European Parliament
2024-2029

TEXTS ADOPTED

P10_TA(2026)0286

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

European Parliament resolution of 15 September 2026 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 5 thereof on EU competences, 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 the United Nations,

– having regard to the provisions on freedom of expression set out in Article 19 of the Universal Declaration of Human Rights, Article 19 of the International Covenant on Civil and Political Rights, Article 10 of the European Convention on Human Rights (ECHR) and Article 11 of the Charter of Fundamental Rights of the European Union,

– 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],

---

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.

– 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 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] (Anti-SLAPP Directive),

– 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] (Transparency and Targeting of Political Advertising Regulation),

– 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] (Cybersecurity Regulation),

– 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] (Resilience of Critical Entities Directive),

– 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

---

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.
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.

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) 2024/1252 of the European Parliament and of the Council of 11 April 2024 establishing a framework for ensuring a secure and sustainable supply of critical raw materials and amending Regulations (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1724 and (EU) 2019/1020[14] (European Critical Raw Materials Act),

– having regard to the joint communication from the Commission and the High Representative of the Union for Foreign Affairs and Security Policy of 3 December 2025 entitled ‘Strengthening EU economic security’ (JOIN(2025)0977),

– 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[15],

– 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[16],

– 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)[17],

– 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[18], 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[19],

---

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, 2024/1252, 3.5.2024, ELI: http://data.europa.eu/eli/reg/2024/1252/oj.
15 OJ L 156, 5.5.2021, p. 1, ELI: http://data.europa.eu/eli/reg/2021/692/oj.
16 OJ L 305, 26.11.2019, p. 17, ELI: http://data.europa.eu/eli/dir/2019/1937/oj.
17 OJ L 95, 15.4.2010, p. 1, ELI: http://data.europa.eu/eli/dir/2010/13/oj.
18 OJ L 78, 17.3.2014, p. 16, ELI: http://data.europa.eu/eli/dec/2014/145(1)/oj.
19 OJ L 78, 17.3.2014, p. 6, ELI: http://data.europa.eu/eli/reg/2014/269/oj.

– 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[20], 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[21],

– 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[22], 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[23],

– 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[24], 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[25],

– having regard to Council Decision (CFSP) 2024/2643 of 8 October 2024 concerning restrictive measures in view of Russia's destabilising activities[26] and Council Regulation (EU) 2024/2642 of 8 October 2024 concerning restrictive measures in view of Russia's destabilizing activities[27],

– having regard to Council Decision 2012/642/CFSP of 15 October 2012 concerning restrictive measures against Belarus[28], and to Council Regulation (EC) No 765/2006 of 18 May 2006 concerning restrictive measures against President Lukashenko and certain officials of Belarus[29],

– 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[30], 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[31],

– having regard to Council Decision (CFSP) 2024/1603 of 31 May 2024 amending Decision (CFSP) 2016/849 concerning restrictive measures against the Democratic

---

20 OJ L 66, 6.3.2014, p. 26, ELI: http://data.europa.eu/eli/dec/2014/119(1)/oj.
21 OJ L 66, 6.3.2014, p. 1, ELI: http://data.europa.eu/eli/reg/2014/208/oj.
22 OJ L 229, 31.7.2014, p. 13, ELI: http://data.europa.eu/eli/dec/2014/512/oj.
23 OJ L 229, 31.7.2014, p. 1, ELI: http://data.europa.eu/eli/reg/2014/833/oj.
24 OJ L 42 I, 23.2.2022, p. 109, ELI: http://data.europa.eu/eli/dec/2022/266/oj.
25 OJ L 42 I, 23.2.2022, p. 77, ELI: http://data.europa.eu/eli/reg/2022/263/oj.
26 OJ L, 2024/2643, 9.10.2024, ELI: http://data.europa.eu/eli/dec/2024/2643/oj.
27 OJ L, 2024/2642, 9.10.2024, ELI: http://data.europa.eu/eli/reg/2024/2642/oj.
28 OJ L 285, 17.10.2012, p. 1, ELI: http://data.europa.eu/eli/dec/2012/642/oj.
29 OJ L 134, 20.5.2006, p. 1, ELI: http://data.europa.eu/eli/reg/2006/765/oj.
30 OJ L 186, 25.7.2023, p. 20, ELI: http://data.europa.eu/eli/dec/2023/1532/oj.
31 OJ L 186, 25.7.2023, p. 1, ELI: http://data.europa.eu/eli/reg/2023/1529/oj.

People's Republic of Korea[32], 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[33],

– 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 Commission proposal of 21 January 2026 for a regulation of the European Parliament and of the Council on digital networks, amending Regulation (EU) 2015/2120, Directive 2002/58/EC and Decision No 676/2002/EC and repealing Regulation (EU) 2018/1971, Directive (EU) 2018/1972 and Decision No 243/2012/EU (Digital Networks Act) (COM(2026)0016),

– having regard to the Commission proposal of 20 January 2026 for a regulation of the European Parliament and of the Council on the European Union Agency for Cybersecurity (ENISA), the European cybersecurity certification framework, and ICT supply chain security and repealing Regulation (EU) 2019/881 (The Cybersecurity Act 2) (COM(2026)0011) (revised Cybersecurity Act),

– having regard to the Commission proposal of 3 June 2026 for a regulation of the European Parliament and of the Council on a framework of measures for strengthening the Union's semiconductor ecosystem, repealing Regulation (EU) 2023/1781 (Chips Act 2.0) (COM(2026)0504),

– having regard to the Commission proposal of 3 June 2026 for a regulation of the European Parliament and of the Council establishing a framework of measures for strengthening Europe's cloud and AI ecosystem (Cloud and AI Development Act) (COM(2026)0502),

– 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))[34],

– having regard to its previous resolutions on the Russian Federation and its aggression against Ukraine, as well as its hostile actions against the Member States, including its resolution of 9 October 2025 on a united response to recent Russian violations of the EU Member States' airspace and critical infrastructure[35],

– having regard to its resolution of 29 April 2026 on the Commission's 2025 Rule of Law report[36],

---

32 OJ L, 2024/1603, 31.5.2024, ELI: http://data.europa.eu/eli/dec/2024/1603/oj.
33 OJ L, 2024/1602, 31.5.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/1602/oj.
34 Texts adopted, P10_TA(2025)0306.
35 Texts adopted, P10_TA(2025)0230.
36 Texts adopted, P10_TA(2026)0147.

– having regard to its resolution of 7 May 2025 on a revamped long-term budget for the Union in a changing world[37],

– having regard to its resolution of 23 January 2025 on Russia's disinformation and historical falsification to justify its war of aggression against Ukraine[38] and to its resolution of 22 October 2025 on the Council's position on the draft general budget of the European Union for the financial year 2026[39], which mentions the project to build a memorial in Brussels,

– 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[40],

– having regard to its resolution of 13 November 2025 on addressing transnational repression of human rights defenders[41],

– having regard to its resolution of 21 January 2026 on addressing impunity through EU sanctions, including the EU Global Human Rights sanctions regime (so-called 'EU Magnitsky Act;)[42],

– having regard to its resolution of 1 June 2023 on foreign interference in all democratic processes in the European Union, including disinformation[43],

– 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[44],

– having regard to its resolution of 23 November 2022 on recognising the Russian Federation as a state sponsor of terrorism[45],

– having regard to its resolution of 9 March 2022 on foreign interference in all democratic processes in the European Union, including disinformation[46],

– having regard to its resolution of 8 March 2022 on the shrinking space for civil society in Europe[47],

– 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[48],

---

37 Texts adopted, P10_TA(2025)0090.
38 OJ C, C/2025/2147, 23.4.2025, ELI: http://data.europa.eu/eli/C/2025/2147/oj.
39 OJ C, C/2026/2114, 29.4.2026, ELI: http://data.europa.eu/eli/C/2026/2114/oj.
40 OJ C, C/2024/4011, 17.7.2024, ELI: http://data.europa.eu/eli/C/2024/4011/oj.
41 OJ C, C/2026/1664, 22.4.2026, ELI: http://data.europa.eu/eli/C/2026/1664/oj.
42 Texts adopted, P10_TA(2026)0015.
43 OJ C, C/2023/1226, 21.12.2023, ELI: http://data.europa.eu/eli/C/2023/1226/oj.
44 OJ C 177, 17.5.2023, p 109.
45 OJ C 167, 11.5.2023, p. 18.
46 OJ C 347, 9.9.2022, p. 61.
47 OJ C 347, 9.9.2022, p. 2.
48 OJ C 184, 5.5.2022, p. 71.

– having regard to its resolution of 23 November 2016 on EU strategic communication to counteract propaganda against it by third parties[49],

– 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[50],

– 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[51],

– 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[52],

– 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),

– having regard to the Commission communication of 3 June 2026 on European Tech Sovereignty, accompanied by an EU Open Source Strategy (COM(2026)0503),

– having regard to the Commission communication of 3 June 2026 entitled 'Strategic Roadmap for Digitalisation and AI in the Energy Sector' (COM(2026)0501),

– 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),

---

49 OJ C 224, 27.6.2018, p. 58.
50 OJ C, C/2024/494, 23.1.2024, ELI: http://data.europa.eu/eli/C/2024/494/oj.
51 OJ C 167, 11.5.2023, p. 105.
52 OJ C 23, 21.1.2021, p. 152.

– 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 National Security Strategy of the United States of America of November 2025, and to the US National Defense Strategy of January 2026,

– 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 preliminary findings of the Commission, announced on 6 February 2026, regarding TikTok’s failure to comply with the Digital Services Act with regard to risk assessments in relation to its recommender systems and addictive design features,

– having regard to the Code of Conduct on Disinformation (established as the Code of Practice on Disinformation in 2018 and strengthened in 2022) endorsed by the European Commission and the European Board for Digital Services on 13 February 2025 as a code of conduct under Article 45 of the Digital Services Act, with the conversion taking effect from 1 July 2025,

– 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[53],

– 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[54],

---

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

54 OJ L, 2023/2836, 20.12.2023, ELI: http://data.europa.eu/eli/reco/2023/2836/oj.

– 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[55],

– having regard to Council Decision (CFSP) 2023/855 of 24 April 2023 on a European Union Partnership Mission in Moldova (EUPM Moldova)[56] ,

– 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[57],

– 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,

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

---

55 OJ C 20, 20.1.2023, p. 1.
56 OJ L 110, 25.4.2023, p. 30, ELI: http://data.europa.eu/eli/dec/2023/855/oj.
57 OJ L 207, 11.6.2021, p. 1, ELI: http://data.europa.eu/eli/agree_interinstit/2021/611/oj.

– 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[58],

– having regard to Parliament's Eurobarometer autumn 2025 survey published in February 2026, outlining public concerns about security risks,

– having regard to the Commission's Special Eurobarometer 568: Protecting and Promoting Democracy, published in May 2025,

– 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 2024 report of the Council of Europe entitled 'Press Freedom in Europe: Time to Turn the Tide – Annual assessment of press freedom in Europe by the partner organisations of the Safety of Journalists Platform',

– 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 the European Union Agency for Law Enforcement Cooperation (Europol) entitled 'EU Serious and Organised Crime Threat Assessment – The changing DNA of serious and organised crime' (EU-SOCTA report), published in 2025,

---

58 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.

– 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 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 US Federal Bureau of Investigation (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 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 2025', published in February 2026,

– 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 Commission press release of 18 December 2023 on its opening of formal proceedings under the Digital Services Act against X to assess possible breaches of its obligations, in particular as regards the mitigation of systemic risks linked to the design and functioning of its recommender systems, as well as obligations related to risk assessment, content moderation, advertising transparency and access to data for researchers,

– having regard to a range of academic and investigative studies on social media recommender systems in the context of the German federal elections, which indicate algorithmic bias and the amplification of polarising or partisan content, thereby shaping users' political information environment,

– having regard to the Commission press release of 30 April 2024 on its opening of formal proceedings under the Digital Services Act against Meta platforms, in particular as regards its handling of political content on its online platforms,

– 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 because of unregulated and remote-control capabilities of PV inverters from high-risk, non-European manufacturers,

– having regard to the White Paper for European Defence – Readiness 2030 presented on 19 March 2025 and Council Regulation (EU) 2025/1106 of 27 May 2025 establishing the Security Action for Europe (SAFE) through the Reinforcement of the European

Defence Industry Instrument[59],

– having regard to the Council presidency conclusions of 28 November 2025 on access to reliable news as part of the European Democracy Shield,

– having regard to Rules 55 and 213 of its Rules of Procedure,

– having regard to the report of the Special Committee on the European Democracy Shield (A10-0199/2026),

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; whereas this initiative provides a unique opportunity to build an effective, whole-of-society approach to the protection of European democracy, freedom and prosperity; whereas democratic resilience and European security are increasingly inseparable;

B. whereas poverty, socio-economic deprivation and marginalisation can leave certain segments of society particularly exposed and vulnerable to external interference and hostile information operations;

C. whereas the threat posed by Russia to Europe's security and democratic integrity remains at unprecedented levels; whereas other actors, including China and Iran, also pose significant challenges; whereas it is necessary to adopt a principle of information deterrence and, where appropriate, apply restrictive measures against actors responsible for foreign information manipulation and interference (FIMI);

D. whereas the joint communication on the European Democracy Shield contains several positive recommendations and proposals, such as the establishment of an European Centre for Democratic Resilience, the extension of its scope to accession countries and the EU neighbourhood and the full enforcement of key EU legislation; whereas both of 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 similar to the proposed European Centre for Democratic Resilience to counter FIMI and disinformation; whereas such a structure should not duplicate existing tools, capabilities and competences, but instead consolidate them into a single entity with a clear vision and mandate, real powers and financing;

E. whereas recent EEAS reports on FIMI attacks 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 Member States and the EU to anticipate, prevent, detect and take timely, coordinated countermeasures; whereas national and European elections are the principal focus of hostile information manipulation campaigns and other forms of malign attacks; whereas these campaigns disparage particular candidates or political parties, attempt to discredit the electoral process itself, instrumentalise divisive issues and attempt to discredit traditional media; whereas EU

---

59 OJ L, 2025/1106, 28.5.2025, ELI: http://data.europa.eu/eli/reg/2025/1106/oj.

and Member States' institutions are also intensively attacked; 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 or functioning transnational or European cooperation mechanisms linking operational response to threat intelligence;

F. whereas ECNE, the Rapid Alert System 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 that connect national operational capacities to EU-level coordination;

G. 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 and democratic processes in its Member States; whereas, ultimately, European citizens are the primary victims of these practices, as their access to reliable information and their capacity to form independent opinions and to participate meaningfully in democratic life are directly weakened, while public security and societal stability are also put at risk;

H. whereas some 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, which have adopted a fact-based, technical and non-partisan approach; whereas these institutions contribute valuable insights on request or on their own initiative but are not appropriately interlinked;

I. whereas the rapid advancement of artificial intelligence (AI) and deepfake technologies is outpacing the adaptive capacity of fragmented national institutions and making old-school solutions, such as transparency or best efforts obligations obsolete; whereas without coordinated EU responses and clear operational and research capabilities, the technological advantage will increasingly favour attackers over defenders, thus threatening the core basis of our democracies; whereas some AI companies have scaled back, instead of increasing, their safety measures to counter the spread and generation of disinformation through their services; whereas AI facilitates disinformation campaigns but it also provides tools to improve our capacity to detect, analyse and counter them;

J. whereas the principle that industries should contribute financially to addressing externalities related to their activities is well-established in Union law and practice; whereas under the Extended Producer Responsibility framework, certain producers are required to finance the management of the waste generated by their products, in direct application of the polluter-pays principle; whereas under the Single Resolution Mechanism, all banks operating in the banking union make annual contributions to the Single Resolution Fund so that the systemic risks related to their activities do not fall on taxpayers; whereas pharmaceutical companies are required to fund post-authorisation safety studies, on the basis that those who profit from placing a product on the market must contribute to monitoring the harms it may cause; whereas this logic should apply

to large information society service providers who benefit from the information ecosystem while simultaneously creating systemic risks to democratic integrity;

