Europäisches Parlament
2024-2029

Sonderausschuss für den Europäischen Schutzschild für die Demokratie

2025/2069(INI)

18.12.2025

ENTWURF EINES BERICHTS

über die Feststellungen und Empfehlungen des Sonderausschusses für den Europäischen Schutzschild für die Demokratie
(2025/2069(INI))

Sonderausschuss für den Europäischen Schutzschild für die Demokratie

Berichterstatter: Tomas Tobé

INHALT

Seite

ENTWURF EINER ENTSCHLIESSUNG DES EUROPÄISCHEN PARLAMENTS 3

BEGRÜNDUNG.....45

ANLAGE: ERKLÄRUNG ZU BEITRÄGEN 48

ENTWURF EINER ENTSCHLIESSUNG DES EUROPÄISCHEN PARLAMENTS

über die Feststellungen und Empfehlungen des Sonderausschusses für den Europäischen Schutzschild für die Demokratie

(2025/2069(INI))

Das Europäische Parlament,

– unter Hinweis auf seinen Beschluss vom 18. Dezember 2024 über die Einsetzung, die Zuständigkeiten, die zahlenmäßige Zusammensetzung und die Mandatszeit des Sonderausschusses für den Europäischen Schutzschild für die Demokratie[1],

– unter Hinweis auf die gemeinsame Erklärung der Kommission und der Hohen Vertreterin der Union für Außen- und Sicherheitspolitik vom 12. November 2025 mit dem Titel „Europäischer Schutzschild für die Demokratie: Förderung starker und widerstandsfähiger Demokratien“ (JOIN(2025)0791),

– gestützt auf den Vertrag über die Europäische Union (EUV), insbesondere Artikel 2 zu den Grundwerten der EU, Artikel 10 zum demokratischen Leben und Artikel 21 zum auswärtigen Handeln,

– gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 114 zum Binnenmarkt und Artikel 222 zur Solidarität,

– unter Hinweis auf die Charta der Grundrechte der Europäischen Union,

– unter Hinweis auf die Verordnung (EU, Euratom) Nr. 2025/2445 des Europäischen Parlaments und des Rates vom 26. November 2025 über das Statut und die Finanzierung europäischer politischer Parteien und europäischer politischer Stiftungen[2],

– unter Hinweis auf die Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz)[3],

– unter Hinweis auf die Verordnung (EU) 2024/1624 des Europäischen Parlaments und des Rates vom 31. Mai 2024 zur Verhinderung der Nutzung des Finanzsystems für Zwecke der Geldwäsche oder der Terrorismusfinanzierung[4],

– unter Hinweis auf die Verordnung (EU) 2024/1083 des Europäischen Parlaments und des Rates vom 11. April 2024 zur Schaffung eines gemeinsamen Rahmens für Mediendienste im Binnenmarkt und zur Änderung der Richtlinie 2010/13/EU

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

(Europäisches Medienfreiheitsgesetz)[5],

– unter Hinweis auf die Richtlinie (EU) 2024/1069 des Europäischen Parlaments und des Rates vom 11. April 2024 über den Schutz von Personen, die sich öffentlich beteiligen, vor offensichtlich unbegründeten Klagen oder missbräuchlichen Gerichtsverfahren („strategische Klagen gegen öffentliche Beteiligung“)[6],

– unter Hinweis auf die Verordnung (EU) 2024/900 des Europäischen Parlaments und des Rates vom 13. März 2024 über die Transparenz und das Targeting politischer Werbung[7],

– unter Hinweis auf die Verordnung (EU, EURATOM) 2023/2841 des Europäischen Parlaments und des Rates vom 13. Dezember 2023 zur Festlegung von Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in den Organen, Einrichtungen und sonstigen Stellen der Union[8],

– unter Hinweis auf die Verordnung (EU) 2023/1114 des Europäischen Parlaments und des Rates vom 31. Mai 2023 über Märkte für Kryptowerte und zur Änderung der Verordnungen (EU) Nr. 1093/2010 und (EU) Nr. 1095/2010 sowie der Richtlinien 2013/36/EU und (EU) 2019/1937[9] (Verordnung über Märkte für Kryptowerte),

– unter Hinweis auf die Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die Resilienz kritischer Einrichtungen und zur Aufhebung der Richtlinie 2008/114/EG des Rates[10],

– unter Hinweis auf die Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie)[11],

– unter Hinweis auf die Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Gesetz über digitale Dienste)[12] und die Verordnung (EU) 2022/1925 des Europäischen Parlaments und des Rates vom 14. September 2022 über bestreitbare und faire Märkte im digitalen Sektor und zur Änderung der Richtlinien (EU) 2019/1937 und (EU) 2020/1828 (Gesetz über digitale Märkte)[13],

---

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

– unter Hinweis auf die Verordnung (EU) 2021/692 des Europäischen Parlaments und des Rates vom 28. April 2021 zur Einrichtung des Programms „Bürgerinnen und Bürger, Gleichstellung, Rechte und Werte“ und zur Aufhebung der Verordnung (EU) Nr. 1381/2013 des Europäischen Parlaments und des Rates und der Verordnung (EU) Nr. 390/2014 des Rates[14],

– unter Hinweis auf die Richtlinie (EU) 2019/1937 des Europäischen Parlaments und des Rates vom 23. Oktober 2019 zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden[15],

– unter Hinweis auf die Richtlinie 2010/13/EU des Europäischen Parlaments und des Rates vom 10. März 2010 zur Koordinierung bestimmter Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Bereitstellung audiovisueller Mediendienste (Richtlinie über audiovisuelle Mediendienste)[16],

– unter Hinweis auf den Beschluss 2014/145/GASP des Rates vom 17. März 2014 über restriktive Maßnahmen angesichts von Handlungen, die die territoriale Unversehrtheit, Souveränität und Unabhängigkeit der Ukraine untergraben oder bedrohen[17], und auf die Verordnung (EU) Nr. 269/2014 des Rates vom 17. März 2014 über restriktive Maßnahmen angesichts von Handlungen, die die territoriale Unversehrtheit, Souveränität und Unabhängigkeit der Ukraine untergraben oder bedrohen[18],

– unter Hinweis auf den Beschluss 2014/119/GASP des Rates vom 5. März 2014 über restriktive Maßnahmen gegen bestimmte Personen, Organisationen und Einrichtungen angesichts der Lage in der Ukraine[19] und auf die Verordnung (EU) Nr. 208/2014 des Rates vom 5. März 2014 über restriktive Maßnahmen gegen bestimmte Personen, Organisationen und Einrichtungen angesichts der Lage in der Ukraine[20],

– unter Hinweis auf den Beschluss 2014/512/GASP des Rates vom 31. Juli 2014 über restriktive Maßnahmen angesichts der Handlungen Russlands, die die Lage in der Ukraine destabilisieren[21], und die Verordnung (EU) Nr. 833/2014 des Rates vom 31. Juli 2014 über restriktive Maßnahmen angesichts der Handlungen Russlands, die die Lage in der Ukraine destabilisieren[22],

– unter Hinweis auf den Beschluss (GASP) 2022/266 des Rates vom 23. Februar 2022 über restriktive Maßnahmen als Reaktion auf die Anerkennung der nicht von der Regierung kontrollierten Gebiete der ukrainischen Regionen Donezk und Luhansk und die Anordnung der Entsendung russischer Streitkräfte in diese Gebiete[23] und auf die Verordnung (EU) 2022/263 des Rates vom 23. Februar 2022 über restriktive Maßnahmen als Reaktion auf die Anerkennung der nicht von der Regierung

---

[14] ABl. L 156 vom 5.5.2021, S. 1, ELI: http://data.europa.eu/eli/reg/2021/692/oj.
[15] ABl. L 305 vom 26.11.2019, S. 17, ELI: http://data.europa.eu/eli/dir/2019/1937/oj.
[16] ABl. L 95 vom 15.4.2010, S. 1, ELI: http://data.europa.eu/eli/dir/2010/13/oj.
[17] ABl. L 78 vom 17.3.2014, S. 16, ELI: http://data.europa.eu/eli/dec/2014/145(1)/oj.
[18] ABl. L 78 vom 17.3.2014, S. 6, ELI: http://data.europa.eu/eli/reg/2014/269/oj.
[19] ABl. L 66 vom 6.3.2014, S. 26, ELI: http://data.europa.eu/eli/dec/2014/119(1)/oj.
[20] ABl. L 66 vom 6.3.2014, S. 1, ELI: http://data.europa.eu/eli/reg/2014/208/oj.
[21] ABl. L 229 vom 31.7.2014, S. 13, ELI: http://data.europa.eu/eli/dec/2014/512/oj.
[22] ABl. L 229 vom 31.7.2014, S. 1, ELI: http://data.europa.eu/eli/reg/2014/833/oj.
[23] ABl. L 42 I vom 23.2.2022, S. 109, ELI: http://data.europa.eu/eli/dec/2022/266/oj.

kontrollierten Gebiete der ukrainischen Regionen Donezk und Luhansk und die Entsendung russischer Streitkräfte in diese Gebiete[24],

