratic integrity and ensure transparency for citizens;

75. Notes with concern the growing evidence of foreign interference and espionage within Europe's political system; welcomes the investigative efforts across the Member States that have led to convictions and ongoing proceedings related to bribery, espionage and the promotion of foreign state interests; underlines the serious risks posed by inadequate safeguards in the recruitment of staff and associates with close links to authoritarian regimes;

76. Welcomes the recently adopted regulation on the revised rules for the statute and funding of European political parties and foundations; notes the provisions concerning the financing and participation of parties from non-EU countries; calls on the co-legislators to ensure its full and effective implementation;

77. Notes that developments in cryptocurrency create a potential vulnerability in terms of both a lack of transparency and of the ability to scrutinise the financing of political parties and movements in Europe; acknowledges the Commission's commitment to bring together national experts under the umbrella of the ECNE, in close cooperation with other EU networks and stakeholders, to exchange best practices, prepare possible guidelines and promote joint actions, in this regard; calls on the Commission to continue monitoring the implementation of the anti-money laundering package and the Markets in Crypto-Assets Regulation and to address any potential gaps in the legislation that may need to be filled;

The role of sanctions in the protection of democracy

78. Considers sanctions against foreign entities, countries or individuals that engage in conduct aimed at undermining the democratic integrity of the EU or its Member States to be an important element of the European Democracy Shield's objectives; further stresses that effective sanctions must include a comprehensive set of activities, including asset freezing and confiscation, attribution and exposure, cost increases and revenue cuts, bans on imports and exports, the denial of access and other relevant restrictive measures;

79. Calls on the Commission and the Member States to regularly and closely assess imposed sanctions in terms of optimal efficiency and possible further expansion, including secondary sanctions targeting entities that engage in the circumvention of sanctions; considers that, particularly in the area of Russian hybrid threats and destabilising activities, the EU should further expand its sanctions regime by targeting the financial and technical enablers that sustain disinformation, cyberattacks and election interference, such as crypto exchanges, advertising networks and hosting providers, while also disrupting Russia's proxy networks in non-EU countries, notably in Africa and the Middle East, by imposing sanctions on media outlets, logistics hubs, and Wagner-linked groups that spread anti-EU narratives; considers that to further raise the cost of hybrid aggression, the EU should expand secondary sanctions on non-EU – and in particular, Chinese – firms that facilitate Russian operations, and that it should ban Russian cyber mercenaries from using EU-based services, such as hosting, domain and cloud services, and publicly expose and impose sanctions on EU politicians or lobbyists covertly funded by Moscow;

80. Considers that identifying and naming source countries, rather than individuals or companies, could be an important step towards acknowledging the problem of clear systematic, multi-layered and often state-sponsored interference that countries such as Russia or Iran are engaging in throughout Europe; welcomes the Commission's decision to list Russia as a high-risk third country under the EU's anti-money laundering and counter-terrorist financing framework, in order to preserve the integrity of the EU financial system; recalls that the new Anti-Money Laundering Regulation will provide an additional legal basis for identifying dangerous countries, including those involved in the proliferation of weapons of mass destruction;

81. Underlines that the effectiveness and credibility of EU sanctions depend on strict and consistent enforcement; highlights that the announced revision of the mandate of the European Public Prosecutor's Office (EPPO) offers an opportunity to strengthen its role to include the investigation and prosecution of sanctions violations;

82. Condemns Russia's politically motivated use of 'blacklists' targeting EU citizens, representatives of state authorities and commercial organisations, journalists, civil society actors and political officials, including democratically elected Members of the European Parliament; calls for a more coordinated and resolute EU response to these arbitrary measures, ensuring the protection and security of those blacklisted and providing them with solidarity and the necessary support; expresses its full support for all individuals affected;

The EU's preparedness

83. Welcomes the EU Preparedness Union Strategy and underlines that the objectives set out in the strategy are closely interconnected with those of the European Democracy Shield; further emphasises that democratic resilience requires societies to be able to function under exceptional or disruptive conditions, and that reforms aimed at strengthening preparedness should therefore form an integral part of the European Democracy Shield;

84. Calls for the swift development and deployment of an EU-wide, interoperable crisis-alert application, providing real-time, reliable, multilingual information to citizens during emergencies; recommends that this app be integrated into national and EU early warning systems, accessible to vulnerable groups, and regularly updated with technological advancements and best practices in crisis management;