K. whereas the EU has, on several occasions, successfully navigated legally contested and emerging policy areas through structured preparatory instruments; whereas notable examples include the 1988 Green Paper on Copyright and the Challenge of Technology, the High-Level Expert Group on Artificial Intelligence, and the pre-legislative consultation process preceding the General Data Protection Regulation[60], among others; whereas FIMI and disinformation present a comparable challenge related to technological, international relations and business models evolving together with societal and legal phenomena while also competing with constitutional considerations; whereas a tailored multidisciplinary preparatory process could be critical for a robust, court-proof legislative framework related to FIMI and disinformation in full respect of Member States' competences and the powers of the EU institutions;

L. 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 and monetisation of divisive content, (f) the use of synthetic content, such as deepfakes and other AI-generated content, (g) recommender systems designed to drive engagement through polarisation and (h) LLM (large language model) grooming and other data poisoning techniques maliciously feeding AI systems with biased, deceptive or false narratives to influence its training; whereas tools to counter these techniques and negative phenomena have been developed but remain widely insufficient;

M. whereas online platforms, through insights into the preferences and vulnerabilities of each individual user, wield greater influence over public discourse than traditional publishers; whereas evidence suggests that platforms' algorithms can be manipulated by their owners and shareholders to prioritise certain political content, thereby distorting the information environment and undermining the possibility of users receiving accurate and pluralistic information; whereas very large online platforms (VLOPs) and very large search engines (VLOSEs) have become de facto gatekeepers of the public space, thereby strongly influencing what information citizens encounter, how it is prioritised, and under what conditions it circulates;

N. whereas the EU and its Member States have recently adopted a set of comprehensive legislative acts to establish a safe and transparent online space, including the Digital Services Act (DSA), the Digital Markets Act (DMA), the Transparency and Targeting of Political Advertising Regulation (TTPA), the European Media Freedom Act (EMFA)

---

60 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

and the Artificial Intelligence Act (AI Act); whereas these acts mark important progress in holding online platforms accountable and protecting democratic processes, increasing transparency, safeguarding freedom of expression, and thus contributing to comprehensive FIMI defences, but their effectiveness depends on full, timely and consistent enforcement, which remains challenging and slow, creating vulnerabilities; whereas structured support for the Member States in this regard is therefore particularly important; whereas the EU and its Member States should also continue to develop non-legislative measures, common approaches and methodologies in order to disrupt FIMI and defend democracy; whereas Parliament plays a strong role in scrutinising and reinforcing the EU's digital legislation, and these efforts should be complemented by regular reviews of Parliament's working methods to ensure effectiveness;

O. whereas evidence demonstrates that the engagement-based recommendation systems of VLOPs, including X, TikTok and Instagram, are structurally driven by attention-based economics to amplify divisive, polarising or misleading content, thereby posing risks to civic discourse and electoral integrity, as evidenced by the amplification of extremist political content during elections across the EU; whereas these systems have undermined the visibility of editorially independent and pluralistic media, and facilitate the rapid spread of AI-generated deepfakes and synthetic or manipulated content, exacerbating the challenge for users, in particular vulnerable groups, of distinguishing between true and false information; whereas the AI Act introduced rules on mandatory labelling of AI-generated content; whereas Articles 34 and 35 DSA require VLOPs to assess and mitigate systemic risks; whereas the DSA also introduced significant new rules to increase algorithmic transparency and accountability, including the option for users to choose non-personalised feeds, thereby reducing reliance on opaque algorithmic curation; whereas challenges within the implementation and user experience remain; whereas effective enforcement of the DSA and the AI Act, supported by up-to-date guidelines and independent oversight, is essential to counter manipulation and safeguard democratic processes;

P. whereas targeted sanctions, threats of tariffs, visa bans, and personal sanctions have been directed by the US administration at EU actors involved in shaping and enforcing the DSA and other digital legislation, undermining the integrity of EU decision-making and the rule of law; whereas the EU, as an open and rules-based single market, must uphold its sovereign right to legislate in line with democratic values, international commitments and the protection of fundamental rights, including freedom of expression, which is a core value shared with the United States and like-minded partners across the democratic world; whereas unfounded allegations of censorship undermine these shared values and divert attention from actual serious free speech violations in countries such as Russia, China or Iran; whereas the enforcement of EU digital legislation must resist delays or limitations resulting from geopolitical considerations, notably in cases involving lobbying by big tech platforms; whereas external pressures, including geoeconomic coercion, strategic acquisitions and support for extremist movements by non-EU public or corporate actors, further threaten the EU's decision-making sovereignty and democratic resilience; whereas the enforcement of the EU's digital rules must remain guided solely by Union law and the protection of democratic interests, free from the undue influence of political, trade or external pressures; whereas unity among the EU Member States and their political alignment in this regard are key;

Q. whereas AI drives innovation, knowledge access, productivity and new digital industries, presenting new opportunities, such as the strengthening of election

management and oversight through the detection of 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, thus requiring timely and effective democratic safeguards and regulatory oversight; whereas credible reports have exposed the operations of a Moscow-based disinformation network known as ‘Pravda’, which has deliberately targeted and infiltrated 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 in order to subtly disseminate false or misleading geopolitical messaging under the guise of authoritative language and undermine democratic discourse and trust in digital technologies; 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 improved AI literacy in education, work and society at large, increased transparency in relation to LLM training, and adequate research funding; whereas AI outputs may reflect biases introduced through the design of the systems;

R. whereas online influencers can play an important role in strengthening the digital resilience of our societies, when raising awareness about media literacy and democratic procedures, promoting fact-based content or contributing to a healthy political debate; whereas, at the same time, a growing share of citizens, especially minors and young adults, rely extensively on content creators and influencers on social media, gaming services and video- and content-sharing services, including for news and current-affairs information, thereby exposing themselves to risks linked to addictive design, harmful content and manipulative practices; whereas online personalities and influencers can have a significant capacity to shape public opinion and information flows without being subject to standards of accountability comparable to those for media;

S. 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 and distort electoral competition; whereas TikTok, one of the most widely used platforms among young voters, claimed to have blocked the creation of over 116 000 spam accounts 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; whereas evidence points to two main operational patterns: the coordinated manipulation of recommendation algorithms through networks of synchronised accounts generating artificial traffic and trend amplification, and the covert instrumentalisation of content creators, and both patterns show how technical platform dynamics can be exploited and can circumvent democratic safeguards;

T. 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, recruitment for sabotage, political propaganda and disinformation relating to EU and national laws; whereas Telegram’s origins in Russia, its opaque ownership structures and its 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 classification as a VLOP under the DSA, making it subject to stricter regulatory obligations and risk-mitigation requirements; whereas the Commission's lengthy assessment has not yet reached a conclusion;

U. 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, satellite communication, cloud services, online platforms, payment solutions and IT software, including in sectors such as defence; whereas fostering home-grown innovation, ensuring fair and competitive digital markets, enforcing the digital rulebook, supporting European start-ups and investing in sovereign digital infrastructure are essential steps towards building a competitive, secure, resilient and independent EU digital ecosystem, while limiting the opportunities for hostile interference, information manipulation and economic coercion; 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; whereas AI is reshaping and accelerating globalisation, creating a new phase of strategic competition; whereas EU digital sovereignty is especially difficult to achieve when VLOPs and VLOSEs operate in a de facto state of oligopoly;

V. 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, which raises 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 to continue to destabilise EU and national information spaces despite regulatory measures; whereas the non-transparent nature of online advertising allows large amounts of money to be funnelled from legitimate brands to disinformation sites, funding polarising content and undermining quality journalism; whereas Meta is the only major tech company to publish limited monetisation data, while others remain non-transparent;

W. 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 that they might ask; whereas in the Netherlands, more than one third of the youngest respondents answered that they were likely to use or might use AI for voting advice; 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; whereas investing in the development of open-source LLMs is one way to reduce concerns about hidden biases, backdoors or data misuse in AI chatbots;

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

persons with inauthentic content;

Y. whereas the fundamental right to freedom of expression and information, as enshrined in Article 19 of the Universal Declaration of Human Rights, as well as 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;

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

AA. whereas authoritarian regimes have used social media platforms to undermine freedom of expression; whereas users expect transparency, due process and the protection of freedom of expression, which must be upheld under the requirements of the DSA; whereas full enforcement of EU digital legislation is therefore necessary to safeguard these principles;

AB. whereas freedom of expression and information, and the freedom and pluralism of the media as enshrined in Article 11(2) of the Charter of Fundamental Rights of the European Union and reflected in Article 10 of the European Convention on Human Rights, are cornerstones of democratic and resilient societies; whereas editorially independent, high-quality, fact-based, well-funded and commercially viable journalism, including that of journalists in exile, is a key safeguard against FIMI and disinformation and an essential tool for informed decision-making;

AC. whereas the term 'information integrity' is regularly used by the EU institutions in policy and operational documents, whereas no official or commonly agreed definition of this concept has been established at EU level; whereas this lack of definition may lead to potential ambiguities in its interpretation and application;

AD. whereas the EMFA represents a milestone in promoting an independent and pluralistic media landscape across Europe; whereas media fulfil a democratic function distinct from that of ordinary commercial entities; whereas robust safeguards are necessary to protect editorial independence, particularly in cases of ownership concentration, takeovers or changes in control, and to ensure transparency, source accountability and professional standards; whereas the Commission should make an effort to better involve candidate countries in the EU's media policy; whereas this should also entail a corresponding commitment from the candidate countries themselves;

AE. whereas the digital advertising ecosystem, while enabling new opportunities for media outreach, has also led to market concentration and unfair competition, with a few large online platforms capturing a disproportionate share of advertising revenue; whereas according to a 2023 report by the French ARCOM and Ministry of Culture, media organisations that invest in news content and audiovisual creation received only 40 % of advertising revenue in 2022, down from 65 % in 2012, and this figure is projected to fall to 29 % by 2030; whereas this is often to the detriment of professional European media companies and the sustainability of independent journalism;

AF. whereas the abusive practices of dominant online advertising market players, such as the practices that resulted in the Commission imposing a EUR 2,95 billion fine against Google for distorting competition in online advertising, underscore the need for more structural measures to ensure fair competition, greater transparency, accountability and safeguards to protect media pluralism, editorial independence and the integrity of democratic processes; whereas structural deficiencies in the digital advertising market can be exploited by malicious actors, as demonstrated by the so-called doppelganger operators using advertisements on social media to target users and by various Russian online campaigns aimed at discouraging Ukrainian men from enlisting;

AG. whereas the DMA is essential for ensuring fair digital markets and media pluralism; whereas challenges remain in its implementation; whereas under the DMA, app developers can inform customers, free of charge, of offers outside app stores; whereas the Commission is investigating a potential DMA breach by Google in demoting media publishers' content; whereas the Commission launched its first review of the DMA on 3 July 2025;

AH. whereas the Audiovisual Media Services Directive regulates audiovisual media services, ensuring consumer protection and fulfilling other public interest objectives in the audiovisual media market; whereas it requires the Member States to take measures to develop media literacy skills and report their efforts every three years; whereas the Commission is currently evaluating the directive and launched a call for contributions in November 2025, in preparation for the renewed assessment scheduled for 2026;

AI. whereas there is a need to equip children with skills to resist disinformation; whereas, in this regard, hostile actors may intensify the targeting of educational systems in order to counter efforts to increase digital literacy; whereas, for different reasons, certain groups are particularly vulnerable to misinformation, including children and young people because of their high digital exposure; whereas there is a need to foster media literacy and critical thinking from an early age;

AJ. whereas EDMO plays a crucial role in monitoring and countering disinformation; whereas EDMO's mandate has been extended to continue its important work; whereas the extension of the mandate is not accompanied by a corresponding increase in financial resources, which may limit EDMO's capacity to fulfil its objectives;

AK. whereas the temporary nature of the Media Resilience programme could provide an opportunity to consider new innovative approaches to supporting independent local and regional media;

AL. whereas the Media Freedom Rapid Response documented 1 481 press freedom violations in 2025, affecting 2 377 media-related persons or entities across 36 European countries, encompassing legal, physical and psychological threats as well as various forms of censorship; whereas this figure, while representing a slight decrease compared to the 1 548 violations recorded in 2024, remains at an alarmingly high level and constitutes a significant increase compared to 2023, thereby underscoring the persistent and systemic nature of the threats to media freedom in Europe; whereas the murders of investigative journalists such as Jan Kuciak, Giorgos Karaivaz, Peter R. de Vries and Daphne Caruana Galizia triggered widespread public outrage;

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

AN. 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 US foreign aid policy; whereas a sustainable funding solution needs to be developed for RFE/RL and other independent media outlets that are essential to the strengthening of democratic resilience in neighbouring countries;

AO. 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, doppelganger campaigns, the mass creation of disinformation outlets and coordinated attacks against journalists; whereas any impersonation of existing media amounts to identity theft and should be addressed appropriately by the judicial authorities; whereas AI models must comply with Union copyright law in order to ensure the protection of rightsholders and legal certainty; whereas the news media sector is facing challenges from the growing influence of AI systems, which is affecting public trust, advertising revenue and copyright protection; whereas the developments in generative AI should be discussed in the context of the Commission's upcoming review of the EU Copyright Directive[61], complemented by a report on the main findings; whereas greater transparency of AI training data is important in the context of media policy;

AP. whereas changes in the United States Agency for International Development (USAID) have affected a number of European media outlets; whereas this highlights the importance of strengthening Europe's own media landscape; whereas EU funding should focus on initiatives with the greatest public impact and include basic operational support;

AQ. whereas measures adopted by the previous Fidesz-led Hungarian Government have led the Commission to open an infringement procedure against Hungary for non-compliance with the EMFA and the Audiovisual Media Services Directive;

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

AS. whereas civil society also plays an essential role in contributing to policymaking, delivering social and community services, raising awareness of important social issues, enhancing resilience, representing diverse groups in vulnerable situations, promoting and protecting the fundamental rights of citizens and ensuring that governments remain

---

61 Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (OJ L 130, 17.5.2019, p. 92, ELI: http://data.europa.eu/eli/dir/2019/790/oj).

transparent and accountable through public scrutiny and democratic oversight;

AT. 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, to 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;

AU. whereas funding for democratic resilience should be strengthened and used in a coordinated and effective manner aiming for maximum impact, while respecting the independence of the entities concerned; whereas the AgoraEU programme, proposed by the Commission for the 2028-2034 multiannual financial framework (MFF), with a proposed budget of EUR 9 billion, constitutes an important step forward in strengthening EU support for culture, media and civil society;

AV. whereas societies that invest effectively in human capital and education are among the most competitive, resilient and economically robust; whereas programmes such as Erasmus+ foster European values and strengthen youth democratic engagement and societal resilience across the EU;

AW. whereas malicious third-country actors have sought to interfere with and exert undue influence over Parliament, including through illicit lobbying and corrupt practices, as evidenced by cases such as the so-called ‘Qatargate’; whereas these developments underscore the need to further strengthen the resilience and integrity of the EU’s decision-making processes;

AX. whereas the French Ministry of the Interior has published a report on the Muslim Brotherhood addressing concerns relating to covert influence activities and entryism; whereas similar concerns have also been raised regarding other religious actors, such as the Russian Orthodox Church (Moscow Patriarchate);

AY. whereas hybrid attacks targeting critical infrastructure in the EU have become more frequent than ever, with incidents linked to the same malicious third-country actors such as Russia, Belarus and China, but also Iran and North Korea; whereas in an increasingly volatile geopolitical environment, the EU must also be prepared for hybrid threats originating from actors other than these; whereas these attacks often target essential systems, networks and facilities that are vital for society’s functioning, including in relation to 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; whereas such attacks demonstrate the need to urgently close vulnerabilities;

AZ. whereas attacks against railway infrastructure endanger the lives and safety of citizens

and compromise strategic logistics networks, as in the unprecedented act of sabotage targeting Polish railway infrastructure on the strategic Warsaw-Lublin route, which was intended to cause a railway disaster and potentially result in multiple fatalities; whereas Russia's military intelligence agency (GRU) has directed a sustained campaign of physical sabotage operations across the EU Member States, including the 2014 explosion at ammunition depots in Vrbětice (Czechia) and the targeting of critical infrastructure in Lithuania by Cuban citizens who had recently been recruited for sabotage operations;