– unter Hinweis auf den Beschluss 2012/642/GASP des Rates vom 15. Oktober 2012 über restriktive Maßnahmen gegen Belarus[25] und auf die Verordnung (EG) Nr. 765/2006 des Rates vom 18. Mai 2006 über restriktive Maßnahmen gegen Präsident Lukaschenko und verschiedene belarussische Amtsträger[26],

– unter Hinweis auf den Beschluss (GASP) 2023/1532 des Rates vom 20. Juli 2023 über restriktive Maßnahmen angesichts der militärischen Unterstützung des Angriffskriegs Russlands gegen die Ukraine durch Iran[27] und auf die Verordnung (EU) 2023/1529 des Rates vom 20. Juli 2023 über restriktive Maßnahmen angesichts der militärischen Unterstützung des Angriffskriegs Russlands gegen die Ukraine durch Iran[28],

– unter Hinweis auf den Beschluss (GASP) 2024/1603 des Rates vom 31. Mai 2024 zur Änderung des Beschlusses (GASP) 2016/849 über restriktive Maßnahmen gegen die Demokratische Volksrepublik Korea[29] und auf die Durchführungsverordnung (EU) 2024/1602 des Rates vom 31. Mai 2024 zur Durchführung der Verordnung (EU) 2017/1509 über restriktive Maßnahmen gegen die Demokratische Volksrepublik Korea[30],

– unter Hinweis auf den Vorschlag der Kommission vom 16. Juli 2025 für eine Verordnung des Rates zur Festlegung des Mehrjährigen Finanzrahmens für die Jahre 2028 bis 2034 (COM(2025)0571),

– unter Hinweis auf die vom Europäischen Parlament am 27. November 2025 angenommenen Änderungsanträge zu dem Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Anforderungen im Binnenmarkt an die Transparenz der Interessenvertretung im Auftrag von Drittländern und zur Änderung der Richtlinie (EU) 2019/1937 (COM(2023)0637 – C9-0464/2023 – 2023/0463(COD))[31],

– unter Hinweis auf seine Entschließung vom 9. Oktober 2025 zu einer geeinten Reaktion auf die jüngsten Verletzungen des Luftraums und die jüngsten Bedrohungen der kritischen Infrastruktur der EU-Mitgliedstaaten durch Russland[32],

– unter Hinweis auf seine Entschließung vom 18. Juni 2025 über den Bericht der Kommission über die Rechtsstaatlichkeit 2024[33],

---

[24] ABl. L 42 I vom 23.2.2022, S. 77, ELI: http://data.europa.eu/eli/reg/2022/263/oj.
[25] ABl. L 285 vom 17.10.2012, S. 1, ELI: http://data.europa.eu/eli/dec/2012/642/oj.
[26] ABl. L 134 vom 20.5.2006, S. 1, ELI: http://data.europa.eu/eli/reg/2006/765/oj.
[27] ABl. L 186 vom 25.7.2023, S. 20, ELI: http://data.europa.eu/eli/dec/2023/1532/oj.
[28] ABl. L 186 vom 25.7.2023, S. 1, ELI: http://data.europa.eu/eli/reg/2023/1529/oj.
[29] ABl. L, 2024/1603, 31.5.2024, ELI: http://data.europa.eu/eli/dec/2024/1603/oj.
[30] ABl. L, 2024/1602, 31.5.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/1602/oj.
[31] Angenommene Texte, P10_TA(2025)0306.
[32] Angenommene Texte, P10_TA(2025)0230.
[33] ABl. C, C/2025/6259, 19.12.2025, ELI: http://data.europa.eu/eli/C/2025/6259/oj.

– unter Hinweis auf seine Entschließung vom 7. Mai 2025 zu einem neu gestalteten langfristigen Haushalt für die Union in einer Welt im Wandel[34],

– unter Hinweis auf seine Entschließung vom 13. Juli 2023 zu Empfehlungen für die Reform der Vorschriften des Europäischen Parlaments zu Transparenz, Integrität, Rechenschaftspflicht und Korruptionsbekämpfung[35],

– unter Hinweis auf seine Entschließung vom 1. Juni 2023 zu Einflussnahme aus dem Ausland auf alle demokratischen Prozesse in der Europäischen Union, einschließlich Desinformation[36],

– unter Hinweis auf seine Entschließung vom 15. Dezember 2022 zum Korruptionsverdacht gegen Katar und zu der umfassenderen Notwendigkeit von Transparenz und Rechenschaftspflicht in den Organen der EU[37],

– unter Hinweis auf seine Entschließung vom 23. November 2022 zur Einstufung der Russischen Föderation als dem Terrorismus Vorschub leistender Staat[38],

– unter Hinweis auf seine Entschließung vom 9. März 2022 zu Einflussnahme aus dem Ausland auf alle demokratischen Prozesse in der Europäischen Union, einschließlich Desinformation[39],

– unter Hinweis auf seine Entschließung vom 8. März 2022 zum schrumpfenden Handlungsspielraum für die Zivilgesellschaft in der EU[40],

– unter Hinweis auf seine Entschließung vom 20. Oktober 2021 zu Europas Medien in der digitalen Dekade: Ein Aktionsplan zur Unterstützung der Erholung und des Wandels[41],

– unter Hinweis auf seine Entschließung vom 23. November 2016 zu dem Thema „Strategische Kommunikation der EU, um gegen sie gerichteter Propaganda von Dritten entgegenzuwirken“[42],

– unter Hinweis auf seine Empfehlung vom 15. Juni 2023 an den Rat und die Kommission nach der Prüfung von behaupteten Verstößen gegen das Unionsrecht und Missständen bei der Anwendung desselben im Zusammenhang mit dem Einsatz von Pegasus und ähnlicher Überwachungs- und Spähsoftware[43],

– unter Hinweis auf seine Empfehlung vom 23. November 2022 an den Rat, die Kommission und den Vizepräsidenten der Kommission und Hohen Vertreter der Union für Außen- und Sicherheitspolitik zu der neuen Strategie der EU für die Erweiterung[44],

---

[34] Angenommene Texte, P10_TA(2025)0090.
[35] ABl. C, C/2024/4011, 17.7.2024, ELI: http://data.europa.eu/eli/C/2024/4011/oj.
[36] ABl. C, C/2023/1226, 21.12.2023, ELI: http://data.europa.eu/eli/C/2023/1226/oj.
[37] ABl. C 177 vom 17.5.2023, S 109.
[38] ABl. C 167 vom 11.5.2023, S. 18.
[39] ABl. C 347 vom 9.9.2022, S. 61.
[40] ABl. C 347 vom 9.9.2022, S. 2.
[41] ABl. C 184 vom 5.5.2022, S. 71.
[42] ABl. C 224 vom 27.6.2018, S. 58.
[43] ABl. C, C/2024/494, 23.1.2024, ELI: http://data.europa.eu/eli/C/2024/494/oj.
[44] ABl. C 167 vom 11.5.2023, S. 105.

– unter Hinweis auf seine Empfehlung vom 13. März 2019 an den Rat und die Vizepräsidentin der Kommission und Hohe Vertreterin der Union für Außen- und Sicherheitspolitik zu der Bestandsaufnahme der Folgemaßnahmen, die zwei Jahre nach dem Bericht des Europäischen Parlaments über das Thema „Strategische Kommunikation der EU, um gegen sie gerichteter Propaganda von Dritten entgegenzuwirken“ durch den EAD ergriffen wurden[45],

– unter Hinweis auf die Folgemaßnahmen der Kommission zu den Empfehlungen des Parlaments in seinen Entschließungen,

– unter Hinweis auf die Mitteilung der Kommission vom 12. November 2025 mit dem Titel „EU-Strategie für die Zivilgesellschaft“ (COM(2025)0790),

– unter Hinweis auf die Mitteilung der Kommission vom 1. April 2025 mit dem Titel „ProtectEU – eine Europäische Strategie für die innere Sicherheit“ (COM(2025)0148),

– unter Hinweis auf die Mitteilung der Kommission vom 24. Juli 2024 mit dem Titel „Bericht über die Rechtsstaatlichkeit 2024 – Die Lage der Rechtsstaatlichkeit in der Europäischen Union“ (COM(2024)0800),

– unter Hinweis auf die Mitteilung der Kommission vom 8. Juli 2025 mit dem Titel „Bericht über die Rechtsstaatlichkeit 2025 – Die Lage der Rechtsstaatlichkeit in der Europäischen Union“ (COM(2025)0900),

– unter Hinweis auf die Mitteilung der Kommission vom 12. Dezember 2023 über die Verteidigung der Demokratie (COM(2023)0630),

– unter Hinweis auf die Mitteilung der Kommission vom 3. Dezember 2020 mit dem Titel „Europäischer Aktionsplan für Demokratie“ (COM(2020)0790),

– unter Hinweis auf die Gemeinsamen Mitteilungen der Kommission und der Hohen Vertreterin der Union für Außen- und Sicherheitspolitik vom 5. Dezember 2018 mit dem Titel „Aktionsplan gegen Desinformation“ (JOIN(2018)0036) und vom 14. Juni 2019 mit dem Titel „Bericht über die Umsetzung des Aktionsplans gegen Desinformation“ (JOIN(2019)0012),

– unter Hinweis auf die Sicherheits- und Verteidigungspartnerschaft zwischen der Europäischen Union und dem Vereinigten Königreich Großbritannien und Nordirland, die am 19. Mai 2025 eingerichtet wurde,

– unter Hinweis auf die politischen Leitlinien für die Amtszeit der Kommission 2024-2029, die von der Präsidentin der Kommission Ursula von der Leyen am 18. Juli 2024 vorgelegt wurden, mit dem Titel „Europa hat die Wahl“,

– unter Hinweis auf den Durchführungsbeschluss der Kommission vom 28. März 2025 zur Finanzierung des Programms „Digitales Europa“ und zur Annahme des Mehrjahres-Arbeitsprogramms 2025-2027 (C(2025)1839),

– unter Hinweis auf den Verhaltenskodex zur Bekämpfung von Desinformation,

[45] ABl. C 23 vom 21.1.2021, S. 152.