85. Welcomes the initiatives in several Member States to distribute a household preparedness booklet, offering clear, practical guidance tailored to Europe's diverse social and geographic realities to help citizens prepare for emergencies; calls on the Commission to produce an EU-level booklet reflecting the cross-border and multinational context, including recommended emergency supplies, practical self-sufficiency instructions for at least 72 hours, basic first aid advice and specific guidance for vulnerable groups, including elderly people, people with disabilities and families with children;

86. Calls for the organisation of regular large-scale, EU-coordinated preparedness exercises involving EU institutions, Member States, regional and local authorities, the private sector and civil society; recommends that these exercises simulate complex, realistic scenarios, including cyberattacks, critical infrastructure disruptions, coordinated disinformation and hybrid crises, in order to assess response capacities, improve interoperability across governance levels and promote a culture of preparedness at all levels; calls, to this end, for the establishment of a European Preparedness Day; considers that the date for this event should be 24 February, the date of Russia's unprovoked full-scale military invasion of Ukraine in 2022, as a symbol of the EU's solidarity with Ukraine and a stark reminder of the necessity for strengthened civilian and defence preparedness against growing threats from authoritarian regimes;

87. Calls on the Commission to examine the possibility of expanding Erasmus+ or similar programmes to include cross-border initiatives on preparedness training for workers in critical sectors, such as firefighters, healthcare workers, civil protection volunteers, public servants and representatives of civil society organisations and the public at large; recommends that these programmes promote cross-border and cross-sectoral knowledge exchange, joint exercises and training on hybrid threats and emergencies, and strengthen local preparedness capacities across all Member States, with a special focus on vulnerable regions;

88. Calls for the accelerated implementation of secure communication systems such as IRIS² and the European Critical Communications System; stresses that these initiatives ensure telecommunications resilience, the continuity of essential services during crises, reduced external dependencies in strategic sectors, and reinforced cybersecurity for these infrastructures;

89. Calls for enhanced coordination between EU institutions, bodies, offices and agencies, the Member States and international partners through shared situational awareness platforms, common methodologies and rapid, secure information-sharing mechanisms; stresses that these tools enable a coherent, agile and coordinated response to hybrid threats, improve risk anticipation and strengthen the EU's collective preparedness and resilience;

90. Highlights the need to mainstream preparedness within the 2028-2034 MFF, in order to build credible resilience and achieve a sufficient level of civilian and defence preparedness; urges the Commission to develop targeted financial instruments combining relevant defence and civil security instruments, such as the Defending Europe Facility and the Securing Europe Facility, in order to provide sufficient and stable funding for resilience-building projects, technological innovation and dual-use capabilities, civil preparedness initiatives, critical infrastructure protection, and efforts to strengthen the EU's industrial and technological sovereignty; notes that dedicated funding streams should also prioritise local preparedness efforts, particularly in territories most exposed to vulnerabilities and hybrid threats;

91. Recommends that the EU's decision-making institutions review and optimise their strategies and contingency plans in case of an open military conflict against one or more Member States and similar crisis scenarios; stresses, furthermore, the need to ensure the highest levels of safety and security in all EU institutions, bodies, offices and agencies, including in the area of cybersecurity and the security and integrity of information, and to create the necessary conditions in this regard, including ensuring accredited secure communication channels and adequate meeting rooms for 'in camera' meetings; underlines the need to strictly enforce rules on breaches of information security and confidentiality, in particular in the context of a heightened risk of espionage and sabotage; stresses that, even outside of open military conflict, hybrid threats continue to pose ever higher risks to the daily functioning of the EU;

92. Welcomes the Commission's efforts to strengthen physical and information security within the EU institutions, as outlined in the Corporate Management Board note of October 2025, including plans for secure meeting rooms, enhanced security clearance procedures for staff handling classified information, and the establishment of the Security College to ensure regular updates on threat developments; notes that these measures respond to heightened risks from espionage, foreign interference and hybrid threats targeting EU decision-making processes; stresses, however, that physical security upgrades must be complemented by robust cybersecurity protocols and counter-intelligence capabilities to address the full spectrum of infiltration risks; calls for the swift adoption of the Commission proposal for a regulation on information security in the institutions, bodies, offices and agencies of the Union (COM/2022/0119); recalls that the Cybersecurity Regulation for the EU institutions, bodies, offices and agencies recommends a cybersecurity budget of 10 % of the overall information and communications technology budget for EU entities;