BA. 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; whereas the proposed Digital Networks Act includes binding EU-level resilience obligations for submarine cable operators, including mandatory compliance with security requirements for information and communications technology (ICT) supply chains under the revised Cybersecurity Act (CSA), as proposed; whereas Finland is leading the establishment of a new Baltic Sea maritime surveillance centre, together with Baltic allies and the Commission, with the aim of protecting critical undersea infrastructure; whereas the presence of Russian ships in Irish waters has increased noticeably since the beginning of Russia's full-scale invasion of Ukraine in 2022, raising concerns about the security of the important interconnector cables running between Ireland and the UK;

BB. whereas the protection of key maritime choke points contributes to democratic resilience, as hybrid attacks against such nodes can result in severe economic, social and security disruption; whereas Chinese companies with strong ties to the Chinese Communist Party now hold stakes in more than 30 European naval port terminals, often in close proximity to European military naval bases; whereas in the joint White Paper on European Defence Readiness 2030, the Commission and the Vice-President of the Commission / High Representative of the Union for Foreign Affairs and Security Policy committed to reviewing existing EU legislation and introducing stricter rules on the ownership and control of critical transport infrastructure;

BC. 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, including 'smuggling balloons' used for cross-border illicit activities, remain under investigation but are widely suspected of forming part of the same pattern of hybrid intimidation and destabilisation directed at Europe;

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

BE. 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 and European strategic autonomy;

BF. whereas the EU remains heavily dependent on US technology and financial services, exposing European data and digital infrastructure to risks stemming from US legal frameworks such as the CLOUD Act, the Foreign Intelligence Surveillance Act and the Patriot Act, which grant US authorities broad access to data held by US companies, even when stored in the EU; whereas the Commission adopted the EU-US Data Privacy Framework in July 2023, allowing the free flow of personal data between the EU and the United States under adequate protection rules and providing a mechanism for EU individuals to access an independent and impartial redress mechanism in relation to the collection and use of their data by US intelligence agencies; whereas Microsoft itself has admitted to the French Senate that it cannot protect EU data from US surveillance;

BG. whereas Spain has awarded Huawei a contract to manage and store judicially authorised wiretaps used by both law enforcement and intelligence services; whereas the Commission has restricted Huawei from 5G networks across the EU because of security concerns;

BH. whereas all US federal government agencies are subject to 'buy American' requirements, which prioritise the purchase of US-made products; whereas the EU procurement framework is different and may, in some cases, contribute to dependencies on non-EU products and related risks for European businesses; whereas despite reasonable European alternatives being available in many cases, the European Parliament and the other EU institutions continue to purchase software and hardware products made outside Europe;

BI. whereas on 20 January 2026, the Commission presented a revised CSA, proposing binding requirements for managing ICT supply chain security in critical infrastructure through systematic risk assessments and restrictions on high-risk vendors from countries that pose elevated security risks; whereas this new framework moves beyond the voluntary 2020 5G security toolbox by proposing mandatory compliance obligations on the Member States; whereas the revised CSA, as proposed, could significantly expand ENISA's operational mandate and budget by more than 80 % to include real-time cyber incident coordination, early warning systems and threat intelligence sharing across the Member States;

BJ. whereas the Digital Networks Act proposed by the Commission on 21 January 2026 establishes EU-level oversight of spectrum allocation, including in relation to satellite service providers, prescribing withdrawal of the right to provide networks and services in cases where the provider is not complying with the ICT supply chain security requirements of the revised CSA, as proposed; whereas among other critical infrastructure, electoral infrastructure increasingly depends on digital networks and diverse communication pathways to avoid single points of failure;

BK. whereas fossil-free energy is a crucial stepping stone for Europe's energy sovereignty; whereas according to analysis published in 2025 by Wood Mackenzie, 9 of the 10 largest global solar inverter suppliers were based in China; whereas hidden communication devices have been discovered in Chinese-made solar power inverters used in Europe and the United States; whereas according to the Czech cybersecurity

office, there are risks regarding data protection and, in extreme cases, remote manipulation of solar inverters; whereas solar power plants interconnected through a decentralised dense network are susceptible to cyberattacks and therefore require adequate cybersecurity safeguards;

BL. whereas hybrid attacks represent a recognised security threat facing the EU and its Member States, with a significant impact on democracy; whereas internal security remains a responsibility of the Member States but the cross-border, interconnected and multi-dimensional nature of those attacks requires strengthened cooperation, systematic information-sharing and coordinated action at EU level, supported by adequate funding; whereas the European internal security strategy of April 2025 underlines that EU criminal law already covers certain forms of FIMI and disinformation activities and that reinforced EU cooperation can contribute to countering that type of conduct more effectively; whereas criminal law tools can contribute to the European Democracy Shield to the extent that the activities concerned constitute criminal offences in accordance with applicable law;

BM. whereas judicial and police cooperation mechanisms and cross-border information exchange tools need to be adjusted and strengthened, in the light of the growing challenges posed by foreign interference to the EU's internal security; whereas new strategies developed by terrorist and criminal organisations are increasingly exploited for running and financing foreign interference operations, including the use of crypto assets and communication via various digital channels, including video games or e-shops, to circumvent sanctions and transfer money illegally; whereas as a consequence, there is a need to provide adequate training for criminal justice and law enforcement authorities on modern investigative methods and technologies and on the entire value chain of manipulation and interference, to ensure that they can properly collect, process, store and use evidence in criminal proceedings; whereas transfers of personal data to third countries or international organisations that are necessary for the purpose of police, criminal justice or border management cooperation are subject to specific conditions under Union law and should only take place when the integrity and security of those data can be ensured;

BN. whereas Europol has warned, in its latest EU-SOCTA report, published in March 2025, about the involvement of criminal organisations in hybrid attacks, including disinformation 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 its mandate as regards new security threats, notably sabotage, hybrid threats and information manipulation; whereas the joint communication on the European Democracy Shield announced that the revision of the mandates of both Europol and the European Union Agency for Criminal Justice Cooperation (Eurojust) would explore ways to further enhance efforts to counter FIMI and disinformation activities;

BO. whereas the Commission has committed to launching a reform that will make Europol a truly operational police agency; whereas law enforcement officers are privileged witnesses of the destabilising effects that FIMI and disinformation campaigns can have on the communities concerned; whereas they can therefore be key partners in safeguarding democratic institutions; whereas the legal, professional and ethical framework required for the performance of this role should be better defined and further harmonised throughout the EU;

BP. whereas Eurojust may be requested by the Member States to assist national authorities in dealing with any type of illegal conduct under their jurisdiction; whereas judicial cooperation can prove particularly challenging when expanding to new criminal areas, requiring a modernised legal toolbox;

BQ. whereas the situation at the external borders of the Member States with Russia and Belarus remains of concern because of persistent hybrid threats; whereas EU justice and home affairs agencies have a key role to play, in cooperation with national authorities, in establishing and maintaining common situational awareness of risks related to such threats and in assisting front-line Member States in crisis situations; whereas the Commission has included the strengthening of the European Border and Coast Guard Agency (Frontex) in its flagship initiatives for the 2024-2029 legislative term; whereas other initiatives such as the Eastern Flank Watch may contribute to strengthening the protection of the external borders and enhancing resilience to hybrid threats;

BR. whereas transnational repression includes systematic intimidation and harassment by third-country authorities, or their proxies, targeting journalists and activists, human rights defenders, political opponents and members of diaspora communities residing in the EU, such as in the case of Russian-led legal harassment against Ukrainian journalists, Turkish and Azerbaijani attempts at silencing opposition, and attacks planned against the Belarusian diaspora in Lithuania; whereas the growing surveillance of human rights defenders should be considered a form of transnational repression; whereas such practices not only violate the safety and fundamental rights of those targeted, but also undermine EU and Member States' sovereignty and security, democratic freedoms and the rule of law; whereas victims of transnational repression in the EU should continue to receive protection;

BS. whereas candidate countries and EU neighbourhood countries, notably Ukraine, Moldova, Armenia, Georgia and the Western Balkans countries, remain acutely targeted by FIMI and hybrid threats; whereas the Republic of Moldova, in particular, is facing persistent, coordinated and state-sponsored disinformation campaigns aimed at undermining democratic institutions, electoral integrity and its path to EU accession; whereas these countries require EU support to build civic and institutional resilience and to fight FIMI and hybrid threats, including through the financial support mechanisms of the Ukraine Facility, the Reform and Growth Facility for the Western Balkans, and the Reform and Growth Facility for Moldova; whereas the EU should take into account the feedback and experience of these countries, as they have been facing Russian hybrid attacks for many years; whereas the effectiveness of the EU's efforts to strengthen institutional resilience in candidate countries depends on their willingness to adopt relevant measures, implement necessary reforms and cooperate effectively;

BT. 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 Partnership countries and the Global South; whereas various sources reveal that Russia's annual budget for spreading disinformation and propaganda amounts to several billion euro; whereas Russia's disinformation warfare has not been matched by the EU with adequate financing or effective strategy; 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 European 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;

BU. whereas operations to manipulate information have already been detected against three candidates for France's 2027 presidential election and have been attributed to Russia;

BV. whereas Russia's war of aggression against Ukraine, as well as its broader hybrid warfare against Europe and interference in the democratic processes of other countries, has been enabled and justified by the nationalist imperialist ideology of 'Ruscism', and forms part of a wider strategy directed against the West and its interests and values, including the international rules-based order, the rule of law, democracy, human rights and common security; whereas Parliament has condemned the ideology, policies and practices of the current Russian regime as incompatible with international law and EU values;

BW. whereas Russia employed a multilayered hybrid interference campaign to disrupt Moldova's 2024 and 2025 elections, combining disinformation, financial manipulation, cyberattacks and proxy networks; whereas Russia invested massively in those attempts, which failed thanks to the efficacy of Moldova's defensive policies and the support provided by the EU; whereas the EU Partnership Mission (EUPM) in the Republic of Moldova was established on 24 April 2023 with the explicit purpose of supporting the Moldovan authorities in combating FIMI;

BX. whereas parliamentary elections were held in Armenia on 7 June 2026 following a period of intensified Russian interference, including through leveraging certain religious actors and the international diaspora to undermine Armenian democratic institutions, derail peace talks with Azerbaijan and reassert Russian influence; whereas according to Armenia's 2026 annual report on external security risks, foreign actors are activating their agents within Armenia;

BY. whereas Serbia has become a key hub for disinformation and a proxy for Russian and, to a lesser extent, Chinese influence operations; whereas in 2024, according to Moldova's court rulings, Serbia and Bosnia's Republika Srpska hosted a Russia-linked militant training camp that recruited and trained agitators to create mass disorder during Moldova's elections and referendum; whereas Serbian cyber infrastructure was used to launch sophisticated spear-phishing attacks impersonating the Belgrade Security Conference and targeting EU and NATO officials and diplomats; whereas Serbia has become a safe haven for Russian spies and oligarchs who monitor Russian opposition figures and find ways to evade sanctions; whereas Serbian citizens, allegedly connected to Russia, have been arrested for carrying out hate-motivated acts in France and Germany, including defacing Jewish sites to sow ethnic and religious discord;

BZ. whereas the concerning reduction in US support for international democracy through the withdrawal from key multilateral and international frameworks has created a substantial global gap in funding, including for countering disinformation and authoritarian influence;

CA. whereas the US National Security Strategy and National Defense Strategy reflect a shift in long-standing US foreign policy, marked, among other indicators, by the explicit focus of US interests in the Western hemisphere and the downplaying of the threat posed by Russia and China; whereas the National Security Strategy also includes critical

references to alleged democratic shortcomings in certain EU Member States and announces actions akin to foreign interference; whereas the strategy frames global developments largely in terms of economic nationalism and strategic interests, revealing a more transactional approach to traditional allies and thus questioning the principles that have underpinned US foreign policy for decades;

CB. whereas China employs more sophisticated methods compared to other actors to gain influence in the EU, including through co-opting political elites, luring former officials with lucrative jobs, and building extensive networks of students, researchers and business operatives who then push pro-Chinese narratives and policies; whereas such methods also extend to coordinated information manipulation and disinformation activities in third countries, as illustrated by reports by a bipartisan US commission that China conducted a disinformation campaign to discredit French Rafale fighter jets used by India against Chinese weapons in the 2025 India-Pakistan conflict;

CC. whereas international initiatives, including those by the UN, the Organisation for Economic Co-operation and Development, the Council of Europe, like-minded countries in East Asia including Japan, South Korea and Taiwan, and the G7, have begun to outline principles and frameworks for safeguarding information integrity, anchored in democratic values, media pluralism and human rights;

CD. whereas FIMI campaigns and activities may also arise from actors within the EU, including Member States; whereas the credibility of democratic institutions also depends on their respective governments refraining from disseminating inaccurate, misleading or politically instrumentalised information, particularly during natural disasters, health emergencies and humanitarian crises; whereas the acceptance of remunerated positions or advisory roles by former high-ranking officials of EU Member States and the EU institutions or other forms of cooperation with authoritarian third-country regimes, or their state-controlled enterprises, risks undermining the credibility of the EU and the independence of its decision-making process;

CE. whereas the phenomenon of information manipulation and interference in the domestic context, as well as its impact, should be further examined and understood, particularly in its interaction with FIMI; whereas 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, digital and AI literacy levels across all age groups; whereas effectively disrupting and countering information manipulation activities requires a whole-of-society approach across sectors;

CF. 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 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;

CG. whereas FIMI in electoral contexts often follows recurring patterns, including efforts to discredit candidates or political actors, erode trust in electoral processes and exploit societal divisions; whereas efforts to ensure election integrity must take a holistic approach;

CH. whereas 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;

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

CJ. 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 and other forms of FIMI operations, not least in the light of the large-scale cyberattacks that targeted the Romanian electoral authorities in autumn 2024; whereas the ENISA annual activity report for 2019 already recommended the classification of election systems, processes and infrastructures as critical infrastructure so that the necessary cybersecurity measures would be put in place;

CK. whereas several reports and investigations, including findings related to doppelganger campaigns impersonating established media outlets, suggest that it is likely that Russia interfered in the 2025 German federal elections by targeting pro-European political parties; whereas it is also possible that other third country actors engaged in interference activities in relation to the same electoral process, as part of a broader pattern of interference observed in multiple European countries;

CL. whereas the covert funding of political parties and movements in the EU by non-EU countries, as evidenced by existing documented instances of foreign interference by authoritarian regimes through direct or indirect financing of political parties, foundations or affiliated media organisations, poses a threat to democratic resilience, electoral integrity and the legitimacy of the democratic process;

CM. whereas Parliament has been the target of espionage and foreign interference, including the conviction of an assistant to former Member of the European Parliament (MEP) Maximilian Krah, a member of the Alternative für Deutschland (AfD), for spying on behalf of China; whereas MEPs and their staff have access to sensitive information and documents within Parliament;

CN. 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;

CO. whereas since 2022, the EU has imposed a total of 21 packages of extensive and unprecedented sanctions in response to Russia's military aggression against Ukraine; whereas those sanctions are aimed at substantially increasing pressure on the Russian war economy by 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; whereas the efficacy of such measures should be strengthened and loopholes allowing for their circumvention should be closed;

CP. whereas since 8 October 2024, the EU sanctions framework has been expanded to enable 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 migration, 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 this sanctions regime now allows 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;

CQ. whereas retaliatory measures including arrest warrants and in-absentia proceedings are commonly used by the Moscow regime against foreign nationals located abroad who are blamed for criticising its policies or resisting its influence; whereas on 28 December 2024, the Russian Government announced that it had ‘significantly expanded’ its blacklist of EU citizens and officials, including representatives of the 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 and false legal accusations, often without any formal notification, justification or right of appeal; whereas such coercion follows a pattern of escalation, beginning with administrative exclusion, progressing to online harassment and culminating in physical threats, surveillance, the intimidation of family members or even violent attacks; whereas the threat of being blacklisted alone may lead EU officials to self-censor in anticipation and to refrain from taking political positions; whereas the Moscow regime in parallel maintains lists of Russian citizens living outside Russia as a means of transnational repression;