– unter Hinweis auf den Bericht der Kooperationsgruppe für Netz- und Informationssysteme vom 23. Januar 2020 mit dem Titel „EU-Instrumentarium für die 5G-Cybersicherheit“,

– unter Hinweis auf den Bericht von Sauli Niinistö, ehemaliger Präsident der Republik Finnland, in seiner Eigenschaft als Sonderberater der Präsidentin der Europäischen Kommission vom 30. Oktober 2024 mit dem Titel „Safer Together – Strengthening Europe’s Civilian and Military Preparedness and Readiness“ (Gemeinsam für mehr Sicherheit – Stärkung der zivilen und militärischen Vorsorge und Bereitschaft Europas),

– unter Hinweis auf die Empfehlung (EU) 2023/2829 der Kommission vom 12. Dezember 2023 für inklusive und stabile Wahlverfahren in der Union und für die Stärkung des europäischen Charakters und eine effiziente Durchführung der Wahlen zum Europäischen Parlament[46],

– unter Hinweis auf die Empfehlung (EU) 2023/2836 der Kommission vom 12. Dezember 2023 zur Förderung der Mitwirkung und der wirksamen Beteiligung von Bürgerinnen und Bürgern und Organisationen der Zivilgesellschaft an politischen Entscheidungsprozessen[47],

– unter Hinweis auf die Einrichtung des Europäischen Kooperationsnetzes für Wahlen (ECNE) im Jahr 2019 durch die Kommission,

– unter Hinweis auf die Pressemitteilung der Kommission vom 13. November 2025 zur Einleitung der Untersuchung eines potenziellen Verstoßes gegen das Gesetz über digitale Märkte durch Google in Form der Herabstufung der Inhalte von Medienverlagen in den Suchergebnissen,

– unter Hinweis auf die Schlussfolgerungen des Rates vom 21. Mai 2024 zu dem Thema „Die Zukunft der Cybersicherheit – gemeinsam umsetzen und sich schützen“,

– unter Hinweis auf die Schlussfolgerungen des Rates vom 17. Oktober 2022 zur Sicherheit von IKT-Lieferketten,

– unter Hinweis auf die Empfehlung des Rates vom 8. Dezember 2022 für eine unionsweite koordinierte Vorgehensweise zur Stärkung der Resilienz kritischer Infrastruktur[48],

– unter Hinweis auf den Beschluss (GASP) 2023/855 des Rates vom 24. April 2023 über eine Partnerschaftsmission der Europäischen Union in Moldau (EUPM Moldova)[49],

– unter Hinweis auf den Aktionsplan mit dem Titel „Ein Strategischer Kompass für Sicherheit und Verteidigung – Für eine Europäische Union, die ihre Bürgerinnen und Bürger, Werte und Interessen schützt und zu Weltfrieden und internationaler Sicherheit beiträgt“, der am 21. März 2022 vom Rat und am 25. März 2022 vom Europäischen Rat gebilligt wurde,

[46] ABl. L, 2023/2829, 20.12.2023, ELI: http://data.europa.eu/eli/reco/2023/2829/oj.
[47] ABl. L, 2023/2836, 20.12.2023, ELI: http://data.europa.eu/eli/reco/2023/2836/oj.
[48] ABl. C 20 vom 20.1.2023, S. 1.
[49] ABl. L 110 vom 25.4.2023, S. 30, ELI: http://data.europa.eu/eli/dec/2023/855/oj.

– unter Hinweis auf die Mitteilung der Länder Litauen, Dänemark, Estland, Finnland, Deutschland, Lettland, Slowenien und Spanien anlässlich der Sitzung des Rates (Verkehr, Telekommunikation und Energie) vom 6. Juni 2025 mit dem Titel „Aufruf zu gemeinsamen Maßnahmen als Reaktion auf Bedrohungen durch gezielte Störung (Jamming) und Fälschung von GPS-Signalen (Spoofing) von globalen Satellitennavigationssystemen (GNSS)“,

– unter Hinweis auf die Interinstitutionelle Vereinbarung vom 20. Mai 2021 zwischen dem Europäischen Parlament, dem Rat der Europäischen Union und der Europäischen Kommission über ein verbindliches Transparenz-Register[50],

– unter Hinweis auf den Sonderbericht Nr. 05/2022 des Europäischen Rechnungshofs vom 29. März 2022 mit dem Titel „Cybersicherheit: Organe, Einrichtungen und sonstige Stellen der EU sind insgesamt nicht ausreichend gegen Bedrohungen gewappnet“,

– unter Hinweis auf die globalen Grundsätze der Vereinten Nationen für Informationsintegrität – Empfehlungen für Maßnahmen verschiedener Akteure, die am 24. Juni 2024 veröffentlicht wurden,

– unter Hinweis auf den Internationalen Pakt über bürgerliche und politische Rechte, insbesondere auf Artikel 20,

– unter Hinweis auf das Seerechtsübereinkommen der Vereinten Nationen vom 10. Dezember 1982, das am 16. November 1994 in Kraft getreten ist,

– unter Hinweis auf die Artikel über die Verantwortlichkeit von Staaten für völkerrechtswidrige Handlungen, die im November 2001 angenommen wurden,

– unter Hinweis auf die Erklärung von Reykjavik, die beim 4. Gipfeltreffen der Staats- und Regierungschefs der Mitgliedstaaten des Europarates vom 16./17. Mai 2023 angenommen wurde,

– unter Hinweis auf den Krisenreaktionsmechanismus der G7, der beim G7-Gipfel in Charlevoix vom 8./9. Juni 2018 eingerichtet wurde,

– unter Hinweis auf das Arbeitspapier zu wiederholten GNSS-Hochfrequenzstörungen in den baltischen, östlichen und nördlichen Regionen Europas und ihren Auswirkungen auf die Sicherheit der internationalen Zivilluftfahrt, die der Internationalen Zivilluftfahrt-Organisation am 13. Juni 2025 von den Ländern Estland, Finnland, Lettland, Litauen, Polen und Schweden vorgelegt wurde,

– unter Hinweis auf den Bericht über das Endergebnis der Konferenz zur Zukunft Europas, der am 9. Mai 2022 veröffentlicht wurde, insbesondere die Vorschläge 27 und 37,

– unter Hinweis auf die vom Sonderausschuss für den Europäischen Schutzschild für die Demokratie des Europäischen Parlaments in Auftrag gegebene Studie zum Thema „Stärkung der Resilienz – Auf dem Weg zum Europäischen Schutzschild für die

[50] ABl. L 207 vom 11.6.2021, S. 1, ELI: http://data.europa.eu/eli/agree_interinstit/2021/611/oj.

Demokratie“, die im Oktober 2025 von der Generaldirektion Bürgerrechte, Justiz und institutionelle Angelegenheiten des Europäischen Parlaments veröffentlicht wurde[51],

– unter Hinweis auf den ersten, zweiten und dritten Bericht des Europäischen Auswärtigen Dienstes (EAD) über Bedrohungen durch Informationsmanipulation und Einflussnahme aus dem Ausland,

– unter Hinweis auf den Bericht der Agentur der Europäischen Union für Cybersicherheit (ENISA) vom 1. Oktober 2025 mit dem Titel „ENISA Threat Landscape 2025“ (ENISA-Gefahrenumfeld 2025),

– unter Hinweis auf den Bericht von Europol mit dem Titel „EU Serious and Organised Crime Threat Assessment – The changing DNA of serious and organised crime“ (Bewertung der Bedrohungslage im Bereich der schweren und organisierten Kriminalität – Neue Formen schwerer und organisierter Kriminalität), der 2025 veröffentlicht wurde,

– unter Hinweis auf den Bericht der Abteilung für die Koordinierung der Algorithmusaufsicht der niederländischen Datenschutzbehörde vom Oktober 2025 mit dem Titel „AI chatbots as voting aid“ (KI-Chatbots als Wahlhilfe),

– unter Hinweis auf die von der italienischen Regulierungsbehörde für Kommunikation (AGCOM) am 3. September 2025 angenommenen Maßnahmen in Bezug auf Influencer,

– unter Hinweis auf den Verhaltenskodex für Influencer-Werbung, der am 7. Juli 2025 in Spanien von AUTOCONTROL angenommen wurde,