93. Recommends that further measures be taken to increase Parliament's security and resilience to foreign interference, and its preparedness for, and ability to function, during crises; calls, in this regard, for reinforced support for its Members, including IT and security checks, training and specific briefings ahead of missions, and enhanced interdisciplinary training and other resilience-building activities combining physical and

information security, safety, and cybersecurity; calls for further targeted training for Parliament staff to prevent information manipulation; recommends strengthening its cybersecurity environment in compliance with the Cybersecurity Regulation, and increasing its operational maturity to further enhance its cybersecurity resilience and improve its threat-detection capacities in the context of a dynamic cybersecurity threat landscape and rapidly changing technological environment;

94. Notes, in the context of Parliament's internal security, that the use by Members and staff of private mobile phones and other devices such as laptops for business purposes constitutes a vulnerability that could be exploited to attack the institution; underlines that Members and staff should be equipped with the necessary IT devices, such as mobile phones and laptops, to perform their tasks; welcomes, in this context, the security screenings offered to Members and staff, upon request, to detect potential spyware on private devices; calls on the administration to extend and systematise this screening to cover all devices used for Parliament-related work; calls for clearer rules and systematic and appropriate guidance to Members and staff, and for safeguards to mitigate these risks, especially during missions;

95. Calls on the Commission and the EEAS to involve Parliament in its preparedness activities and exercises, such as the EU Integrated Resolve, as a matter of course;

°

° °

96. Instructs its President to forward this resolution to the Council, the Commission, the Vice-President of the Commission / High Representative of the Union for Foreign Affairs and Security Policy, and the governments and parliaments of the Member States.

EXPLANATORY STATEMENT

The European Union is founded on the values of democracy, the rule of law and fundamental rights, which form the basis of its political order, institutional legitimacy and societal cohesion. Over the past years, these foundations have been increasingly targeted by a rapid intensification of hostile activities. Foreign information manipulation and interference (FIMI), hybrid operations, coordinated disinformation campaigns, and other forms of malign influence have grown in scale, sophistication and impact.

These tactics deliberately exploit social fractures, manipulate public debate, and seek to undermine citizens' confidence in the institutions and democratic processes of the Union and its Member States. Their increasingly digital nature – amplified through opaque online platforms and cross-border dissemination networks – has made the threat landscape more complex and more difficult for Member States to confront individually. Against this backdrop, the Union has recognised the need for a more strategic, coordinated, and anticipatory response. Building on the work carried out by its previous special committees dedicated to foreign interference in democratic processes (INGE and INGE2), the European Parliament decided in December 2024 to establish a Special Committee on the European Democracy Shield (EUDS), tasked with examining how the Union can better defend its democratic foundations.

The Joint Communication on the European Democracy Shield, presented by the Commission together with the VP/HR, marks an important contribution to this effort. It provides a structured overview of the current threat environment and identifies several domains where further action is required to protect the Union against FIMI and disinformation, and to strengthen societal resilience. The rapporteur has welcomed this initiative and recognised its added value in consolidating the Union's understanding of the challenges ahead.

However, while the communication sets the right direction, its level of ambition remains too limited in light of the scale of the threats. What is needed is not only a framework for reflection but a concrete reform agenda capable of delivering operational capacity, accountability, and long-term preparedness.

The Union has developed a growing ecosystem of structures, tools, and programmes aimed at countering foreign information manipulation and disinformation. These efforts – including the work of relevant task forces, cooperation networks, and early-warning mechanisms – are significant. Yet, to take this work to the next level, reforms must also be put in place. The proposal to establish a European Centre for Democratic Resilience is a welcome and promising initiative. However, in the form presented in the Communication, such initiative lacks the operational clarity required for the Centre to become an effective hub of expertise and action. Concrete recommendations have been put forward in the draft report for this objective to be achieved.

Regarding the digital sphere – which in many ways is exploited by malign third-country actors to conduct their operations – the rapporteur is of the view that relevant EU legislation must be upheld and that the Commission needs to intensify its enforcement actions, particularly where there are indications of election-related manipulation, systemic algorithmic opacity, coordinated inauthentic behaviour, or large-scale misuse of platform functionalities.