CR. whereas the Russian blacklist should be recognised as an instrument of hybrid warfare and foreign coercion; whereas an adequate response from the EU should include enhanced intelligence-sharing, as well as targeted sanctions, such as asset freezes and travel bans on foreign officials, handlers and financial facilitators who are responsible for coercive practices, and disruption of the financial and logistical networks enabling these operations, including cryptocurrency channels;

CS. whereas the EU has adopted an Anti-Coercion Instrument to protect itself and its Member States from economic coercion by third countries;

CT. 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, institutions 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 well as threatening the future of the whole of Europe, as has been seen throughout Russia’s aggression against Ukraine;

CU. whereas effective civilian and defence preparedness requires a comprehensive, whole-of-society, whole-of-government and all-hazards approach that facilitates the

cooperation and integration of the national authorities of the Member States with the EU institutions, bodies, offices and agencies, as well as businesses, academia, civil society and individual citizens; whereas the European Democracy Shield is a unique opportunity to establish this approach; whereas this effort needs to be accompanied by long-term investment that realistically matches the scale of the challenge, as well as effective coordinated deployment of funds, strategic foresight and the embedding of resilience into policymaking, infrastructure development, education systems and supply chains; whereas EU defence and preparedness initiatives should be aligned and work in synergy;

CV. whereas empowering citizens through knowledge, education, media and digital literacy, critical thinking and access to reliable information is key to societal resilience, ensuring that all citizens can anticipate risks, recognise manipulation, respond appropriately during emergencies and actively contribute to the collective resilience of democratic societies; whereas terrestrial broadcast radio is present across the EU and provides a reliable and stable means to inform citizens in the event of human-induced or natural disasters, particularly outages of the internet and other communication tools; whereas 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 for people of all ages and social backgrounds;

CW. whereas civil-military cooperation, dual-use capabilities and the integration of preparedness into educational programmes, along with practical skills and knowledge in the field of civil defence, 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; whereas there is a need to promote civic responsibility, threat awareness and an understanding of the role of citizens in ensuring security;

CX. 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; whereas European telecommunications companies have been targets of cyberespionage, as confirmed by the recent examples attributed to China-linked group Salt Typhoon; whereas the telecommunications sector, as a cornerstone of these ecosystems, requires robust cybersecurity and resilience measures to remain secure and operational;

CY. whereas preparedness depends on seamless cooperation between the EU institutions, agencies, Member States and like-minded international partners, supported by joint exercises and training, shared situational awareness platforms and rapid information exchange; whereas Taiwan, a leading partner in terms of situational awareness, has been organising extensive civil defence and resilience exercises aiming to combat China’s increasing grey-zone warfare tactics, complementing its military drills; whereas Taiwan’s whole-of-society approach and best practice can contribute to developing the concept of preparedness in the EU, and strengthening shared situational awareness, early-warning capacities and the overall effectiveness of the European Democracy Shield;

CZ. 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, particularly in the digital field;

whereas this effort requires the exploration of new targeted funding mechanisms;

Introduction

1. Welcomes the joint communication on the 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 amid an ever-evolving threat landscape and ultimately contribute to safeguarding the values enshrined in Article 2 TEU; takes the view that the measures set out in the communication do not fully reflect the level of ambition, foresight and capacity required and should be further developed and progressively strengthened over time, with a view to ensuring the effective establishment of robust and binding actions to protect democracy, in line with the scale of the challenges identified, while respecting the EU's Treaty-based division of powers; stresses that soft policy measures are often insufficient where democratic values are deliberately undermined and that the fight against foreign interference, hybrid threats and disinformation requires ambition and strong action; takes the position that the credibility of the European Democracy Shield also depends on the will and determination to enforce existing EU legislation of relevance to the defence of democracy; recalls, furthermore, that the fragmentation of the EU remains a vulnerability in the defence of democracy;

2. Notes with concern the increasingly complex and evolving threat landscape undermining democratic processes and institutions in the EU and its Member States, characterised by FIMI, hybrid attacks and disinformation campaigns conducted by malicious third-country actors and their proxies in the EU; stresses that hybrid warfare goes beyond cyber or information attacks alone, and encompasses the economic, technological and societal dimensions of strategic confrontation; underlines that this reality is shared by many of the EU's like-minded partners in its neighbourhood and worldwide;

3. Emphasises that social cohesion and trust in public institutions constitute cornerstones of democratic resilience; stresses that weaknesses in the rule of law, notably in areas such as judicial independence, media pluralism and the effectiveness of anti-corruption frameworks, risk undermining public confidence and being instrumentalised by both internal and external actors with a view to weakening democratic consensus and exacerbating societal polarisation; highlights the need for a comprehensive approach aimed at addressing concerns relating to the rule of law and reinforcing social cohesion, democratic legitimacy and societal trust across the EU and its Member States; further recalls that strengthening the rule of law in candidate countries is key to supporting their alignment with EU values and enhancing overall European democratic resilience;

4. Considers Russia to be the primary external threat to Europe's security and democratic integrity and reiterates its view that Russia is a state sponsor of terrorism; underlines the need for a comprehensive and forward-looking strategy to safeguard European democracy;

5. Insists 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 media and investigative journalism – must be sufficiently funded in the upcoming MFF;

underscores that investment in democratic resilience is crucial for EU security, sovereignty and prosperity; expresses its support for the Commission's commitment to mainstreaming democratic resilience across EU funding programmes; underlines, in that context, the need for various aspects of hybrid defence to be integrated into EU defence initiatives; stresses, however, that clear goals with measurable actions and outcomes are needed to use EU and national resources effectively and avoid waste or fragmented funding;

6. Condemns third-country interference in certain outermost regions and overseas countries and territories, where the impact may be further compounded by their isolation and geographical distance from the European continent;

European Centre for Democratic Resilience

7. 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 fully operational in the course of 2026; notes, however, the lack of clarity regarding the timeline and concrete milestones for the progressive roll-out of the Centre, as the reference to a 'gradual' implementation based on the voluntary participation of Member States does not provide sufficient predictability, accountability or operational certainty; welcomes the Commission's commitment to regularly updating and involving Parliament in the process of implementing the European Democracy Shield and the Centre;

8. Regrets, however, that the Centre, as set out in the proposal, lacks a clear mandate and empowerment through a legal act, as well as dedicated budgetary resources and personnel, a specific governance structure 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; stresses that the Centre should add value beyond existing structures and not become another hub, network, platform or framework among others, thus further reducing the EU's capacity to make efficient use of the full spectrum of tools available at present by duplicating work, increasing institutional ambiguity, exacerbating fragmentation and stretching budgets; firmly believes that the Centre should serve as an aggregator and consolidator of existing EU-level action by assisting, extending, complementing and, whenever feasible, coordinating national actions;

9. 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 that 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 the end of 2026 to be set as the deadline for this integration; calls for the integration to include operational responsibility for an enhanced Rapid Alert System with a capacity to address information manipulation in real time, the deployment and operation of a

unified FIMI intelligence database, thus further developing the EUvsDisinfo resource, including by mapping platforms used to spread FIMI and disinformation, ECNE, and the Commission's Task Force on Disinformation and Strategic Communication, among others; calls on the Commission to ensure that the Centre has the capacity to assess coordinated attacks on information integrity; emphasises that the Centre must be equipped to trace, monitor and respond to foreign interference and hybrid threats, while ensuring all affiliated organisations remain independent, particularly of big tech;

10. 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 propose as a next step a legal act for the establishment of the Centre as a structurally autonomous 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; considers that the establishment of the Centre as a permanent structure by a legal act would represent a qualitative shift from fragmented coordination towards a more integrated, operational and strategic EU-level capacity; stresses that, to ensure coherent and timely action across the EU in view of rapidly changing realities, there should be an ambitious timeline for the establishment of the Centre by a legal act;

11. Calls for the governance of the Centre to include representatives of each Member State; notes that the voluntary nature of Member State participation, as proposed in the Commission's communication, risks perpetuating an inefficient and fragmented architecture with different levels of protection and responses to common threats faced across the EU; notes that a lack of governance with representation from all Member States risks an architecture that operates on the basis of a lowest common denominator;

12. Stresses that enhanced EU-level action to protect democracy must be accompanied by strong democratic oversight; calls on the Commission to report regularly to Parliament on the activities of the Centre, including its budgetary, operational and strategic dimensions; stresses that the Centre's governance should include representatives of the European Parliament, strengthening its democratic legitimacy;

13. Calls on the Commission to endow the Centre with a clear mandate, decision-making mechanisms and competence to act, thus allowing it to function as an independent centre of excellence for detecting, analysing and combating FIMI and disinformation operations, as a capability-building platform contributing to the establishment of common definitions, standards, training and technical tools across the EU, and as an operational backbone translating threat analysis and early warning into concrete, timely and evidence-based operational output and providing real-time coordination of technical support in countering active information manipulation campaigns, in close cooperation with national authorities and the relevant EU bodies; stresses the need for the Centre to have the capacity to act swiftly in crisis situations, particularly in the run-up to and during elections, in order to translate situational awareness into effective action; notes that the interference tactics of malign actors will evolve over time alongside technological progress and the Centre's mandate should provide flexibility to enable it to address new challenges; stresses that the Centre must have a stable, multidisciplinary staff that includes FIMI analysts, open-source intelligence (OSINT) experts, and cybersecurity and financial tracking specialists, and must be authorised to coordinate cross-border task forces with the competent authorities of the Member States;

14. Calls on the Commission to ensure that the Centre's analytical and monitoring capacity is formally structured as a source of independent expert input into the systemic risk assessment processes established under the DSA, including with Digital Services Coordinators in each Member State, and under the EMFA, the TTPA and the Artificial Intelligence Act, by cooperating on the collection, preservation and analysis of evidence related to FIMI and disinformation, feeding directly into enforcement actions and by providing timely threat-intelligence reports, FIMI-pattern analyses and democracy-risk indicators, among others; stresses that the Centre's role in these processes must remain advisory and analytical, so as to preserve the independence of regulatory decision-making; stresses that, where FIMI and disinformation activities undermine EU law, the Centre's coordination role should ensure a direct link to bodies that have the power to initiate investigations and judicial proceedings; calls for relevant findings on systemic shortcomings or recurring vulnerabilities to be duly considered and reflected in the Commission's annual rule of law report in dedicated subsections addressing disinformation and media integrity under the media pluralism and freedom pillar, and addressing electoral integrity and safeguards against undue influence under the checks and balances pillar; notes that the Centre could also contribute to the training of Digital Services Coordinators and the staff of national media regulators on the topic of FIMI and disinformation;

15. Welcomes the concept of a stakeholder platform; notes, however, that its purpose, structure and added value remain insufficiently defined, including in relation to existing networks and initiatives; acknowledges the added value of input from civil society in the development of the Centre's mandate; calls on the Commission to ensure that the Centre's coordination encompasses existing efforts by civil society and academia through the proposed platform; insists that the Centre must also provide opportunities for connections and learning between governments and diverse stakeholders across borders;

16. Calls on the Commission to ensure that the Centre's mandate includes responsibility for safeguarding 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 and strengthening electoral integrity; notes that coordinated information manipulation campaigns often target the EU's information space as a whole, thereby justifying a dedicated EU-level operational capacity to protect democratic processes beyond purely national contexts; 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; stresses that working methods and data use must be fully interoperable between existing EU and national structures; underlines, in this respect, the need for common open-source methodologies, and effective collaboration across networks of actors including OSINT researchers, journalists, communicators and policymakers;

17. Calls on those 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 and evaluation process for Member State capacity development; underlines that such a process would provide a basis for gradually raising the level of ambition of the Centre;

18. Calls on the Commission to assess the feasibility of empowering the Centre to administer dedicated EU funding under the present and upcoming MFFs and relevant EU programmes whenever they relate to countering FIMI, strengthening democratic resilience and promoting information integrity; calls on the Commission to avoid programming that disperses and fragments efforts, or that creates unsustainable, temporary, small-scale initiatives, but to focus on coordinated, strategic, scalable efforts that are sustainable for all actors involved;

19. Calls on the Commission to provide sufficient and predictable funding for the Centre and its activities, including sufficient staff and financial resources under the next MFF and a dedicated EU budget line for the Centre's operations, with a clear separation between operational funding and general coordination costs; furthermore, calls on the Commission to secure sufficient human resources and bridge funding from existing budgets to enable preparatory work before the 2028-2034 MFF;

20. Calls on the Commission to assess the feasibility of establishing a financing mechanism to complement the dedicated budget line for the Centre's operations; takes the position that such a mechanism should include within its contributors large information society service providers whose activities represent a systemic risk to democratic integrity; stresses that any such mechanism must be accompanied by the strongest possible guarantees of independence and the total absence of conflicts of interest;

Digital resilience

21. Calls for the full implementation and effective enforcement of the entire digital-related EU *acquis*, including key legislation such as the DSA, the DMA, the TTPA, the AI Act and the EMFA, across all Member States and in full respect of fundamental rights; stresses that rigorous, consistent, systematic and timely enforcement is an essential pillar of European digital sovereignty and deterrence, and must be a precondition for operating in the single market; urges the Commission to report regularly on the enforcement and application of EU law, notably the DSA, avoid excessive delays in investigations, and impose strong sanctions for persistent breaches by VLOPs and VLOSEs; takes the position that the continued implementation of digital legislation should have a strengthened focus on countering FIMI and online disinformation, ensuring information integrity and protecting democratic discourse during and outside election periods;

22. Expresses serious concern that the engagement-based recommendation systems of certain VLOPs often cause systemic risk to civic discourse and electoral processes, as they amplify divisive, polarising or misleading content, often fuelling disinformation from foreign and domestic actors, while disproportionately favouring sensationalist material over fact-based content; recalls that Articles 34 and 35 DSA oblige VLOPs to assess and mitigate such risks; maintains that effective risk mitigation measures should also ensure that synthetic or manipulated content, such as deepfakes, can be clearly distinguished from authentic material, and that editorially independent and pluralistic media and verified sources have due prominence; calls on the Commission to investigate compliance with DSA obligations in this regard and take appropriate measures, including imposing interim measures; suggests that such interim measures include the limitation of engagement-based recommender systems that pose systemic risk, where necessary; further calls on the Commission to promote greater transparency and accountability in the design of algorithmic recommendation and advertising

systems, especially together with other algorithmic systems, in order to enhance user choice and ensure non-manipulative default settings, all while promoting freedom of expression and information; reminds VLOPs, in this context, of their obligation to mitigate systemic risks, which may include testing and adapting their algorithmic systems, including their recommender systems, and of their obligation to provide at least one option for each of their recommender systems which is not based on profiling, in line with Articles 35(1)(d) and 38 DSA; further calls on the Commission, in cooperation with the Digital Services Coordinators and with the involvement of independent third parties through public consultations, to ensure that there are up-to-date guidelines for systemic risk mitigation, and to ensure consistent enforcement and a high level of protection against large-scale manipulation;

23. Condemns the targeted sanctions and attempts at coercion by the US administration against EU actors involved in shaping and enforcing the DSA and other digital regulations, in particular against a former commissioner; calls for the immediate lifting of these measures; urges the Commission and the Member States to resist such pressure, uphold EU legislation, and defend the right to self-governance and digital sovereignty; underlines that freedom of expression is a fundamental right in the EU and a core value shared with the United States and like-minded partners across the democratic world; stresses that political and trade considerations, as well as pressure from third countries or large technology companies, should not unduly influence the enforcement of EU digital legislation; stresses that decisions concerning the application of EU digital rules must be guided solely by EU law and the protection of democratic interests, and that the EU, as an open and rules-based single market, retains the sovereign right to regulate its economic activity in line with democratic values and international commitments; calls on the Commission and the Member States to ensure that the protective and redress mechanisms of EU digital legislation are shielded from any interference that could compromise their independence or effectiveness, and to establish robust safeguards against such risks;