– unter Hinweis auf die Warnung der tschechischen nationalen Agentur für Cyber- und Informationssicherheit (NÚKIB) vom 3. September 2025 zu Cybersicherheitsbedrohungen in Verbindung mit der Übertragung von Daten an und Fernverwaltung durch die Volksrepublik China und ihre Sonderverwaltungsregionen,

– unter Hinweis auf den Bericht mit dem Titel „Manipulation d’algorithmes et instrumentalisation d’influenceurs: enseignements de l’élection présidentielle en Roumanie & risques pour la France“ (Manipulation von Algorithmen und Instrumentalisierung von Influencern: Aus der Präsidentschaftswahl in Rumänien gezogene Lehren und Risiken für Frankreich), der im Februar 2025 vom Dienst für Wachsamkeit und Schutz vor digitaler Einflussnahme aus dem Ausland (VIGINUM) der französischen Regierung veröffentlicht wurde,

– unter Hinweis auf das 2020 von dem finnischen Netzwerk Mediapooli herausgegebene Influencer-Handbuch,

– unter Hinweis auf den Bericht des US-Außenministeriums vom August 2020 mit dem Titel „Pillars of Russia’s Disinformation and Propaganda Ecosystem“ (Säulen des russischen Desinformations- und Propaganda-Ökosystems),

[51] Studie: „Stärkung der Resilienz – Auf dem Weg zum Europäischen Schutzschild für die Demokratie“, Europäisches Parlament, Generaldirektion Bürgerrechte, Justiz und institutionelle Angelegenheiten, Fachabteilung Justiz, bürgerliche Freiheiten und institutionelle Angelegenheiten, Oktober 2025.

– unter Hinweis auf den gemeinsamen Ratgeber zu Cybersicherheit der US-amerikanischen Agentur für Cybersicherheit und Infrastruktursicherheit, der Nationalen Sicherheitsagentur der Vereinigten Staaten (National Security Agency – NSA), des FBI und internationaler Partner vom August 2025 mit dem Titel „Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage Systems“ (Bekämpfung chinesischer staatlich finanzierter Akteure, die Netzwerke weltweit kompromittieren, um globale Spionagesysteme zu versorgen),

– unter Hinweis auf den Bericht von „Reporter ohne Grenzen“ vom 25. September 2025 mit dem Titel „The Propaganda Monitor: The Russian Edition“ (Propaganda-Monitor: Russische Fassung),

– unter Hinweis auf den vom Zentrum für Medienpluralismus und -freiheit beim Europäischen Hochschulinstitut veröffentlichten Artikel vom 1. November 2025 mit dem Titel „Influencers as news creators: implications for media regulation“ (Influencer als neue Schöpfer: Auswirkungen auf Medienvorschriften),

– unter Hinweis auf den am 28. Oktober 2025 vom Konsortium AlgoSoc veröffentlichten Artikel mit dem Titel „1 in 10 Dutch citizens are likely to ask AI for election advice. This is why they shouldn’t“ (Ein Zehntel aller Niederländer nutzt wahrscheinlich KI für Wahlberatung – Gründe, die dagegen sprechen),

– unter Hinweis auf den Bericht von What to Fix vom Juni 2025 mit dem Titel „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“ (Finanzierung sanktionierter Unternehmen: Wie Meta Platforms Ireland Ltd. möglicherweise gegen EU-Sanktionen verstoßen und über die Umsatzumverteilungsprogramme von Facebook Gelder an RT, Sputnik und andere von der EU sanktionierte Einrichtungen weitergeleitet hat),

– unter Hinweis auf den Sonderbericht von NewsGuard vom 6. März 2025 mit dem Titel „A Well-funded Moscow-based Global “News” Network has Infected Western Artificial Intelligence with Russian Propaganda“ (Ein finanzstarkes globales „Nachrichten“-Netzwerk mit Sitz in Moskau hat die westliche künstliche Intelligenz mit russischer Propaganda infiziert),

– unter Hinweis auf den Bericht von Media Freedom Rapid Response mit dem Titel „Mapping Media Freedom – Monitoring Report 2024“ (Medienfreiheit kartografieren – Monitoring-Bericht 2024), der im Februar 2025 veröffentlicht wurde,

– unter Hinweis auf den Bericht des Weltwirtschaftsforums vom Januar 2025 mit dem Titel „Global Cybersecurity Outlook 2025“ (Globaler Ausblick auf die Cybersicherheit 2025),

– unter Hinweis auf den am 26. Februar 2024 von VSquare, Delfi Estonia und Partner-Medienorganisationen veröffentlichten Investigativbericht mit dem Titel „Kremlin Leaks: Secret Files Reveal How Putin Pre-Rigged his Reelection“ (Kreml-Leaks: Geheime Akten enthüllen, wie Putin seine Wiederwahl manipuliert hat),

– unter Hinweis auf den ethischen Verhaltenskodex für Influencer und Ersteller von Inhalten in den sozialen Medien, der 2024 vom Aspen Institute Germany veröffentlicht wurde,

– unter Hinweis auf den am 4. Mai 2023 von Debunk.org veröffentlichten Artikel mit dem Titel „Kremlin spent 1.9 billion USD on propaganda last year, the budget exceeded by a quarter“ (Kreml gab im vergangenen Jahr 1,9 Mrd. USD für Propaganda aus, das Budget wurde um ein Viertel überschritten),

– unter Hinweis auf die Erklärung des Außenministeriums der Russischen Föderation vom 28. Dezember 2024 zu Maßnahmen als Reaktion auf das 15. Sanktionspaket der EU gegen Russland, in der es die Erweiterung der Liste der EU-Beamten und -Staatsbürger, denen die Einreise in das Land untersagt ist, bekanntgab,

– unter Hinweis auf den Artikel der russischen Nachrichtenagentur TASS vom 28. Dezember 2024 mit dem Titel „Russia substantially expands blacklist of EU officials in response to sanctions – MFA“ (Russland erweitert als Reaktion auf Sanktionen die schwarze Liste von EU-Beamten erheblich – Außenministerium),

– unter Hinweis auf die Erklärung von TikTok vom Dezember 2024 zur Fortführung des Schutzes der Integrität von TikTok während der Wahl in Rumänien,

– unter Hinweis auf die Erklärung des European Solar Manufacturing Council vom 30. April 2025 mit dem Titel „Restrict Remote Access of PV Inverters from High-Risk Vendors“ (Einschränkung des Fernzugriffs auf PV-Wechselrichter von risikoreichen Anbietern), worin er vor den Risiken für die Energiesouveränität Europas aufgrund unregulierter und ferngesteuerter Funktionen von PV-Wechselrichtern von risikoreichen, außereuropäischen Herstellern warnte,

– gestützt auf Artikel 55 seiner Geschäftsordnung,

– unter Hinweis auf den Bericht des Sonderausschusses für den Europäischen Schutzschild für die Demokratie (A10-0000/2025),

A. in der Erwägung, dass die Kommission und die Hohe Vertreterin der Union für Außen- und Sicherheitspolitik am 12. November 2025 eine gemeinsame Erklärung zur Einrichtung des Europäischen Schutzschilds für die Demokratie vorgelegt haben, in der eine Reihe von Maßnahmen dargelegt werden mit dem Ziel, starke und resiliente Demokratien überall in der EU zu stärken, zu schützen und zu fördern;

B. in der Erwägung, dass das Europäische Zentrum für demokratische Resilienz das Herzstück des Europäischen Schutzschilds für die Demokratie bildet; in der Erwägung, dass beide Sonderausschüsse zu Einflussnahme aus dem Ausland auf alle demokratischen Prozesse in der Europäischen Union, einschließlich Desinformation, des Parlaments (INGE und INGE 2) bereits gefordert hatten, dass eine EU-Struktur zur Bekämpfung von ausländischer Informationsmanipulation und Einmischung eingerichtet wird;

C. in der Erwägung, dass aus den jüngsten Berichten des EAD über Bedrohungen durch ausländische Informationsmanipulation und Einmischung hervorgeht, dass das Verständnis in Bezug auf die Methoden böswilliger Akteure, die technische

Infrastruktur und die angestrebten Narrative zusehends wächst, dass sich dieses Situationsbewusstsein jedoch noch nicht in nachhaltigen operativen Mechanismen niedergeschlagen hat, die es der EU ermöglichen, rechtzeitig koordinierte Gegenmaßnahmen zu ergreifen; in der Erwägung, dass mit feindseligen Kampagnen zur Informationsmanipulation vorrangig versucht wird, die Verflechtung der Einrichtungen der EU ins Visier zu nehmen; in der Erwägung, dass es in der EU kein gemeinsames Vorgehen zur Bekämpfung von ausländischer Informationsmanipulation und Einmischung sowie von Desinformation gibt, wobei die Unterschiede zwischen den einzelnen Mitgliedstaaten im Hinblick auf ihre Kapazitäten beträchtlich sind und es keinen übergeordneten strategischen Rahmen gibt, durch den die operativen Reaktionen und die Informationen über Bedrohungen zueinander in Beziehung gesetzt werden;