The evolving threat environment also requires the Member States to cooperate more effectively at Union level on the conduct of elections. The integrity of electoral processes lies at the heart of democratic resilience. In this context, the draft report stresses the need for significantly enhancing the European Cooperation Network on Elections (ECNE) and encourages a comprehensive reform to make this network more ambitious and operationally relevant. Furthermore, election-related infrastructure should be recognised as part of the Union's critical infrastructure and protected accordingly.

The rapporteur has also welcomed that the Joint Communication on the European Democracy Shield includes an external dimension. The objectives of the Democracy Shield cannot be achieved without close cooperation with partners in the Union's neighbourhood, particularly candidate countries that are increasingly exposed to intense foreign interference. Support for their resilience – including through capacity-building, training, and the provision of expertise – is indispensable for safeguarding Europe's wider democratic space. The draft report calls on the EEAS to systematically incorporate hybrid-threat preparedness measures into the mandates of CSDP missions and operations, thereby strengthening the ability of national counterparts to detect and counter malign influence. As part of the Shield's external dimension, a review of relevant sanctions instruments should also be undertaken to ensure they are optimally calibrated to target actors undermining Europe's democratic integrity. Alignment with like-minded partners is also important with a view to ensuring effective collective responses; the rapporteur welcomes the use of multilateral and bilateral channels of cooperation, including the existing EU Security and Defence Partnerships.

The draft report further emphasises the need for an ambitious agenda to make society more resilient. Reforms to support the media sector are an important component of this, alongside measures to strengthen media literacy. Civil society and the EU's civil society strategy constitute another key aspect: a strong and independent civil society is essential for democratic resilience. The rapporteur pleads in favour of robust programmes supporting the policy priorities outlined in the European Democracy Shield initiative within the next multiannual financial framework 2028-2034.

In strengthening societal resilience, enhanced protection of critical infrastructure is also crucial and should be reassessed in light of the objectives of the Democracy Shield. This in turn necessitates reforms to increase European sovereignty over digital infrastructure, operating systems, data centres, semiconductors, AI, cybersecurity, cloud computing, and various digital platforms and services. The revision of the mandates of relevant EU agencies, such as Europol and Frontex, can also play a significant role in improving resilience and protection against hybrid threats.

Finally, the draft report stresses that building democratic resilience also requires societies that can continue to function under exceptional or disruptive conditions. Reforms aimed at strengthening preparedness – from crisis-management capacities to the continuity of democratic institutions – must therefore form an integral part of the European Democracy Shield. The draft report concludes that protecting and strengthening Europe's democratic systems requires not only vigilance and resilience at every level of society, but also a coordinated and forward-looking Union strategy, backed by sufficient resources and political commitment.

ANNEX: DECLARATION OF INPUT

Pursuant to Article 8 of Annex I to the Rules of Procedure, the rapporteur declares that he included in his report input on matters pertaining to the subject of the file that he received, in the preparation of the draft report, from the following interest representatives falling within the scope of the Interinstitutional Agreement on a mandatory transparency register[1], or from the following representatives of public authorities of third countries, including their diplomatic missions and embassies:

1. Interest representatives falling within the scope of the Interinstitutional Agreement on a mandatory transparency register
European Partnership for Democracy
EU DisinfoLab
Schibsted ASA
European Confederation of Police
Reporters sans frontières
TikTok Technology Ltd
Europe MédiaLab
Psychological Defence Research Institute
Civil Society Europe (CSE)
European Fact-Checking Standards Network
Stiftung Mercator
The Foundation for European Progressive Studies (FEPS)
Konrad Adenauer Foundation
Association of Commercial Television in Europe (ACT)
European Association for Local Democracy (ALDA)
Martens Center
2. Representatives of public authorities of third countries, including their diplomatic missions and embassies
n.a.

The list above is drawn up under the exclusive responsibility of the rapporteur.

Where natural persons are identified in the list by their name, by their function or by both, the rapporteur declares that he has submitted to the natural persons concerned the European Parliament's Data Protection Notice No 484 (https://www.europarl.europa.eu/data-protect/index.do), which sets out the conditions applicable to the processing of their personal data and the rights linked to that processing.

[1] Interinstitutional Agreement of May 2021 between the European Parliament, the Council of the European Union and the European Commission on a mandatory transparency register (OJ L 207, 11.6.2021, p. 1, ELI:http://data.europa.eu/eli/agree_interinstit/2021/611/oj).