24. Calls on the Commission to increase efforts to promote and align the DSA and other key EU digital legislative acts in candidate and potential candidate countries and ensure that these countries have the support, tools and guidance needed for the implementation of such laws, enabling gradual integration into relevant EU enforcement and cooperation mechanisms, where appropriate; stresses that efforts to demonetise disinformation should explicitly include candidate and potential candidate countries, in order to prevent regulatory loopholes and cross-border spillover effects; stresses the need to take particular note of trends observed in candidate and potential candidate countries when conducting election-related work under the Code of Conduct on Disinformation;

25. Notes the official integration of the voluntary Code of Practice on Disinformation into the framework of the DSA as a Code of Conduct on Disinformation, becoming a relevant benchmark for determining DSA compliance regarding disinformation risks, to complement other effective mitigation measures by VLOPs and VLOSEs to address systemic risks to democratic processes; notes that the implications of potential non-compliance with the code vis-à-vis DSA compliance and enforcement could be further clarified; underlines that the code should remain a dynamic instrument that follows the latest trends and that the Commission should continue to oversee the effective implementation by the signatories; considers that the implementation of the DSA should address the coordinated inauthentic use of online platforms, e.g. through bots, fake

accounts, polarising algorithms, and artificial engagement and amplification creating the illusion of public support; considers these phenomena to be among the most serious risks to free, authentic and open discourse online, particularly in election periods; stresses that foreign authoritarian actors, in particular Russia, have developed disinformation playbooks whose effects have become increasingly visible during recent elections across Europe; calls urgently on all VLOPs and VLOSEs operating in the EU to fully adhere to the code, and urges the platform X to rejoin it;

26. Welcomes the Commission's commitment to draw up a DSA incidents and crisis protocol, including clear processes for coordination between relevant authorities, to further address major incidents and interference in the information environment; considers that this protocol should encourage the participation of online platforms and online search engines and 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; stresses the need for platforms to respond quickly and effectively through preventive and corrective measures against such interference, and for the authorities to react swiftly in cases of non-compliance, rather than relying on ex post measures and late enforcement; welcomes, in this context, Google's proactive removal in 2025 of nearly 11 000 YouTube channels and accounts linked to state-backed propaganda from China, Russia, and other malicious actors, and urges all platforms to systematically address such threats;

27. Welcomes 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 , as well as the Commission's decision to start investigations of Grok AI's integration into X and to expand existing investigations into X's recommender systems; urges the Commission to accelerate remaining investigations, including into Meta, particularly in the light of preliminary findings on breaches of transparency and user-protection obligations, and reports indicating persistent issues related to scam advertising and regulatory circumvention; stresses the need for enforcement action in cases of election interference, persistent algorithmic opacity and the large-scale proliferation of fake accounts and bot networks that distort public discourse; calls on the Commission, in this context, to swiftly conclude investigations into TikTok's compliance with the DSA in relation to foreign interference in the 2024 Romanian presidential elections, which highlighted worrying possibilities of recommender systems and bot networks being exploited, and in relation to TikTok's obligation to mitigate systemic risks to democratic processes and to ensure deterrence during electoral periods; further takes note of the Commission's preliminary evaluation indicating that TikTok is in breach of the DSA for its addictive design;

28. Underlines the need for increased transparency regarding actors behind online content and accounts, particularly for advertising purposes; stresses that measures to combat coordinated inauthentic behaviour without abolishing anonymity online are essential to prevent FIMI, bot farms and covert political campaigning; invites the Commission to explore possible measures that would support online platforms in adopting proportionate steps to verify that a human is behind an account, thereby countering the activities of bot accounts; calls on platforms to prioritise the development of effective mechanisms to identify, scrutinise and, where necessary, suspend inauthentic accounts, especially those involved in coordinated influence operations; stresses that measures targeting inauthentic accounts must not undermine the ability to remain anonymous

online, which is essential for protecting journalists, activists, marginalised communities and individuals in vulnerable situations (such as whistle-blowers, dissidents and political opponents of autocratic regimes), and should continue to allow space for satirical and humorous accounts;

29. Calls on the Commission and relevant regulatory authorities to systematically investigate covert disinformation campaigns aimed at exploiting generative AI systems, included coordinated propaganda and narrative-laundering networks, such as the activities of the Moscow-based 'Pravda' network and the explicit manipulation of Grok (xAI) and to expose these campaigns publicly in a way that does not promote their spread; highlights the importance of clarifying the exact obligations of providers and deployers in relation to the 'AI-generated' labelling requirements set out in Article 50 of the AI Act and the Code of Practice on Disinformation, and specifying to what extent end users and platforms are covered under this framework; urges providers of AI systems to duly address and mitigate this phenomenon through their AI risk management systems; calls, furthermore, for the AI Office to enhance its efforts to monitor the security landscape of AI models and help develop methodologies for AI, including LLMs, ensuring improved transparency and respect for personal integrity in the training of data sources;

30. Calls on the Commission, in cooperation with the Belgian regulator, to urgently complete its assessment of Telegram's user base and functionality, as was done with WhatsApp, with a view to determining its classification as a VLOP under the DSA, and to take into consideration possible new evidence or changes in usage patterns; urges the Commission and relevant authorities to investigate Telegram's potential role in facilitating criminal activity, election interference and the dissemination of disinformation, extremism and terrorist content within the EU, as well as to clarify its possible links to Russian intelligence services and the security of its servers and data handling practices; stresses the need to take all available enforcement steps to ensure that Telegram fully complies with all applicable EU rules on transparency, content moderation and data access requirements, to ensure a level playing field and uphold citizens' trust in the digital information space; strongly encourages Telegram, furthermore, to join the voluntary Code of Practice on Disinformation;

31. 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; welcomes the Commission's commitment to an assessment of the role of online influencers in the upcoming evaluation of the Audiovisual Media Services Directive or as part of the forthcoming Digital Fairness Act; stresses, in this regard, the need for guidance and robust standards on transparency, including on platform-facilitated funding, remuneration and sponsorship arrangements, as well as on the distinction between advertised and organic content, and on 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 more transparent; suggests that ethical standards and obligations for journalists could serve as inspiration for preparing standards for influencers; calls further on the Commission to continue enforcing the TTPA, especially in relation to online platforms, and to facilitate compliance for influencers via the planned EU network of influencers;

32. Urges the development of regulatory sandboxes and funding mechanisms to support EU tech start-ups and value-driven European alternatives, based on fair remuneration, such as those emerging in the Netherlands, to reduce strategic dependencies; welcomes the Commission's EU Open Source strategy; further supports the long-term vision of EU social media platforms designed in accordance with EU values of transparency, data protection, fundamental rights, freedom of expression and democratic accountability;

33. Underlines that advertising and revenue-sharing practices may incentivise the spread of manipulative or harmful content, undermine electoral integrity and lead to the emergence of new disinformation actors and networks; recalls that disinformation cannot be demonetised without existing monetisation practices being sufficiently transparent; calls on the Commission, the EU digital regulators, the national competent authorities and online platforms to work together to detect and prevent illicit financing and ensure transparency in revenue redistribution programmes, advertising policies and other monetisation services that could allow FIMI actors or even sanctioned entities to earn income or other benefits; calls on platforms to publicly disclose renumeration flows and their beneficiaries, at least once a year; 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; considers the monetisation of content from sanctioned entities to be a systemic risk, requiring swift corrective action such as suspending revenue-sharing; underlines that genuine creators and media outlets should be compensated for their losses in cases of erroneous or unfair demonetisation; is concerned by the gradual rollback of corporate commitments to internet freedom initiatives;

34. Notes with concern the findings of the Dutch data protection authority, which are indicative of wider concerns across the EU, indicating that AI chatbots may provide biased and unreliable voting advice, thereby posing risks to electoral integrity; calls on the AI Office to investigate whether such practices breach applicable law, especially the AI Act, and to deliver on its commitment to prepare guidance on the application of AI in electoral processes in order to ensure the responsible use of AI;

Freedom of expression

35. 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 the fact that human rights protections in the EU are among the strongest worldwide, and that companies wishing to operate in the EU and attract European customers share a responsibility to respect and safeguard those protections; therefore underlines that VLOPs and VLOSEs must acknowledge and effectively address the broader societal and democratic consequences of their services, including through robust systemic risk assessment and mitigation measures, in accordance with Union law; notes, in this regard, that the amplification of certain content or opinions, and the silencing of others, may constitute a systemic risk to civic discourse and electoral processes or a breach of freedom of expression, in particular the freedom to freely receive and impart information and ideas; calls on the Commission to ensure that platforms are held accountable in this regard under the DSA; underlines, in this context, that the EU must continue to actively counter false narratives that claim that its digital and democratic legislation undermines freedom of expression; stresses that freedom of expression and information has been designed to protect human beings, not machines or software that exhibits inauthentic behaviour, such as AI and bot-driven amplification

and engagement, and automated software programs performing repetitive tasks over a network with the aim of imitating real users; further emphasises that the commitment to freedom of expression must not be used as a pretext for tolerating illegal content or the hybrid operations of authoritarian regimes that aim to destabilise the EU and its democratic processes;

36. Recalls that online platforms play an essential role in enabling open public debate, journalistic activity and political pluralism; recognises, therefore, the importance of effective safeguards for users when exercising their democratic rights, including the ability to challenge the content moderation and monetisation decisions of platforms, including before administrative and judicial authorities, and to enforce the obligations of online platforms to inform users when their content gets removed or restricted; underlines, in this context, the importance of ensuring access to high-quality content moderation in all EU languages; recalls the obligation under the DSA for online platforms to provide full transparency and a separate complaint-handling mechanism for this purpose and to ensure that notice, reporting and the possibility of redress remain easy to access and user-friendly; notes that not all online platforms have implemented such mechanisms in accordance with the provisions of the DSA and urges the Commission and the Member States to complete enforcement actions; 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

37. Takes the view that measures to promote and support free, credible and editorially independent media, including media at local and regional level, are a central part of achieving the objectives set by the European Democracy Shield; further stresses that safeguarding the media sector from political, economic or structural capture is a precondition for ensuring democratic resilience; notes that protecting independent media is vital for countering hybrid threats from hostile actors; further observes, in this context, that the current digital information environment often disadvantages media actors that assume editorial responsibility and public-interest obligations in favour of intermediaries that do not bear comparable duties; welcomes the groundbreaking common minimum standards on media freedom and pluralism established through the adoption of the EMFA; reminds Member States of the obligations in the regulation to protect media from undue media market concentrations; underlines, however, that the significance of the EMFA can only be assessed on the basis of its implementation in practice; calls on the Member States to swiftly implement the EMFA and on the Commission to ensure robust enforcement of its provisions, including taking action when obligations, in particular those of VLOPs aimed at protecting editorial content from undue removal or restriction of visibility, are not respected; welcomes the new commitments announced on media support via the Media Resilience programme and calls for matching long-term commitments in the upcoming MFF; further highlights that the financing crisis facing European media points to the need to explore new funding solutions;

38. Emphasises the need to carefully assess the potential impact of EU initiatives on journalism and editorial media, with particular regard to safeguarding media pluralism and to the sustainability of media companies' business models; calls for evidence-based impact assessments and the appropriate consultation of media stakeholders ahead of

initiatives that may affect the viability of European media companies; stresses, in this context, the importance of monitoring developments affecting media freedom and pluralism across the EU, and considers the annual rule of law report, with its chapter on media freedom and media pluralism, as a central tool in this endeavour; calls on the Commission to further develop this pillar of the report to better capture emerging challenges;

39. Underlines, in the context of media companies offering subscriptions via apps, the importance of the full implementation and effective enforcement of the DMA; notes the Commission's non-compliance decision of 23 April 2025 with regard to Apple and Meta, as well as ongoing investigations into a potential breach of the DMA by Google in demoting media publishers' content in search results; stresses that robust and timely enforcement of the DMA is essential to ensure fairness, contestability and pluralism in the EU's digital environment and to address structural dependencies and market concentration, including in the context of AI-driven services;

40. 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; points out that current media literacy initiatives remain fragmented across the EU; calls for more coherent, EU-wide approaches and for complementary measures to be explored, including the creation of digital tools and platforms at EU level; encourages the systematic exchange of best practice between national authorities, including through the reinforced media literacy expert group and EDMO; further highlights the role of cultural education in strengthening democratic literacy and resilience to disinformation; 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; stresses the importance of fostering a critical understanding of AI-generated content, as part of broader media and digital literacy efforts;

41. Welcomes the announced update of the Commission recommendation on the safety of journalists[62] and the forthcoming review of the Anti-SLAPP Recommendation[63]; underlines that these updates and reviews must take into account the evolving and recurring nature of threats, violence, sabotage and other actions aimed at hindering journalistic work, including emerging challenges, for example, identity thefts and coordinated deepfake campaigns, which may undermine journalists' safety and independence; stresses that particular attention should be paid to the chilling effects created by sustained climates of fear, political pressure or undue interference by public or private actors; calls on the Member States, in accordance with their national legal

---

62 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).

63 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).

frameworks and established practices, to consider introducing specific aggravating circumstances in criminal law for offences committed against journalists when such acts are motivated by or connected to their professional activities; further notes the potential relevance of developing support measures to assist journalists in dealing with emerging issues such as AI-driven impersonation and deepfake content;

42. Stresses the importance of protecting journalists from abusive lawsuits; welcomes, in this regard, the adoption of the Anti-SLAPP Directive 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 continue providing support to ensure full and timely implementation of the directive as a matter of priority; calls on the Commission to draft a comprehensive evaluation report on the effectiveness of the implementation; further invites the EU and the Member States to consider additional measures to complement the directive in order to protect journalists engaged in investigative work, especially in cross-border or sensitive contexts; underlines, in this context, the ongoing discussion on the establishment of a European protection status for investigative journalists as a possible avenue to explore;

43. Recognises the essential role of public service media in ensuring that all citizens, including those in remote and minority communities and candidate countries, have access to reliable, impartial and diverse news across multiple platforms, formats and languages, thereby contributing to the fight against news desertification; further stresses that access to quality and reliable information is essential in the fight against misinformation and disinformation; reaffirms that safeguarding public service media from political interference and capture is fundamental to preserving democratic accountability and the rule of law, stresses that the credibility of public service media depends on full editorial and organisational autonomy in accordance with Article 5 EMFA, and invites the Commission to actively monitor threats to the independence of public service media and to take effective measures against practices that compromise media freedom; notes, in this context, that attempts to undermine the independence of public service media can be early indicators of democratic backsliding;

44. Strongly emphasises the need to guarantee the highest level of protection for journalists and other media actors from illegal spyware, intrusive surveillance technologies and other forms of digital threats; recalls that the EMFA strictly prohibits the Member States from deploying intrusive surveillance software on any material, digital device, machine or tool used by media service providers or their editorial staff, with the exception of national security cases; further stresses that the surveillance of journalists constitutes interference with the rights guaranteed under Articles 7, 8 and 11 of the Charter of Fundamental Rights of the European Union; notes that the use of spyware undermines journalists' work by eroding their sources' trust in them, and that the failure to effectively enforce EU legislation poses a serious threat to freedom of information;

45. Reaffirms the importance of transparency, fair competition and the sustainability of European editorial media within the existing legal framework, including the DSA, the DMA, the EMFA and the TTPA; notes that these instruments address manipulation, foreign interference and anticompetitive practices while safeguarding editorial responsibility and free expression; calls on the Commission to assess how these instruments can best be used for these purposes; urges VLOPs and VLOSEs not to unjustifiably delist, demote or otherwise interfere with the visibility and fair ranking of lawful European editorial media content, and to ensure transparent and non-

discriminatory ranking systems;