D. in der Erwägung, dass das ECNE, das Schnellwarnsystem (RAS) und die Europäische Beobachtungsstelle für digitale Medien (EDMO) wichtige Elemente der allgemeinen Resilienz der EU gegenüber ausländischer Informationsmanipulation und Einmischung sowie Desinformation sind, ihre Relevanz jedoch stark eingeschränkt ist, da es keine spezielle operative Struktur innerhalb der EU gibt, die befugt ist, Maßnahmen zur Stärkung der Resilienz sowie Krisenreaktions- und Eskalationsmechanismen zu koordinieren, wodurch nationale operative Kapazitäten mit der Koordinierung auf EU-Ebene in Verbindung gebracht werden;

E. in der Erwägung, dass die Bedrohungen, die von ausländischer Informationsmanipulation und Einmischung sowie von Desinformation ausgehen, nicht nur einzelne Mitgliedstaaten betreffen, sondern einen Angriff auf das Herzstück des europäischen Projekts darstellen; in der Erwägung, dass Maßnahmen ausländischer Informationsmanipulation und Einmischung systematisch auf die in Artikel 2 EUV verankerten demokratischen Grundwerte und den in Artikel 1 EUV verankerten Grundsatz offener und transparenter Entscheidungsprozesse ausgerichtet sind, und zwar in einer Art und Weise, die den Interessen der EU schadet;

F. in der Erwägung, dass einzelne Mitgliedstaaten, die in spezielle operative Strukturen mit klaren Statuten und Mandaten sowie ausreichender Finanz- und Personalausstattung investiert haben, aufzeigen, was machbar ist; in der Erwägung, dass in diesem Zusammenhang insbesondere der französische Dienst VIGINUM und die schwedische Agentur für psychologische Verteidigung erwähnt werden können;

G. in der Erwägung, dass fragmentierte nationale Einrichtungen, was ihre Anpassungsfähigkeit anbelangt, mit dem Tempo, in dem künstliche Intelligenz (KI) und Deepfake-Technologien weiterentwickelt werden, nicht Schritt halten können; in der Erwägung, dass ohne ein koordiniertes Vorgehen der EU und ohne klare operative Kapazitäten zunehmend die Angreifer und nicht die Verteidiger von den technologischen Vorteilen profitieren werden;

H. in der Erwägung, dass sich aufgrund der Tatsache, dass sich das Gesetz über digitale Dienste, das Gesetz über digitale Märkte, die Verordnung über künstliche Intelligenz und das Europäische Medienfreiheitsgesetz zeitgleich in frühen Phasen der Durchführung befinden, die Gelegenheit bietet, umfassende Mechanismen zur Abwehr von ausländischer Informationsmanipulation und Einmischung zu entwickeln;

I. in der Erwägung, dass demokratische Gesellschaften in der EU verstärkt von hybriden Bedrohungen, von Desinformation sowie von ausländischer Informationsmanipulation und Einmischung betroffen sind, insbesondere im digitalen Bereich; in der Erwägung, dass das Internet die Verbreitung neuer Manipulationstechniken ermöglicht, darunter a) die unehrliche Nutzung sozialer Medien durch die Verwendung automatisierter Softwareprogramme, gefälschter Social-Media-Konten und von Trollfabriken, botbasierter Verstärkung und Steuerung, b) Astroturfing und Informationsüberflutung zur Beeinflussung der öffentlichen Debatte im Internet, c) Personalisierung, Verfolgung und Microtargeting von Einzelpersonen, d) Websites, die amtliche Quellen nachahmen, e) das künstliche Aufblasen spaltender Inhalte, f) die Verwendung synthetischer Inhalte wie Deepfakes und anderer KI-generierter Inhalte sowie g) Empfehlungssysteme, mit denen durch Polarisierung das Kaufverhalten manipuliert werden soll;

J. in der Erwägung, dass Online-Plattformen die Entscheidung, welche Inhalte im Feed eines Nutzers angezeigt werden, auf Grundlage von Informationen zu Präferenzen und Schwächen jedes einzelnen Nutzers fällen, wodurch sie einen größeren Einfluss haben als traditionelle Verleger;

K. in der Erwägung, dass die EU kürzlich eine Reihe umfassender Rechtsakte angenommen hat, um für Sicherheit und Transparenz im Internet zu sorgen, darunter das Gesetz über digitale Dienste, die Verordnung über die Transparenz und das Targeting politischer Werbung sowie die Verordnung über künstliche Intelligenz; in der Erwägung, dass diese Rechtsakte einen wichtigen Schritt in die richtige Richtung darstellen, d. h. digitale Plattformen zur Rechenschaft zu ziehen, demokratische Prozesse zu schützen, die Transparenz zu erhöhen und die freie Meinungsäußerung zu bewahren; in der Erwägung, dass ihre Durchsetzung aber nach wie vor eine Herausforderung darstellt;

L. in der Erwägung, dass der Einsatz von KI neue Möglichkeiten für die Stärkung der Wahlleitung und der Wahlaufsicht bietet, z. B. durch die Aufdeckung ungewöhnlicher Online-Aktivitäten und koordinierten manipulativen Verhaltens; in der Erwägung, dass der Einsatz von KI, einschließlich generativer KI-Modelle und Deepfakes, auch mit beträchtlichen Herausforderungen für die Informationsintegrität und Wahlprozesse einhergeht; in der Erwägung, dass in seriösen Berichten die Tätigkeiten des in Moskau ansässigen Desinformationsnetzwerks „Pravda“ aufgedeckt wurden, das große Sprachmodelle mit kremlfreundlichen Narrativen, die Neutralität und Faktenbasiertheit nachahmen sollen, vorsätzlich angegriffen und infiltriert hat; in der Erwägung, dass solche Taktiken eine gefährliche Weiterentwicklung ausländischer Informationsmanipulation und Einmischung darstellen, da dabei die Undurchsichtigkeit und Skalierbarkeit von KI-Systemen genutzt wird, um unter dem Deckmantel einer Sprache, die verbindlich wirkt, falsche oder irreführende geopolitische Botschaften zu verbreiten; in der Erwägung, dass diese Form der algorithmischen Manipulation das Vertrauen der Öffentlichkeit in KI-Technologien zu untergraben, den demokratischen Diskurs zu verzerren und das Desinformationsrisiko in der gesamten EU und weltweit zu verschärfen droht; in der Erwägung, dass dies deutlich macht, dass KI-Kompetenz im Hinblick auf Bildung, Beschäftigung und die Gesellschaft als Ganzes gefördert werden muss;

M. in der Erwägung, dass Influencer eine wichtige Rolle bei der Stärkung der digitalen Resilienz unserer Gesellschaften spielen können, wenn es darum geht, das Bewusstsein

für Medienkompetenz und demokratische Verfahren zu schärfen oder zu einer gesunden politischen Debatte beizutragen;

N. in der Erwägung, dass bei der Präsidentschaftswahl im Herbst 2024 in Rumänien erhebliche Schwachstellen im Online-Informationsumfeld aufgedeckt wurden, wobei seriöse Berichte auf die weitverbreitete Nutzung von gefälschten Konten, Bots und algorithmisch verstärkten Inhalten zur Förderung bestimmter politischer Narrative hinweisen; in der Erwägung, dass TikTok, eine der von jungen Wählern am häufigsten genutzten Plattformen, nach eigenen Angaben die Erstellung von mehr als 116 000 Spam-Konten verhindert und 59 000 gefälschte Konten nach der Wahl entfernt hat; in der Erwägung, dass das Anwerben von Influencern, einschließlich Nano- und Mikroinfluencern, durch ausländische Akteure überdies deutlich macht, dass Akteure mit geringer Sichtbarkeit, deren Dienste kostengünstig in Anspruch genommen werden können, als Werkzeug eingesetzt werden können, um nicht aufgedeckt zu werden und die öffentliche Meinung unter Verstoß gegen demokratische Normen zu beeinflussen;

O. in der Erwägung, dass Telegram, eine Nachrichtenplattform mit immer mehr Nutzern aus der EU, verstärkt als Kanal für Desinformation, Einflussnahme aus dem Ausland und illegale Aktivitäten, einschließlich der Verbreitung extremistischer Inhalte und nicht rückverfolgbarer politischer Propaganda, angeführt wird; in der Erwägung, dass Telegram seine Ursprünge in Russland hat und das Fehlen einer sinnvollen Moderation von Inhalten anhaltende Bedenken hinsichtlich seiner Rolle bei der Untergrabung des demokratischen Diskurses hervorgerufen hat; in der Erwägung, dass Telegram zu einem der wichtigsten Kanäle für die Anwerbung von „Einweg-Agenten“ und die Durchführung hybrider Operationen geworden ist; in der Erwägung, dass festgestellt wurde, dass böswillige staatliche Akteure die technologischen Fähigkeiten, den finanziellen Bedarf und die Naivität von Telegram-Nutzern, insbesondere von jungen Menschen, ausnutzen, um Spionage- und Sabotagetätigkeiten zu minimalen Kosten durchzuführen, und dabei gleichzeitig eine glaubhafte Abstreitbarkeit aufrechterhalten; in der Erwägung, dass Telegram Berichten zufolge den Schwellenwert an Nutzern erreicht hat, um als sehr große Online-Plattform im Sinne des Gesetzes über digitale Dienste eingestuft zu werden, wodurch es strengeren regulatorischen Verpflichtungen und Anforderungen an die Risikominderung unterliegt;

P. in der Erwägung, dass der zunehmende Einfluss außereuropäischer Technologieunternehmen – insbesondere derjenigen mit Sitz in den Vereinigten Staaten und China – die strategischen Abhängigkeiten der EU in kritischen Bereichen wie Dateninfrastruktur, Cloud-Dienste und Social-Media-Plattformen deutlich gemacht hat; in der Erwägung, dass die Förderung einheimischer Innovationen, die Unterstützung europäischer Start-up-Unternehmen und Investitionen in souveräne digitale Infrastruktur wesentliche Schritte für den Aufbau eines wettbewerbsfähigen, sicheren und resilienten digitalen Ökosystems in der EU darstellen; in der Erwägung, dass die Angleichung digitaler Innovationen an demokratische Werte und Grundrechte der EU die Möglichkeit bietet, bei verantwortungsvollen und auf den Menschen ausgerichteten Technologien weltweit führend zu werden;

Q. in der Erwägung, dass im Rahmen von Untersuchungen eine besorgniserregende Entwicklung im Hinblick auf die Programme zur Umverteilung der Einnahmen von Online-Plattformen festgestellt und aufgezeigt wurde, dass Medienunternehmen, die Sanktionen unterliegen, wie Sputnik und Russia Today, auch Monate nach der

Verhängung von Sanktionen gegen Russland durch die EU noch als „Partner-Publisher“ auf Facebook geführt werden, was die Frage aufwirft, ob sie weiterhin finanziell profitieren; in der Erwägung, dass solche undurchsichtigen Monetarisierungsmechanismen es ausländischen, mit dem Staat verbundenen Akteuren ermöglichen, von der Weitergabe von Desinformation zu profitieren, und die Informationsräume der EU trotz regulatorischer Maßnahmen weiterhin destabilisieren;

R. in der Erwägung, dass in einer Umfrage, die im Vorfeld der Parlamentswahl 2025 in den Niederlanden durchgeführt wurde, jeder zehnte Befragte erklärte, dass er wahrscheinlich KI um Rat bitten wird, wen er wählen soll, während weitere 13 % erklärten, dass sie KI möglicherweise nutzen werden; in der Erwägung, dass sich in den Niederlanden mehr als ein Drittel der jüngsten Wähler für diese beiden Antwortmöglichkeiten entschieden hat; in der Erwägung, dass dieser Trend mit den Erkenntnissen, die in den Mitgliedstaaten und auf der ganzen Welt erlangt wurden, im Einklang steht; in der Erwägung, dass aus einer aktuellen Studie der niederländischen Datenschutzbehörde hervorgeht, dass die von KI-Chatbots generierten Stimmempfehlungen häufig auf einer stark verzerrten und polarisierten Sichtweise der politischen Landschaft basieren;

S. in der Erwägung, dass das Grundrecht auf Freiheit der Meinungsäußerung und Informationsfreiheit, das in Artikel 11 der Charta der Grundrechte der Europäischen Union und in Artikel 10 der Europäischen Menschenrechtskonvention verankert ist, ein Eckpfeiler der Demokratie ist; in der Erwägung, dass das Engagement der EU für das Recht auf freie Meinungsäußerung eine kohärente und grundsatzorientierte Strategie zur Bekämpfung ausländischer Informationsmanipulation und Einmischung darstellt, die in klarem Gegensatz zu den Beschränkungen steht, die autoritäre Akteure ihrer Bevölkerung systematisch auferlegen; in der Erwägung, dass die Freiheit und Pluralität der Medien und die Existenz eines dynamischen zivilgesellschaftlichen Raums Gesellschaften in die Lage versetzen, manipulative Narrative durch demokratische Überlegungen zu erkennen, aufzudecken und abzulehnen;

T. in der Erwägung, dass die Freiheit der Meinungsäußerung und die Informationsfreiheit ein Grundrecht ist, dessen Ziel es ist, Menschen zu schützen und nicht etwa Maschinen, Bots oder KI;

U. in der Erwägung, dass Akteure in Bezug auf ausländische Informationsmanipulation und Einmischung Technologien nutzen, um koordinierte unauthentische Desinformationskampagnen zu orchestrieren; in der Erwägung, dass diese Technologien, insbesondere Bots und KI-gestützte Softwareprogramme, in der Lage sind, autonom zu handeln und in der Folge einen echten öffentlichen Diskurs zu verzerren und zu zerstören, sowie die Äußerungen echter Personen mit unauthentischen Inhalten zu überfluten;

V. in der Erwägung, dass die Freiheit und Pluralität der Medien Eckpfeiler der europäischen Lebensweise sind, die in Artikel 11 Absatz 2 der Charta der Grundrechte der Europäischen Union verankert sind; in der Erwägung, dass redaktionell unabhängiger und hochwertiger Journalismus ein wirksames Gegenmittel gegen ausländische Informationsmanipulation und Einmischung sowie Desinformation ist;

W. in der Erwägung, dass im Rahmen des Gesetzes über digitale Märkte App-Entwickler, die ihre Apps über App-Stores anbieten, die Kunden kostenlos über alternative Angebote außerhalb der App-Stores informieren können sollten; in der Erwägung, dass die Kommission eine Untersuchung eines möglichen Verstoßes gegen das Gesetz über digitale Märkte durch Google eingeleitet hat, da es die Inhalte von Medienverlagen in den Suchergebnissen herabgestuft hat; in der Erwägung, dass die Kommission am 3. Juli 2025 ihre erste Überprüfung des Gesetzes über digitale Märkte eingeleitet hat;

X. in der Erwägung, dass die Mitgliedstaaten gemäß der Richtlinie über audiovisuelle Mediendienste verpflichtet sind, Maßnahmen zur Entwicklung von Medienkompetenz zu ergreifen und alle drei Jahre über ihre Bemühungen Bericht zu erstatten;

Y. in der Erwägung, dass Media Freedom Rapid Response im Jahr 2024 1 548 Verstöße gegen die Pressefreiheit dokumentiert hat, die sowohl rechtliche, physische und psychologische Drohungen als auch Formen von Zensur umfassten und gegen 2 567 Personen oder Einrichtungen mit Medienbezug aus 35 europäischen Ländern gerichtet waren, was einen alarmierenden Anstieg gegenüber den 1 153 Verstößen im Jahr 2023 darstellt;

Z. in der Erwägung, dass die Verhandlungsführer des Parlaments und des Rates am 11. Dezember 2025 eine vorläufige Einigung über die vorgeschlagene Verordnung über die Überprüfung ausländischer Investitionen in der Union erzielt haben;

AA. in der Erwägung, dass die Arbeit von Radio Free Europe/Radio Liberty (RFE/RL) für die EU von strategischem Interesse ist; in der Erwägung, dass die EU nach der Reform der Außenhilfepolitik der Vereinigten Staaten Soforthilfe in Höhe von 5,5 Mio. EUR für seine Arbeit bewilligt hat; in der Erwägung, dass eine nachhaltige Finanzierungslösung für RFE/RL gefunden werden muss;

AB. in der Erwägung, dass neue Technologien wie KI die Arbeitsbedingungen und -methoden von Journalisten verbessern können, sie aber auch neuen Bedrohungen aussetzen können, beispielsweise schnellen und billigen Kopien bestehender Medien, der massenhaften Schaffung von Desinformationskanälen und koordinierten Angriffen auf Journalisten;

AC. in der Erwägung, dass der anhaltende Angriffskrieg Russlands gegen die Ukraine verdeutlicht, wie wichtig die Rolle der Zivilgesellschaft in Krisensituationen ist, insbesondere wenn es darum geht, humanitäre Hilfe zu leisten, die Grundbedürfnisse zu decken und den Fortbestand des täglichen Lebens der betroffenen Bevölkerungsgruppen sicherzustellen;

AD. in der Erwägung, dass die Zivilgesellschaft auch eine wesentliche Rolle spielt, wenn es darum geht, zur Politikgestaltung beizutragen, soziale und kommunale Dienste zu erbringen, das Bewusstsein für wichtige soziale Fragen zu schärfen, verschiedene Gruppen in prekären Situationen zu vertreten und die Grundrechte der Bürger zu fördern und zu schützen;

AE. in der Erwägung, dass die Kommission die EU-Strategie für die Zivilgesellschaft veröffentlicht hat, die die in der gemeinsamen Mitteilung über den Europäischen Schutzschild für die Demokratie dargelegten Maßnahmen ergänzen soll; in der Erwägung, dass in der EU-Strategie für die Zivilgesellschaft bestätigt wird, dass die