46. Calls on the Commission to further study and, where relevant, consider measures to improve competitiveness, accessibility and fairness in online advertising for all value chain players, including editorial media; notes that editorially independent, high-quality and fact-based journalism faces challenges from engagement-driven recommender systems and AI-based search features of VLOPs, which reduce the visibility of high-quality content and limit traffic to media websites; notes, with concern, that traffic numbers correlating with the roll-out of Google AI-summaries have declined – up to 70 % in one measured case; encourages incentives for advertisers to support trusted European media, the use of contextual advertising instead of behavioural targeting, and stronger traceability and transparency in the online advertising supply chain to address market distortions and prevent malicious actors monetising disinformation content and purposefully destabilising society in the EU; calls on the Commission, in this context, to assess possible measures to boost the development and uptake of European infrastructure for contextual online advertising;

47. Welcomes the recently adopted Foreign Direct Investment Regulation[64], 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; stresses, in this context, the need for more transparency of investment in European news outlets; further points out that EU-based audiovisual media are subject to stricter requirements than media based outside the EU that are available to EU audiences through other means of distribution; stresses the importance of ensuring that media that are accessible to EU audiences respect fair and pluralistic information standards;

48. 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, including via the use of Global Europe; 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; invites the Commission to explore new ways of supporting free and editorially independent media in the EU neighbourhood, particularly in regions disproportionately affected by Russian disinformation and propaganda such as the Western Balkans;

49. Underlines that society-based independent fact-checking networks can play a role in detecting and combating disinformation campaigns and provide valuable insights for DSA risk assessments and mitigation; notes that independent fact-checking organisations need technical support and stable conditions in which to operate; considers that the European Network of Fact-Checkers, announced by the Commission in 2025, could serve as a valuable tool to achieve this; stresses that, to be credible and effective, fact-checking organisations must uphold strict standards of political neutrality, independence from online platform providers, and methodological objectivity; emphasises the importance of collaboration between fact-checkers, OSINT

---

64 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).

researchers, journalists, communicators and policymakers; further underlines the importance of supporting networks of fact-checkers in candidate and potential candidate countries;

Civil society, academia, culture and civic participation

50. Stresses the crucial role that active, vibrant and independent civil society plays as one of the core pillars in defending our democracy, not only in acting as a watchdog by exposing and actively combating malicious interference in 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;

51. Welcomes the Commission's EU Strategy for Civil Society, published alongside the joint communication on the European Democracy Shield; welcomes the Commission's approach of linking this strategy to its work on the European Democracy Shield, as a tool to further bolster civic engagement; considers the strategy an important first step, as it represents the EU's first comprehensive approach to civil society, while noting the need for the next steps to include a more ambitious approach, encompassing measures to effectively safeguard the role of civil society in democratic processes; highlights that future initiatives in this area should address the shrinking of civic space, while also recognising that civil society organisations and human rights defenders are particularly vulnerable, and emphasises that this is especially true for organisations working on specific topics, such as LGBTIQ+, gender equality and anti-racism issues;

52. 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, FIMI and transnational repression as well as improving situational awareness; underlines, in this context, the importance of diaspora-focused civic engagement; recalls, furthermore, that parts of civil society have extensive experience with foreign interference and should, within the context of civil dialogue, be involved in shaping policy to address it;

53. Highlights the role and responsibility that civil society has shouldered in democratic processes in candidate countries; calls on the Commission to liaise, where possible, with civil society organisations from candidate and potential candidate countries on current and future initiatives of the EU Strategy for Civil Society, particularly those organisations consistently engaged in fostering digital alignment, information integrity, election integrity and democratic resilience;

54. Calls on the Member States to ensure sustainable and diversified funding, including stable operating support and capacity-building measures, for civil society organisations, recognising their essential role in upholding democratic values and enabling them to operate effectively and independently; stresses the importance of concrete EU funding programmes to complement these efforts, such as the Citizens, Equality, Rights and Values (CERV) programme; and welcomes the Commission's intention to maintain the CERV programme by incorporating it into the new AgoraEU programme for 2028-

2034; calls on the co-legislators to ensure ambitious and predictable funding for this strand of AgoraEU, which meets the needs of civil society organisations and is implemented under the direct management of the Commission;

55. Emphasises that culture constitutes a strategic pillar of the European project, as cultural freedom, heritage and creativity foster democratic participation, critical thinking and trust in institutions; highlights the fact that programmes such as AgoraEU can play a key role in translating these values into tangible support; notes, with concern, that attacks on liberal democracy are increasingly targeting cultural actors and institutions, in particular through various forms of political pressure; underlines, therefore, that safeguarding artistic freedom and cultural institutions is essential to the defence of democracy in the EU;

56. Emphasises the importance of preserving Europe's cultural history and collective memory and of countering the manipulation and falsification of historical facts, in order to strengthen democratic resilience; underlines, in this regard, the need to reinforce a common European culture of remembrance and reiterates its support for a pan-European memorial to the victims of 20th-century totalitarian regimes, as well as for a Commission report on European remembrance by early 2027; condemns the Russian regime's historical revisionism and its use of distorted narratives to deny the sovereignty of formerly subjugated nations and to justify external interference;

57. Recalls that different interest representative actors, including civil society organisations, think tanks and umbrella 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; emphasises that financial transparency measures, if appropriately designed and with safeguards taking into account the size of organisations, can help mitigate the risk of future undue influence from authoritarian states; stresses that, as an institution, Parliament bears particular responsibility for strengthening integrity, transparency and accountability standards in the light of lessons learned from past cases of corruption and foreign interference; 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 and their decisive role in strengthening our democracies;

58. Highlights the importance of the Commission's proposed directive on interest representation carried out on behalf of third countries as a central 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 third-country entities; stresses that common rules in this regard can contribute to accountability and trust in EU decision-making by introducing transparency with regard to the influence of non-EU countries; calls on the co-legislators to finalise the legislative process without delay; underlines that the Member States should ensure that compliance with this directive should not lead to any restriction of fundamental rights;

59. 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 citizen engagement tools that are accessible, user-friendly, multilingual and capable of reaching citizens at scale; 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; highlights, in this context, the importance of actively engaging young people in democratic life, recognising that they are key actors in strengthening civic and political participation, including through the development of participatory digital platforms and youth councils to ensure meaningful involvement in decision-making processes at local, national and EU levels;

60. Stresses that academic freedom, including the freedom of research, teaching and scholarly expression, constitutes a fundamental pillar of democratic societies; condemns attacks on academic freedom and stresses the need to strengthen Europe's research independence and resilience to foreign interference; warns, in particular, against the manipulation of history by external actors; reiterates its call on the Commission to put forward a legislative proposal protecting the fundamental freedom of scientific research, including minimum standards for researchers' rights, ethical conduct, integrity and institutional independence, and supported by effective monitoring mechanisms;

Protecting critical infrastructure

61. Takes the position that protecting the EU and its Member States from both physical and cyber acts of sabotage targeting critical infrastructure is a vital element in safeguarding democratic resilience; calls for a proactive strategy to deter threats, the adoption of robust preventive measures, strengthened cross-border cooperation and enhanced EU capacity to detect, deter and respond to such hostile activities; emphasises that foreign state-linked ownership of critical infrastructure increases exposure to security risks and warrants enhanced scrutiny, particularly in communications infrastructure, digital infrastructure, undersea cables, energy infrastructure, transport hubs, hospitals and public service infrastructure;

62. Strongly condemns escalatory drone and other airborne incursions targeting and interfering with critical infrastructure, including civil airports, ports, military bases, industrial hubs, border management infrastructure 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 by shooting down aircraft, drones and other airborne threats; urges the Commission and the Member States to work on knowledge transfer programmes with Ukraine and on the joint training and certification of drone pilots in the light of the knowledge acquired in Ukraine about the conduct of modern warfare;

63. Emphasises the strategic role of EU agencies in ensuring the protection of cross-border critical infrastructure in the EU and its Member States, as well as the need to strengthen cooperation on seaports, airports and land border crossings, including through joint vulnerability assessments; draws particular attention to the threats of GPS jamming and spoofing conducted by Russia and Belarus and their potential to disrupt critical infrastructure operations, compromise navigational safety and undermine the continuity and resilience of essential cross-border services;

64. Stresses that a range of hybrid activities that 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; notes that Russia is vulnerable to cyber operations, as the breach of Russia's Aeroflot by Cyber Partisans has demonstrated; underlines Ukraine's extensive experience in inflicting damage on Russian capabilities and the need to accelerate support for Ukraine in strengthening its offensive cyber capabilities;

65. Emphasises that cross-border coordination in countering hybrid threats in maritime areas should be further strengthened, underpinned by dedicated and adequate EU funding, and that the EU must step up its operational response, particularly to threats linked to the Russian shadow fleet; calls, in this context, on the Commission and the Member States to establish a coordinated, EU-wide interpretation of the UN Convention on the Law of the Sea (UNCLOS) in order to ensure coherent action against hybrid activities, acts of sabotage, unreported illegal and unregulated fishing and violations of sovereign rights in the EU's maritime areas, notably in the Baltic Sea, while recalling UNCLOS's objective of ensuring the peaceful use of the seas; welcomes, furthermore, the Commission recommendation on secure and resilient submarine cable infrastructures[65] and the EU action plan on cable security; urges the Commission and the Member States to accelerate the implementation of these initiatives by mapping cable infrastructure, developing coordinated risk assessments and stress tests, deploying mitigation measures, and strengthening incident response and repair capacity, including by supporting modular repair equipment and maintaining strategic stockpiles of essential spare parts;

66. Calls for the effective criminalisation and deterrence of hybrid activities and acts of sabotage, including attack on undersea cables and connectors; encourages the Commission and the Member States to learn from the Australian example of establishing 'cable protection zones', providing legal safeguards and criminalising damage to submarine cables beyond the 12-nautical-mile territorial sea limit, accompanied by active monitoring, surveillance and response in cooperation with relevant third-country partners;

67. Encourages the Member States to explore the use of the mandate of the proliferation security initiative in order to board vessels linked to such shadow fleets, and calls on the Financial Action Task Force to play a more active role in scrutinising flag-registry governance within its mutual evaluation and greylisting processes;

68. Reiterates its call for the establishment of European maritime security hubs in the Black Sea, the North Sea and the Baltic Sea in response to Russia's war of aggression against Ukraine and underlines that such hubs should enhance maritime situational awareness, enable real-time monitoring from space to seabed and strengthen early warning capacities and reactions to the increased threats from the Russian shadow fleet, while also taking environmental perspectives into account and ensuring the security of commercial routes; calls on the Commission and the Member States to prevent the shadow fleet from entering European waters and to perform frequent and thorough

---

65 Commission Recommendation (EU) 2024/779 of 26 February 2024 on Secure and Resilient Submarine Cable Infrastructures (OJ L, 2024/779, 8.3.2024, ELI: http://data.europa.eu/eli/reco/2024/779/oj).

inspections to make sure the shadow fleet is not violating any laws and does not pose any danger;

69. Strongly emphasises that existing structural dependencies, through market concentration and foreign control, including the dominance of US big tech companies, in the EU's digital infrastructure and in operating systems, data centres, semiconductor manufacturing, AI, data-driven decision making tools, payment infrastructure, cybersecurity, cloud computing and various online platforms and services pose a high risk to democracy, freedom, security and competitiveness within the EU; regrets the recent incidents, in which Microsoft, Visa and Mastercard suspended services and halted the transactions of US-sanctioned staff members of the International Criminal Court; highlights, in this respect, the EU's vulnerability to similar external decisions that could disrupt public services and economic activities; calls on the Commission to systematically integrate dependency reduction and European industrial capacity-building objectives into the implementation of the European Democracy Shield;

70. Considers a resilient, competitive EU digital infrastructure – including secure local data centres, an EU sovereign cloud, edge computing capacities and gigabit networks – to be a strategic pillar of digital resilience, ensuring openness, competition and global interoperability; stresses that such infrastructure should help protect the sensitive data of EU citizens from risks linked to storage abroad and exposure to non-EU laws, and address complexities around foreign ownership and investment in essential infrastructures, including through digital autonomy stress tests to map dependencies on large commercial tech companies for essential public services; regrets that, after six years of drafting, the European Cybersecurity Certification Scheme for Cloud Services (EUCS) still lacks a certification assurance level enabling European cloud providers to guarantee the highest protection of strategic data against non-European jurisdictions, and underlines that robust cybersecurity certification is essential for the integrity and resilience of digital services underpinning democratic processes; stresses that, with the Cloud and AI Development Act and the revised CSA, the work on the EUCS should be resumed; welcomes the introduction of graduated EU assurance levels in the proposal for the Cloud and AI Development Act, and calls for the highest assurance level to provide effective protection of the most sensitive and strategic data against access under non-EU jurisdictions, while avoiding unnecessary barriers to innovation and investment;

71. Stresses the need to address risks related to strategic and sensitive network-connected hardware and software components and services capable of remote access, data transmission or system control sourced from high-risk third countries, including China; notes with concern the risks associated with the dominance of Chinese solar inverters and other components, in certain cases placed on the EU market at artificially low prices through state-backed non-market practices; welcomes, in this context, the fact that the revised CSA, as proposed, aims to provide a framework to ban network-connected components capable of remote access, such as inverters, from high-risk suppliers, and that the strategic roadmap for digitalisation and AI in the energy sector provides for a risk assessment of solar installations and a review of the energy security-of-supply framework; calls for the swift adoption of these measures to protect critical energy infrastructure from remote manipulation, blackouts and supply-chain risks; calls on the Commission and the Member States to promote secure, EU-based and EU-produced alternatives, review current procurement rules to assess whether they hinder digital sovereignty, and pursue a comprehensive EU tech sovereignty agenda with clear resilience standards and criteria for developing or procuring technology or digital

infrastructure, ensuring that regulatory frameworks, trade and competition policies effectively prevent unfair market practices and reduce dependencies on non-EU providers; stresses that digital success is driven by competition, openness and technological excellence, and that the EU should have a strategy to attract, maintain and retain critical technologies, while taking due account of factors related to foreign acquisitions; reiterates the need to be guided by a 'buy European' policy for critical infrastructure, which should be designed and implemented in a well-balanced and proportionate manner; supports a sovereign EU digital infrastructure with privacy-enhancing technologies and an EU application programming interface (API) ecosystem, leveraging fossil-free energy for data centres and cloud infrastructure, including through market-driven and public-private initiatives, such as joint ventures or federated networks in areas like AI, gigafactories and cloud services;

72. Welcomes the objectives set out in the European Critical Raw Materials Act (CRMA) for extracting, processing, recycling and mitigating the consumption of critical raw materials and emphasises that, in times of sudden crisis, dependency on Chinese rare earths may prove to be just as damaging as dependency on Russian carbon resources; reiterates the need to fully implement the CRMA, to stockpile, recycle and substitute critical raw materials, to accelerate the diversification of critical raw materials from China to more reliable partners, to increase the EU's own extraction and processing and to make resource use more efficient;

73. Calls for the formal recognition of hack-for-hire operations as a distinct threat to democratic institutions and processes, which could be better addressed by updating criminal law definitions; encourages the Commission and the Member States to launch a coordinated international initiative to counter so-called bulletproof hosting providers that knowingly lease infrastructure to cybercriminals, including through the blocking and filtering of abusive autonomous system numbers, with a view to effectively limiting the jurisdictions from which such providers are able to operate; highlights the continued risk of trading corporate vulnerabilities on the darknet, which exposes digital communication systems and devices to foreign interference;

74. Highlights the need to ensure greater integration and strategic coordination between digital infrastructure deployment, counter-FIMI and disinformation measures, and cybersecurity and defence policy, in order to advance the strategic autonomy of the EU; underlines the need to leverage dual-use infrastructure, such as resilient data centres scattered across the EU, to ensure operational continuity in the face of natural disasters and hybrid or wartime threats; highlights, furthermore, the need to increase investments in military mobility and secure communications, including the urgent and prioritised deployment of gigabit networks and space-based capabilities such as IRIS², in order to provide encrypted communication services for public and defence use; calls for these critical communications capabilities to be made available to Ukraine and Taiwan;

75. Stresses the need to increase investment in secure, interoperable and resilient information-sharing systems and local data centres, which are not subject to extraterritorial legislation; underlines that such investment is essential to ensure faster and more reliable communication between competent authorities at national and EU level, to strengthen protection against cyberattacks and data breaches, and to guarantee the integrity, availability and confidentiality of sensitive data, including through enhanced cybersecurity capabilities and modern EU digital infrastructure; underlines that redundancies are key to ensure operational security and communications security,

such as ground-based secure communication systems or inertial navigation systems;

76. Stresses that cybersecurity frameworks such as the NIS 2 Directive, the Cyber Resilience Act[66] and the Cyber Solidarity Act[67] must work in alignment to support secure-by-design standards and avoid regulatory fragmentation; takes note, in this context, of the targeted revision of the NIS 2 Directive; welcomes the Commission's proposal to significantly strengthen and expand ENISA's operational mandate and resources through the revised CSA; calls for the revision to explicitly include FIMI experts among the stakeholders represented in the ENISA Advisory Group; calls on the Commission to secure sufficient funding in the 2028-2034 MFF to ensure that undertakings, especially those in the ICT sector, can afford the additional investments arising from the revised CSA; underlines further that small and medium-sized enterprises need support with compliance, in addition to exemptions that should ensure that their security and, as a consequence, the collective cybersecurity, is not weakened;

77. Recalls the low level of transposition of the NIS 2 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 had 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 NIS 2 Directive, as well as the Cyber Resilience Act and the Cyber Solidarity Act, as stipulated in the ProtectEU internal security strategy; calls on the Commission and the Member States to address the gaps in situational awareness, risk mitigation and coordinated action across cyberthreats and hybrid and information threats;

Cooperation in the area of justice and home affairs

78. 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; stresses the need for competent national authorities to be equipped with adequate tools and cooperation channels to prevent, investigate, detect and prosecute criminal offences related to foreign interference; considers that the corruption and intimidation of elected and public officials by criminal networks should be addressed as part of the EU's response to hybrid threats via strengthened cooperation between specialised anti-corruption agencies, law enforcement authorities and relevant Union bodies; asks the Commission to assess the added value of establishing in Union law minimum rules on

---

66 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).