Plattform der Zivilgesellschaft, die die Kommission angekündigt hat und die im Rahmen der Umsetzung der Strategie eingerichtet werden soll, einen beständigen und strukturierten Rahmen für den Schutz und die Förderung der Werte der EU sowie die Optimierung und Stärkung des Engagements für Grundrechte, Demokratie, Gleichheit und Rechtsstaatlichkeit bieten und 2026 einsatzbereit sein wird; in der Erwägung, dass die Strategie auch die Einrichtung einer Online-Wissensplattform zum Thema zivilgesellschaftlicher Raum beinhaltet, die bestehende Initiativen, Berichte und Schutzressourcen zur Überwachung des zivilgesellschaftlichen Raums auf nationaler, europäischer und internationaler Ebene in Zusammenarbeit mit der Agentur der Europäischen Union für Grundrechte dokumentieren sollte;

AF. in der Erwägung, dass das von der Kommission für den Mehrjährigen Finanzrahmen (MFR) 2028-2034 vorgeschlagene Programm AgoraEU mit einem veranschlagten Budget von 9 Mrd. EUR einen wichtigen Schritt in Richtung Verstärkung der Unterstützung der EU für Kultur, Medien und die Zivilgesellschaft darstellt;

AG. in der Erwägung, dass Hybridangriffe auf kritische Infrastrukturen in der EU immer häufiger vorkommen, wobei Vorfälle mit denselben böswilligen Akteuren wie Russland und China, aber auch mit Iran und Nordkorea in Verbindung stehen; in der Erwägung, dass diese Angriffe häufig gegen essenzielle Systeme, Netzwerke und Einrichtungen gerichtet sind, die für das Funktionieren einer Gesellschaft von entscheidender Bedeutung sind, einschließlich öffentlicher Sicherheit und wirtschaftlicher Stabilität; in der Erwägung, dass solche Angriffe verschiedene Formen annehmen können, wie physische Sabotage, Brandanschläge, Spionage und Störsignale sowie Cyberangriffe und andere Aktivitäten in der Grauzone, die allesamt koordinierte Anstrengungen zeigen, um die Sicherheit und die gesellschaftliche Resilienz der EU zu testen, zu stören und zu untergraben;

AH. in der Erwägung, dass in der Ostsee die Zahl der Störungen im Zusammenhang mit Seekabeln, die für die Internetanbindung und die Stromversorgung in der gesamten baltischen und nordischen Region von entscheidender Bedeutung sind, beispiellos gestiegen ist; in der Erwägung, dass seit 2023 mindestens 11 Kabelschäden verzeichnet wurden, was auf koordinierte Sabotage hindeutet;

AI. in der Erwägung, dass in den letzten Monaten über mehreren EU-Mitgliedstaaten und benachbarten NATO-Verbündeten, darunter Polen, die baltischen Staaten, Rumänien, Dänemark, Schweden, Deutschland, Belgien und Norwegen, mehrere Verletzungen des Luftraums und ein unbefugtes Eindringen von Drohnen gemeldet wurden; in der Erwägung, dass eine Reihe dieser Vorfälle eindeutig russischen Militärflugzeugen und Drohnen zugeschrieben werden kann, während andere Vorfälle, bei denen es um nicht identifizierte Luftfahrzeuge geht, nach wie vor untersucht werden, jedoch weithin der Verdacht besteht, dass sie Teil desselben Musters hybrider Einschüchterung und Destabilisierung sind, das sich gegen Europa richtet;

AJ. in der Erwägung, dass mehrere europäische Länder, darunter Frankreich, Estland, Deutschland, Tschechien und Norwegen, in jüngster Zeit mit großen Cyberangriffen auf Regierungssysteme, kritische Infrastrukturen und private Unternehmen konfrontiert waren, die dem russischen Militärgeheimdienst und mit dem chinesischen Staat verbundenen Akteuren zugeschrieben werden können, was die dringende

Notwendigkeit unterstreicht, die kollektive Cyberabwehrfähigkeit und die Fähigkeiten der EU zur Zuordnung von Cyberangriffen zu stärken;

AK. in der Erwägung, dass die Abhängigkeit der EU von ausländischen Akteuren und im Ausland hergestellten Technologien in kritischen Infrastrukturen und Lieferketten nach wie vor Anlass zu großer Sorge gibt und eine der größten Schwachstellen der EU darstellt; in der Erwägung, dass dies in den Bereichen Technologie und Digitales besonders verbreitet ist und eine zentrale Herausforderung für die Cybersicherheit darstellt;

AL. in der Erwägung, dass strafrechtliche Instrumente zum Europäischen Schutzschild für die Demokratie beitragen können, soweit die betreffenden Tätigkeiten Straftaten darstellen;

AM. in der Erwägung, dass die Mechanismen der justiziellen und polizeilichen Zusammenarbeit und die Instrumente für den grenzüberschreitenden Informationsaustausch angesichts der zunehmenden Herausforderungen, die sich aus der Einflussnahme aus dem Ausland für die innere Sicherheit der EU ergeben, angepasst und gestärkt werden müssen;

AN. in der Erwägung, dass die Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung (Europol) in ihrem jüngsten Bericht über die Bewertung der Bedrohungslage im Bereich der schweren und organisierten Kriminalität in der EU, der im März 2025 veröffentlicht wurde, vor der Beteiligung krimineller Organisationen an hybriden Kampagnen gewarnt hat; in der Erwägung, dass in der Mitteilung der Kommission über ProtectEU anerkannt wird, dass verschiedene Faktoren Europol daran hindern, sein operatives Potenzial zur Unterstützung von Tätigkeiten zur Bekämpfung der grenzüberschreitenden Kriminalität voll auszuschöpfen, einschließlich Lücken im Mandat der Agentur in Bezug auf neue Sicherheitsbedrohungen, insbesondere Sabotage, hybride Bedrohungen und Informationsmanipulation;

AO. in der Erwägung, dass sich die Kommission verpflichtet hat, eine Reform einzuleiten, durch die Europol zu einer wirklich operativen Polizeiagentur wird; in der Erwägung, dass Polizeibeamte wichtige Partner für den Schutz demokratischer Institutionen sind; in der Erwägung, dass dies in den einschlägigen Politikbereichen deutlicher anerkannt werden sollte;

AP. in der Erwägung, dass die Agentur der Europäischen Union für justizielle Zusammenarbeit in Strafsachen (Eurojust) von den Mitgliedstaaten ersucht werden kann, die nationalen Behörden bei der Bekämpfung jeder Art von rechtswidrigem Verhalten in ihrem Zuständigkeitsbereich zu unterstützen; in der Erwägung, dass sich die justizielle Zusammenarbeit bei der Ausweitung auf neue Kriminalitätsbereiche als besonders schwierig erweisen kann, was ein modernisiertes rechtliches Instrumentarium erfordert;

AQ. in der Erwägung, dass Agenturen der Europäischen Union, die in den Bereichen Grenzen, Migration und Asylmanagement tätig sind, d. h. die Europäische Agentur für die Grenz- und Küstenwache (Frontex) und die Asylagentur der Europäischen Union (EUAA), in Zusammenarbeit mit nationalen Behörden eine weitere Schlüsselrolle bei der Schaffung und Aufrechterhaltung eines gemeinsamen Situationsbewusstseins für Risiken im Zusammenhang mit der Nutzung der Migrationsströme für politische

Zwecke und bei der Unterstützung der Mitgliedstaaten an den Außengrenzen in Krisensituationen spielen; in der Erwägung, dass die Kommission die Stärkung von Frontex in ihre Leitinitiativen für die Wahlperiode 2024-2029 aufgenommen hat;

AR. in der Erwägung, dass die Bewerberländer und die Nachbarländer der EU, insbesondere die Ukraine, Moldau und der Westbalkan, nach wie vor stark von ausländischer Informationsmanipulation und Einmischung sowie hybriden Bedrohungen betroffen sind und die Unterstützung der EU benötigen, um die Resilienz der Zivilgesellschaft und der Institutionen aufzubauen;

AS. in der Erwägung, dass der Angriffskrieg Russlands gegen die Ukraine und Chinas selbstbewusste geopolitische Haltung den Einsatz von Desinformation, wirtschaftlichem Zwang und strategischem Einfluss verstärkt haben und sich nicht nur gegen die EU, sondern auch gegen gefährdete Regionen wie den Westbalkan, die Länder der Östlichen Partnerschaft und den Globalen Süden richten; in der Erwägung, dass aus verschiedenen Quellen hervorgeht, dass sich das Budget Russlands für die Verbreitung von Desinformation und Propaganda auf 1 Mrd. bis 2 Mrd. USD pro Jahr beläuft; in der Erwägung, dass sich bei Wahlen und politischen Ereignissen in ganz Europa die anhaltende, gezielte, ausgefeilte, groß angelegte, offensive sowie hybride Kriegsführung Russlands zeigt, die darauf abzielt, das Vertrauen in unsere politischen Systeme und Institutionen zu destabilisieren und eine ständige Verwechslung von Fakten und falschen Informationen zu schaffen; in der Erwägung, dass eine solche Kriegsführung eine angemessene Reaktion und einen Übergang von einer rein defensiven zu einer offensiven Strategie erfordert;

AT. in der Erwägung, dass die EUPM Moldova am 24. April 2023 mit dem ausdrücklichen Ziel eingerichtet wurde, die moldauischen Behörden bei der Bekämpfung ausländischer Informationsmanipulation und Einflussnahme zu unterstützen;