67 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).

the definition of and sanctions for the criminal offence of knowingly participating in organised activities of interference on behalf of foreign powers; notes that the forthcoming revision of the mandates of a number of EU bodies in the area of justice and home affairs could provide an opportunity to strengthen the operational dimension of the European Democracy Shield; 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;

79. 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 for the co-legislators to perform, during the ongoing revision of the mandates of Europol and Eurojust, a careful assessment of the legal gaps and limitations that currently prevent those agencies from providing their full assistance to the Member States confronted with hybrid threats, and to explore ways to overcome those limitations while respecting fundamental rights and Treaty-based competences; considers that the addition of hybrid threats in Annex I to the Europol Regulation[68] would clarify the legal framework and facilitate Europol's work in this area; underlines, moreover, the need to ensure that Europol and Eurojust are provided with adequate financial and human resources to effectively implement the upcoming strengthening of their mandates;

80. Considers transnational repression to be a growing and serious threat to democracy and internal security in the EU; underlines that transnational repression can be perpetrated online, via hate and defamation campaigns and the spreading of illegal content, but can also lead to physical assaults and murder; 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; 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 close remaining loopholes in Union law and further reinforce EU-level coordination in the field of criminal justice and law enforcement through a police and judicial cooperation framework dedicated to transnational repression as part of the European Democracy Shield, while involving individuals and groups that are targeted and ensuring their protection; draws attention to the urgency of addressing the abuse of Interpol red notices for politically motivated purposes;

81. Strongly condemns the instrumentalisation of migration by third countries or hostile non-state actors with the aim of destabilising a Member State or the EU; takes the position that this phenomenon constitutes an unacceptable attempt to exert political pressure on front-line Member States and on the EU; underlines that such practices also represent a grave abuse of vulnerable persons who may be entitled to international protection and should not adversely affect the right to seek asylum; notes the specific provisions on the instrumentalisation of migration recently included in key pieces of EU legislation; further welcomes the recent revision of the EU legal framework to include hybrid threats among the grounds triggering the EU visa suspension mechanism;

---

68 Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA (OJ L 135, 24.5.2016, p. 53, ELI: http://data.europa.eu/eli/reg/2016/794/oj).

underlines that a credible and effective EU response must also be based on close coordination and sincere cooperation between neighbouring Member States, and between them and EU institutions, in a spirit of loyalty and mutual solidarity, and on enhanced technological and operational capabilities in border management, while preserving the integrity of the Schengen area and ensuring full respect for the fundamental values of the EU;

82. Notes the Commission's announced revision of the mandate of Frontex; underlines that the revision should provide for the necessary legal basis, analytical capabilities and adequate human, financial and technical resources to enable effective assistance for Member States in the management and protection of the external borders in compliance with relevant Union law, including fundamental rights; stresses, in this context, the need to further strengthen the EU's capacity to support Member States in matters related to home affairs under the 2028-2034 MFF, including in responding to threats of a hybrid nature;

External dimension

83. Underlines the need for the European Democracy Shield to have a strong external dimension and welcomes actions that support countries beyond the EU, in particular through capacity-building to strengthen candidate and potential candidate countries' resilience to FIMI, hybrid interference and transnational repression, support for independent media and journalism, and improved ability to detect and counter disinformation before and during elections; underlines the need for adequate funding, including core funding via the Global Europe instrument, for independent media in neighbouring countries; notes that capacities and commitments among candidate countries vary, which calls for a differentiated, context-sensitive implementation of the European Democracy Shield in full respect of EU values; underlines that strengthening democratic resilience is key both for the credibility of enlargement and for the EU's security and stability; calls for the systematic involvement of candidate countries in relevant actions, support mechanisms and expert networks under the external dimension;

84. Calls for the European Democracy Shield to serve as a two-way mechanism for expertise, where the EU integrates the successful rapid-response models, civil-military cooperation frameworks and real-time detection techniques, and recalls the expertise of front-line partners who are experiencing Russian aggression and interference; emphasises that the EU has a significant amount to learn from the resilience of Moldova and Ukraine;

85. Notes Taiwan's leading role in high-tech development, and its extensive experience in defending itself against China's hybrid attacks and FIMI; calls for regular exchanges on relevant security issues, as well as for stronger cooperation on countering FIMI and the sabotage of undersea cables with like-minded partners in East Asia, including Taiwan, Japan and South Korea;

86. Calls for the development of a comprehensive strategy, in priority regions, whereby EU Delegations and common security and defence policy (CSDP) missions and operations, in close coordination with the diplomatic missions of the EU Member States, are mobilised to enhance the understanding of local circumstances that may lead to foreign interference and to deliver a tailored response; notes the possibility for EU Delegations

and Member States' embassies to support the organisation of awareness-raising campaigns in host countries; 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; is therefore concerned by the reports regarding the risks of possible downsizing of EU Delegations and their staffing, in particular in the context of the growing international challenges and geopolitical tensions;

87. Highlights that 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; calls for the visibility and strategic communication of the benefits, presence and role of CSDP missions and operations around the world to be enhanced, especially in the EU's immediate neighbourhood and in candidate and potential candidate countries; calls on the Vice-President of the Commission / High Representative of the Union for Foreign Affairs and Security Policy and the Council to include FIMI monitoring and response teams within CSDP missions, ensure FIMI training for all relevant current and future missions and operations, and strengthen coordination between civilian and military operations to counter hybrid influence;

88. Stresses the importance of joint exercises, capacity building and technical assistance for partner countries facing persistent hybrid pressure; calls on the Member States and the EEAS to integrate capacity-building activities and training on hybrid threats into the mandates of individual missions and operations, to increase the preparedness of partner countries; welcomes the deployment of EU hybrid rapid response teams and of cyber rapid response teams as useful instruments in building capacity and resilience in countries targeted by cyberattacks and hybrid and FIMI attacks, as illustrated by the recent example of Moldova; notes, in this context, the presence of Frontex in several relevant third countries and the potential added value of its capacities in this regard;

89. Stresses that repeated attempts to normalise relations with Russia, without addressing the underlying nature of the Russian state and its imperial strategic objectives, have contributed to increased instability, have weakened deterrence and have undermined European and global security; underlines that future EU and Member States' policies must be based on a realistic assessment of this historical continuity, prioritising deterrence, resilience and the security of countries in Russia's neighbourhood over short-term economic or political considerations; welcomes the efforts in recent years to decouple the EU economy from dependence on Russian fossil fuels; further stresses that the complete and irreversible phase-out of such dependence should be a strategic priority for the EU and its Member States;

90. Welcomes the strengthened commitment in the joint communication to developing capacities for offensive information operations; 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 and reinforced information measures to counter destabilising efforts as well as other hostile state and state-sponsored coordinated information manipulation, cognitive warfare operations and hostile influence campaigns by authoritarian or malign actors; highlights the need to disseminate factual and trustworthy information to the populations living in authoritarian regimes, notably Russia and Belarus, in order to reveal their rulers' destructive governance practices, which pose danger to freedom and peace, not only in

neighbouring countries but primarily in their own country; calls for every possible use of the digital and cyber space and its borderless nature to achieve this goal;

91. Notes with grave concern that, in certain Member States, government actions and strategic decisions have repeatedly served Russian interests; recalls the case of the former Fidesz government in Hungary as a particularly clear example, including, among others, the failure to duly report and investigate intrusions by Russian state-linked cyber actors, the conclusion of long-term gas contracts with Russia at prices above market levels, the systematic obstruction of EU assistance for Ukraine, and alignment with Russian positions in key EU foreign and security policy decisions; calls for the proper reporting and investigation of activities and campaigns that may be linked to foreign influence and interference; calls for increased vigilance, enhanced monitoring and the full use of EU instruments to protect the EU against internal vectors of foreign influence and interference;

92. Notes that candidate and potential candidate countries and countries in the EU's neighbourhood, in particular the Western Balkans, Moldova, Ukraine, Armenia and Georgia, have been a clear focal point of Russian FIMI operations, with one of the aims being to discredit the EU and diminish the perceived value of EU integration; calls on the Commission and the EEAS to deepen cooperation with relevant actors in these countries on information resilience, cybersecurity and hybrid threats, and to move from ad hoc support to systematic, long-term assistance aimed at building institutional, legal and civic resilience; calls for EU funding for regional coordination hubs for countering threats to online information integrity and FIMI in relevant parts of the EU's neighbourhood, and for support for investigative journalism and media regulators to be boosted; underlines the need for a specific focus on election integrity assistance in candidate or potential candidate countries, including in the context of the USAID funding withdrawal, affecting, in particular, the Western Balkans;

93. Underlines that efforts by the EU to support candidate countries in strengthening their resilience against foreign interference should be accompanied by the proven implementation of relevant reforms and tangible results on their part; calls on the Commission to continue applying a rigorous approach in its examination of candidate countries' progress under accession chapters; stresses that shortcomings in addressing key issues such as corruption, lack of independent media, violations of human rights and weaknesses in democratic processes undermine citizens' trust in national and EU institutions, thereby creating anti-EU narratives that may be exploited by third countries and actors engaged in FIMI;

94. Calls on the Commission to establish regional EDMO hubs covering relevant EU candidate, potential candidate and neighbourhood countries, following the model of the existing hub for Moldova;

95. Calls on the Commission to make media literacy programmes a permanent part of pre-accession assistance and the European Neighbourhood Instrument; stresses that cultural cooperation should be an integral component of these instruments, strengthening societal cohesion, shared values and people-to-people engagement in candidate and neighbouring countries; highlights that the removal of the thematic programmes and related financial allocations for human rights and democracy, and for civil society organisations, as provided for by the Commission proposal on the 2028-2034 MFF and by the proposal for a new Global Europe programme, leave significant uncertainty over

how these EU Treaty-based obligations will be effectively mainstreamed, operationalised and monitored; reiterates its call on the Commission to strengthen the programmes aimed at meaningfully engaging and supporting civil society, human rights defenders, journalists and investigative media in third countries; insists that the new MFF provide predictable funding that allows rapid responses to threats against fundamental freedoms and supports local initiatives;

96. Urgently calls for EU efforts to support partner countries in its Eastern and Southern neighbourhood, as well as in priority countries in sub-Saharan Africa, the Asia-Pacific region and Latin America, to build resilience to FIMI, strengthen democratic processes and ensure electoral integrity, including through dedicated funding under the next MFF; emphasises, in particular, that transformations unfolding in North Africa and the Sahel region have a direct impact on the EU's security and democratic resilience, and notes that these regions are particularly vulnerable to FIMIs, notably due to political instability and fragile information ecosystems; underlines that Russia and China increasingly cooperate in amplifying revisionist narratives about alleged Western decline and 'neo-colonialism' in these regions, revealing a strategic communication gap that undermines the EU's credibility and influence; underlines, in particular, the need to continue developing targeted FIMI resilience measures for these regions, including support for independent media, civil society, digital and AI literacy, strategic communication in local languages, and enhanced monitoring and response mechanisms, such as the flagship EUvsDisinfo project, in addition to financial support mechanisms;

97. 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 cyberthreats and hybrid 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 for the establishment of similar missions in other partner countries; considers that such agreements should be prioritised with countries whose internal instability directly affects the security of the EU; takes note of the parliamentary elections held in Moldova on 28 September 2025, as well as the presidential election on 3 November 2024, and of the strong victory of pro-European forces, despite significant efforts and resources deployed by Russia to destabilise the situation in Moldova and divert it from its European and Euro-Atlantic path;

98. Notes, with concern, that Armenia faced an intensification of Russian-linked hybrid threats aimed at influencing the outcome of its June 2026 elections and undermining its democratic processes, social cohesion and peacebuilding efforts, including malign cyber activities, coordinated information manipulation, electoral interference, economic coercion, and overt and covert threats by senior Russian officials, as well as the activation of influence networks; recalls that the Armenian Foreign Intelligence Service has reported the use of overt and covert information operations, distortive narratives and efforts to manipulate public discourse in ways that are detrimental to Armenia's national interests, and stresses that such hybrid pressure may involve both state and non-state actors, including domestic amplifiers such as certain religious actors and oligarchic networks connected to broader Russian influence strategies in the region; welcomes the establishment of EUPM Armenia to provide strategic advice and capacity building to Armenian institutions on countering FIMI, cyberattacks and illicit financial flows; encourages the EU Mission in Armenia (EUMA) to strengthen its outreach to local democratic actors, community organisations and independent media as part of its contribution to democratic resilience; recalls that Armenia is still a member of the

Russian-run Collective Security Treaty Organisation and calls on Armenia to fully leave it;

99. Deeply regrets the decision of 7 January 2026 by the US President to withdraw from, suspend participation in, or terminate engagement with a significant number of international organisations, including numerous UN bodies; expresses its serious concern that such a move will undermine the financial sustainability of the UN system, weaken multilateral cooperation at a time when it is most needed and embolden authoritarian and revisionist actors, who have historically sought to exploit any withdrawal or disengagement by Western powers from international organisations; stresses, therefore, the need for the EU to reinforce its leadership in supporting and strengthening multilateral organisations, and to uphold democratic institutions; encourages the US administration to reflect on its decision and to reaffirm its commitment to the UN and multilateral cooperation;

100. Expresses its strong disagreement with the recent US National Security Strategy, in particular its negative characterisation of the EU and its challenges and risks, and the vision of international relations that is based on spheres of influence; condemns any attempts to influence or undermine democratic processes in the EU; stresses the importance of safeguarding the integrity of EU institutions and EU decision-making; expresses concerns about the fact that certain elements of the strategy fall significantly short in adequately addressing the threat posed by Russia, notably for European and hence also for American security; regrets, furthermore, the strategy's flawed assessment of the EU as a political system and its groundless adversarial stance towards the EU; considers that the strategy further reinforces the imperative for the EU to advance its strategic autonomy, reduce dependencies and diversify partnerships;

101. Underlines the importance of prioritising the principles and objectives of the European Democracy Shield in international cooperation with like-minded partners, including the G7, NATO, the UN, the Organization for Security and Co-operation in Europe and the Council of Europe; encourages the further development of shared open-source standards, frontier AI safety frameworks, data models, methodologies and taxonomies among like-minded partners to enable more effective collaboration; affirms NATO's key role in countering hybrid warfare targeting democratic institutions and recalls its dedicated instruments and strategies in this regard, notably through its Strategic Communications Centre of Excellence; highlights the fact that, following the accession of Finland and Sweden, 23 of the 27 EU Member States are also NATO allies, and underlines the need for strong synergy between EU and NATO strategies; welcomes the steps already taken in bilateral and multilateral frameworks, including the UN Code of Conduct for Information Integrity on Digital Platforms, the commitments made in the Council of Europe Reykjavik Declaration to safeguard electoral systems against foreign interference, the continued efforts of the G7 Rapid Response Mechanism, and the establishment of security and defence partnerships, especially those focusing on countering cyberattacks, hybrid threats and FIMI, and on protecting critical infrastructure; reiterates, in this context, its sincere appreciation of the United Kingdom's continued engagement in European security;

Election systems and electoral resilience

102. 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 and in candidate

countries; calls on the Commission and the Member States to work together, with full respect for the principle of subsidiarity and within the scope as defined by the Treaties, to implement reforms aimed at strengthening the resilience of electoral processes in Europe, with a particular focus on measures to prevent foreign interference; notes that attacks on election integrity are multifaceted, integrated and long-term, as part of an ecosystem of threats that need to be tackled through a whole-of-society approach; proposes that the European Democracy Shield initiative should support the coordination of efforts, both online and offline, to maintain the integrity of European elections, including efforts addressing hybrid threats, cyberthreats, the financing of interference and information manipulation;

103. 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; calls on the Commission and the Member States to work towards the systematic development and expansion of election-focused stress-testing exercises at both national and cross-border levels, drawing on practical experience and lessons learned from previous electoral cycles, in order to better anticipate, simulate and mitigate risks linked to information manipulation, cyber interference and platform-driven amplification;

104. 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, whether in terms of providing personnel training and the necessary digital tools or in terms of ensuring sufficient investment in electoral bodies and election infrastructure;

105. Considers that hate campaigns, intimidation 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, including through disinformation tactics such as deepfakes falsely depicting real political candidates and deliberately designed to mislead voters; 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;

106. Stresses that the safety and security of women in political life are prerequisites for equal representation and resilient democracy; condemns disinformation campaigns, including via deepfakes and non-consensual sexual content, used to harass, threaten and intimidate female candidates, frequently relying on narratives challenging their competence, credibility and moral integrity, thereby discouraging women's political participation and undermining trust in democratic institutions; welcomes the AI Act's targeted ban on 'nudification' applications and recalls that the DSA identifies gender-based violence and the protection of minors as a systemic risk; calls on the Commission to include in the forthcoming recommendations on safety in politics specific provisions regarding the monitoring, prevention and countering of disinformation campaigns specifically targeting female candidates;

107. Condemns fraudulent advertisements that impersonate and misappropriate the identity of politicians, political candidates and other public figures; warns that, although the primary purpose of such scams is often financial gain, the unauthorised use of a public

figure's image and likeness manufactured to falsely suggest authenticity or endorsement may cause reputational harm, contributing to the erosion of the boundary between authentic information and fabricated content, and further undermines public trust in democratic processes and political actors; calls on the Commission and the Member States to investigate the compliance of online platforms as regards their processes for removing illegal advertisements;

108. Underlines the key role of ECNE in promoting the exchange of best practice in electoral resilience across the EU and its Member States, while noting ECNE's current limitations and welcoming the Commission's commitment to strengthening it; calls for an ambitious reform of ECNE, including a review of its resources and staffing, further development of the joint mechanism for electoral resilience and the stronger involvement of candidate countries; calls on the Commission, within the ECNE framework, 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; further calls for Parliament and the Authority for European Political Parties and European Political Foundations (APPF) to be included as permanent partners in all ECNE meetings;

109. Stresses that electoral infrastructure is a fundamental component of the EU's democratic resilience and must be effectively protected against growing threats of a physical and cyber nature; 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; asks the Commission to ensure that this inclusion is then echoed in the NIS 2 Directive and ENISA guidelines;

110. 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 countries funding 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; is concerned by continued deficiencies with the functioning registers of ultimate beneficial owners in the Member States, including the quality of data or risk of overly restricted access, for persons with legitimate interests such as journalists or civil society organisations; urges Member States to fully and faithfully transpose the Anti-Money Laundering Directive[69], which harmonises the rules on access to beneficial ownership registers; further stresses that political advertising and political communication in the online environment must be fully transparent regarding the identity of the sponsor and the source of funding, in accordance with EU transparency rules; calls for the rigorous enforcement of existing measures to prevent the use of proxy financing in politics; underlines the importance of

---

69 Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (OJ L 141, 5.6.2015, p. 73, ELI: http://data.europa.eu/eli/dir/2015/849/oj).

effective EU-wide monitoring and cooperation among authorities to ensure compliance with transparency obligations; invites, in this sense, the Commission and the Member States to look into the options available for improving cooperation between the anti-corruption authorities and the independent election commissions in the Member States;

111. Notes, with concern, the growing evidence of foreign interference and espionage targeting political institutions and processes at both EU and Member State level; welcomes the investigations in several Member States leading to convictions and ongoing cases involving bribery, espionage and foreign influence activities; underlines the serious risks posed by insufficient safeguards in the recruitment of staff and associates with close links to authoritarian regimes; stresses that protecting the integrity and functioning of the EU institutions requires robust measures against espionage and infiltration; further highlights the need to investigate the serious and evolving allegations that Hungarian officials, acting under the previous Fidesz-led Hungarian Government, conducted espionage activities targeting the EU institutions, including reports that sensitive information from EU meetings was shared with Russian counterparts, raising concerns about breaches of confidentiality, intelligence leakage and the integrity of EU decision-making processes;

112. 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, in particular regarding the fact that non-EU parties should not have any veto powers or control over European parties; calls on the co-legislators to ensure the full and effective implementation of the regulation;

113. Reiterates its call on the Commission to strengthen the annual rule of law report and reinforce democracies against foreign interference, including by addressing free and fair elections, robust legal guarantees, checks and balances, and the functioning of democratic institutions, in order to provide a more complete picture of rule of law standards across the EU;

114. Notes that rapid developments in cryptocurrency, including platforms or service providers operating outside the EU, create a potential vulnerability in terms of a lack of transparency and an inability to scrutinise the financing of political parties and movements in Europe; highlights the fact that, given their pseudonymous nature and global reach, and the availability of anonymising techniques and services, crypto-assets can present challenges in identifying the origin of political donations and mitigating potential foreign influence in democratic processes; stresses that political donations involving crypto-assets should be subject to the ‘know your donor’ principle, with the same transparency and accountability standards as traditional financial contributions; acknowledges the Commission’s commitment to bring together national experts under the umbrella of ECNE, in close cooperation with other EU networks and stakeholders, to exchange best practice, prepare possible guidelines and promote joint actions; calls on the Commission, in this regard, to continue monitoring the implementation of the anti-money laundering package and the Markets in Crypto-Assets Regulation (MiCA), to ensure effective and consistent enforcement and address any potential gaps in the legislation that may need to be filled; notes in this regard that the market integration and supervisory package includes a proposed revision of the MiCA;

115. Calls on the Member States to exchange best practice in the oversight of political party

funding; expresses concern that certain financial intelligence units do not possess the requisite mandate to submit information regarding interference in elections to the competent national and European authorities; calls on the Commission to assess the added value of expanding the role, mandate and resources of the APPF to further enhance the coordination of national and EU authorities responsible for the oversight of political party financing; underlines, in this context, the need to strengthen cooperation between the APPF and ECNE;

The role of sanctions in the protection of democracy

116. Considers sanctions against individuals and state and non-state entities engaged in actions aimed at undermining the democratic integrity of the EU or its Member States to be an essential component of the European Democracy Shield's toolbox; further stresses that effective sanctions must be adopted based on objective and consistent criteria and must include a comprehensive set of measures, including asset freezing and confiscation, clear attribution and public exposure, cost increases and revenue cuts, bans on imports and exports, travel bans, the denial of access to EU markets and financial systems, and other effective, robust and impactful restrictive measures; reiterates its call on the Council to gradually transition to qualified majority voting for decisions in areas of the common foreign and security policy such as sanctions;

117. Calls for the effectiveness and impact of EU sanctions adopted following Russia's invasion of Ukraine to be improved, so as to definitively undermine Russia's ability to continue waging its brutal war of aggression and threatening the security of other neighbouring countries; 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 sanctions targeting individuals and entities that engage in the active circumvention of the EU sanctions against Russia; 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, the Middle East and Latin America, 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 sanctions targeting non-EU (and in particular Chinese) individuals and entities that are responsible for the active circumvention of sanctions and the facilitation of 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 who are covertly funded by Moscow;

118. Considers that identifying and naming source countries, in addition to attributing responsibility to individuals or companies, could be an important step towards acknowledging the problem of clear systematic, multilayered 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; calls on the Commission to assess whether further listing Belarus would be appropriate, given its risk profile and links to the Russian political and economic structures; recalls that the new Anti-Money

Laundering Regulation will provide extended possibilities for identifying and listing high-risk third countries; calls on the Commission, with the assistance of the Anti-Money Laundering Authority, to fully use its powers with regard to ensuring the implementation of targeted financial sanctions;

119. Underlines that the effectiveness and credibility of EU sanctions depend on strict and consistent enforcement; calls, therefore, on the Member States to establish a mechanism for the effective monitoring of enforcement activities, including through collaboration with civil society and academia, to improve coordination and to work together on closing loopholes and harmonising procedures; welcomes the fact 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; stresses that the reform should be matched by adequate funding to enable the EPPO to effectively carry out its enhanced responsibilities;

120. Recalls that the EU's Anti-Coercion Instrument, which has been in place since 2023, provides for a wide range of EU measures to counteract third countries' attempts at economic coercion against the EU or a Member State; stresses that the Anti-Coercion Instrument should be part of a proactive escalation strategy to respond to threats targeting European territorial integrity and digital, regulatory, financial or economic sovereignty; recalls that access to the internal market for operators from non-EU countries is subject to compliance with EU law;

121. Condemns the politically motivated use by foreign governments, not least Russia, of blacklists, visa bans and other restrictive or retaliatory measures targeting EU citizens, representatives of state authorities and commercial organisations, journalists, civil society actors, humanitarian organisations and political officials, including democratically elected MEPs; is concerned that such practices, which aim at exerting undue political pressure on the EU's regulatory autonomy and fundamental rights framework, undermine diplomatic norms and the principle of mutual respect between jurisdictions; calls for a more coordinated and resolute EU response to these arbitrary measures alongside continued diplomatic efforts, ensuring the protection and security of those blacklisted and providing them with solidarity and the necessary assistance; expresses its full support for all individuals affected; stresses the need to establish a system for continuously assessing and informing targeted individuals, in particular in relation to the Russian blacklist, including MEPs and their staff, and EU officials, to ensure transparency and protection;

The EU's preparedness

122. 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; welcomes Member State initiatives, such as those in Sweden and Finland, to strengthen societal preparedness, cooperation and clear communication about citizens' responsibilities; underlines that an effective preparedness policy must be based on inclusion across all ages, communities and social and economic groups; highlights, in this context, the role of companies, associations and skilled individuals in supporting essential services and care; stresses that effective civil resilience requires

citizens to be engaged and educated on how and when to contribute;

123. Calls for the establishment of an annual, publicly accessible EU activity report on the overall state of preparedness across the EU with a comprehensive structured overview for each Member State; emphasises that such a report could set out, among other things, institutional readiness, state of civil-military cooperation, strategic capabilities, preventive measures, response mechanisms, vulnerabilities and key trends, while respecting national security considerations; underlines that such a report could contribute to the exchange of best practice and serve as a guidance and advisory instrument for the implementation of Member States' preparedness strategies; notes that consideration should be given to whether the European Centre for Democratic Resilience could play a coordinating role in the preparation of such a report;

124. Calls for the swift development and deployment of an EU-wide, interoperable crisis-alert application, providing real-time, reliable, multilingual information to residents during emergencies; recommends that this app be integrated into national and EU early warning systems, be accessible to all persons, with a special focus on availability for vulnerable groups, and be regularly updated with technological advances and in line with best practice in crisis management;

125. Welcomes the initiatives in several Member States to distribute a household preparedness booklet, offering clear, practical guidance tailored to Europe's diverse social and geographical 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, instructions for practical self-sufficiency for a minimum of 72 hours, basic first aid advice and specific guidance for vulnerable groups, including elderly people, people with disabilities and families with children;

126. Calls for the organisation of regular large-scale, EU-coordinated preparedness exercises involving EU institutions, EU agencies, Member States, regional and local authorities, the private sector and civil society; considers that preparation for scenarios ranging from floods, forest fires, earthquakes and medical emergencies to chemical, biological, radiological and nuclear incidents may also contribute to strengthening Europe's capacity to prevent, withstand and respond to threats, such as those demonstrated in Russia's aggression against Ukraine and hybrid attacks against Europe as a whole; recommends that these exercises simulate complex and realistic scenarios, including cyberattacks, disruption to critical infrastructure, coordinated disinformation campaigns and hybrid crises, in order to assess response capacities, improve interoperability across governance levels, share best practice and promote a culture of preparedness at all levels; underlines, in this context, that EU initiatives on military mobility are also highly relevant with regard to civilian preparedness and the ability to transport relief supplies in emergencies; further calls 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 need to strengthen civilian and defence preparedness against growing threats from authoritarian regimes;

127. 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 for 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;

128. Calls for the accelerated implementation of secure communication systems such as IRIS² and the European Critical Communications System, while building on already existing systems at Member State level; stresses that these initiatives ensure telecommunications resilience, the continuity of essential services during crises, reduced external dependencies in strategic sectors, and reinforced cybersecurity for this infrastructure through harmonised spectrum authorisation, cybersecurity certification and ICT supply chain security measures in line with the Commission's proposals for a Digital Networks Act and a revised CSA;

129. Calls for enhanced coordination between EU institutions, bodies, offices and agencies, the Member States and like-minded 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; emphasises, in this context, that preparedness and resilience are collective responsibilities requiring societal participation;

130. 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 that are most exposed to vulnerabilities and hybrid threats, in particular information warfare;

131. Recommends that the EU's decision-making institutions review and optimise the strategies and contingency plans they would deploy in the event of an open military conflict against one or more Member States and similar crisis scenarios, including in cases of activation of Article 42.7 TEU; 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, including through effective investigation and prosecution of such breaches, in particular in the context of a heightened risk of espionage and sabotage; calls, in this regard, for regular auditing of vulnerabilities and dependencies, particularly in the digital space, in all EU institutions, bodies, offices and agencies; stresses that, even outside of open military conflict, hybrid threats continue to pose ever higher risks to the daily functioning of the EU;

132. 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 who handle 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[70]; 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; welcomes the activities of the Cybersecurity Service for the Union institutions, bodies, offices and agencies (CERT-EU) and insists on the need to ensure that it has a sufficient budget and proper staffing;

133. Recommends further measures to strengthen Parliament's security, resilience to foreign interference and ability to operate effectively in crises, including reinforced support for MEPs and staff through IT and security checks, targeted training, pre-mission briefings and interdisciplinary resilience-building activities integrating physical security, information security and cybersecurity; stresses the need to further enhance its cybersecurity framework in line with the Cybersecurity Regulation, improve operational maturity and strengthen threat detection capabilities in an evolving technological and threat landscape, while also providing more targeted training for staff to counter information manipulation and applying stricter security clearances for sensitive meetings and missions; notes that the use of private mobile devices and laptops for parliamentary work constitutes a potential vulnerability and underlines that MEPs and staff should be equipped with secure institutional devices; welcomes existing voluntary spyware screening and calls for its systematic extension to all devices used for parliamentary business; further calls on the Commission and the EEAS to systematically involve Parliament in preparedness activities and exercises, such as the EU Integrated Resolve;

°

° °

134. 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.

---

70 Commission proposal of 23 March 2022 for a regulation of the European Parliament and of the Council on information security in the institutions, bodies, offices and agencies of the Union (COM(2022)0119).