AU. in der Erwägung, dass die Abnahme der Unterstützung der USA für die internationale Demokratie zu einer erheblichen globalen Finanzierungslücke bei der Bekämpfung von Desinformation und autoritärem Einfluss geführt hat;

AV. in der Erwägung, dass mit internationalen Initiativen, einschließlich der Initiativen der Vereinten Nationen, der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung und der G7, Grundsätze und Rahmenbedingungen für den Schutz der Integrität von Informationen allmählich festgelegt werden, die in demokratischen Werten, Medienpluralismus und Menschenrechten verankert sind;

AW. in der Erwägung, dass ausländische Informationsmanipulation und Einmischung eine zunehmende Herausforderung für die demokratische Resilienz der EU darstellt; in der Erwägung, dass bestimmte Formen manipulativer Informationstätigkeiten auch von Akteuren ausgehen können, die in der EU tätig sind; in der Erwägung, dass das Phänomen der Informationsmanipulation und Einmischung im innerstaatlichen Kontext weiter untersucht und verstanden werden sollte, insbesondere im Zusammenhang mit ausländischer Informationsmanipulation und Einmischung; in der Erwägung, dass die vorgestellten Maßnahmen zur Bekämpfung ausländischer Informationsmanipulation und Einmischung auch dazu beitragen, die allgemeine Resilienz der Gesellschaften im nationalen Kontext zu verbessern, insbesondere im Hinblick auf die Steigerung des

Situationsbewusstseins, die Verstärkung der Transparenz und Pluralität sowie die Stärkung der Medienkompetenz und der digitalen Kompetenz in allen Altersgruppen;

AX. in der Erwägung, dass die im Dezember 2023 veröffentlichten Empfehlungen der Kommission zu inklusiven und stabilen Wahlprozessen in der Union noch in allen Mitgliedstaaten vollständig umgesetzt werden müssen, einschließlich der Bestimmungen, die darauf abzielen, die Zusammenarbeit zwischen den nationalen Behörden während und im Vorfeld von Wahlprozessen durch die Einrichtung nationaler Wahlnetze zu stärken;

AY. in der Erwägung, dass das ECNE in den letzten Jahren eine immer wichtigere Rolle gespielt hat, es derzeit jedoch nicht über die erforderlichen Ressourcen und Kapazitäten verfügt, um seine Tätigkeiten aufzuwerten;

AZ. in der Erwägung, dass die Bewerberländer eingeladen wurden, an den Sitzungen des ECNE teilzunehmen; in der Erwägung, dass zusätzlich zu dieser Beteiligung noch erhebliches Potenzial besteht, die Zusammenarbeit mit diesen Ländern im Rahmen der Tätigkeiten des Netzes weiter zu verbessern, voneinander zu lernen, wenn sie Bedrohungen ausgesetzt sind, und sich über bewährte Verfahren zur Bekämpfung dieser Bedrohungen auszutauschen;

BA. in der Erwägung, dass es eindeutig notwendig ist, den Schutz der Wahlinfrastruktur und der nationalen politischen Parteien, die ebenfalls Ziel von Cyberangriffen waren, zu stärken, nicht zuletzt angesichts der groß angelegten Cyberangriffe auf die rumänischen Wahlbehörden im Herbst 2024;

BB. in der Erwägung, dass die verdeckte Finanzierung politischer Parteien und Bewegungen in der EU durch Drittländer eine Bedrohung für die Legitimität des demokratischen Prozesses darstellt;

BC. in der Erwägung, dass die Unabhängigkeit der Justiz ein unverzichtbares strukturelles Element der Integrität von Wahlen ist; in der Erwägung, dass die Integrität von Wahlen davon abhängt, dass es zugängliche und wirksame Rechtsbehelfe gegen Verstöße gegen das Wahlrecht und gegen Wahlverfahren gibt, die vor politischer Einflussnahme bzw. Einflussnahme durch die Exekutive geschützt sind;

BD. in der Erwägung, dass die EU zwischen 2022 und 2025 insgesamt 19 Pakete mit umfassenden und beispiellosen Sanktionen als Reaktion auf den Angriffskrieg Russlands gegen die Ukraine verhängt hat, wodurch der Druck auf die Kriegswirtschaft Russlands erheblich zugenommen hat und Schlüsselsektoren, insbesondere der Energie-, Finanz- und Verteidigungssektor, Sonderwirtschaftszonen sowie Unterstützer und Nutznießer seines Angriffskriegs ins Visier genommen wurden und die Abhängigkeit der EU von Einfuhren fossiler Brennstoffe aus Russland beendet wurde; in der Erwägung, dass die EU außerdem Sanktionen gegen Belarus, Iran und Nordkorea verhängt hat, weil sie den Angriffskrieg Russlands gegen die Ukraine unterstützen;

BE. in der Erwägung, dass seit dem 8. Oktober 2024 der Sanktionsrahmen der EU die Bekämpfung einer Vielzahl hybrider Aktivitäten Russlands ermöglicht, darunter die Beeinträchtigung von Wahlprozessen und der Funktionsweise demokratischer Institutionen, Bedrohungen und Sabotageakte gegen wirtschaftliche Aktivitäten, Dienste von öffentlichem Interesse und kritische Infrastruktur, der Einsatz koordinierter

Desinformation, ausländische Informationsmanipulation und Einmischung, böswillige Cyberaktivitäten, die Instrumentalisierung von Migration und andere destabilisierende Aktivitäten; in der Erwägung, dass dieser Rahmen bereits dazu geführt hat, dass Dutzende von Personen und Organisationen, darunter russische Oligarchen, Propagandisten, Mitarbeiter militärischer Nachrichtendienste, Medien und Unternehmen, wegen der Verbreitung kremlfreundlicher Narrative, der Durchführung von Sabotageakten und der Aushöhlung demokratischer Prozesse mit Sanktionen belegt wurden; in der Erwägung, dass die EU im Rahmen der entsprechenden Maßnahmen nun Vermögenswerte einfrieren, Reiseverbote verhängen, Rundfunklizenzen aussetzen und Finanz- und Kryptowerttransaktionen im Zusammenhang mit hybriden Aktivitäten untersagen kann;

BF. in der Erwägung, dass die Staatsorgane Russlands am 28. Dezember 2024 bekannt gegeben hat, dass sie ihre schwarze Liste von EU-Bürgerinnen und Bürgern sowie Amtsträgern, darunter auch Vertreter von Organen, Einrichtungen und sonstigen Stellen der EU, nationalen Regierungen, Strafverfolgungsbehörden und Handelsorganisationen, erheblich erweitert habe; in der Erwägung, dass diese schwarzen Liste, die sich gegen diejenigen richtet, die demokratische Werte fördern und sich gegen den Angriffskrieg Russlands in der Ukraine aussprechen, darauf abzielt, durch undurchsichtige und willkürliche Beschränkungen, häufig ohne formelle Benachrichtigung, Begründung oder Recht auf Berufung, einzuschüchtern und Stimmen zum Schweigen zu bringen;

BG. in der Erwägung, dass sich hybride Bedrohungen, Einmischung aus dem Ausland und Desinformationskampagnen zu komplexen, umfassenden und sektorübergreifenden Krisen entwickelt haben, die sich nachteilig auf die Sicherheit, das Wohlergehen der Bürgerinnen und Bürger und das Funktionieren der Gesellschaft und der Wirtschaft insgesamt auswirken, eine zentrale Herausforderung für die inneren Angelegenheiten der EU darstellen und die demokratischen Institutionen in allen Mitgliedstaaten destabilisieren, wie der Angriffskrieg Russlands gegen die Ukraine gezeigt hat;

BH. in der Erwägung, dass zivile und militärische Vorsorge eines umfassenden gesamtgesellschaftlichen, gesamtstaatlichen und gefahrenübergreifenden Ansatzes bedarf, bei dem die nationalen Behörden der Mitgliedstaaten zusammen mit den Organen, Einrichtungen und sonstigen Stellen der EU sowie Unternehmen, Hochschulen, der Zivilgesellschaft und einzelnen Bürgerinnen und Bürgern einbezogen werden; in der Erwägung, dass diese Bemühungen mit langfristigen Investitionen, strategischer Vorausschau und der Verankerung von Resilienz in der Politikgestaltung, der Infrastrukturentwicklung, den Bildungssystemen und den Lieferketten einhergehen müssen;

BI. in der Erwägung, dass die Stärkung der Bürgerteilhabe für die Resilienz der Gesellschaft von entscheidender Bedeutung ist und dass die Vorsorge praktische Instrumente wie eine unionsweite Krisenwarn-App, eine Informationsbroschüre zur Notfallvorsorge von Haushalten und weitreichende Sensibilisierungskampagnen zur Förderung der Selbstversorgung und Krisenvorsorge umfassen muss;

BJ. in der Erwägung, dass die zivil-militärische Zusammenarbeit, Fähigkeiten mit doppeltem Verwendungszweck und die Einbeziehung der Vorsorge in Bildungsprogramme von wesentlicher Bedeutung sind, um die Verteidigungsbereitschaft durch gezielte Schulungen nicht nur für Beschäftigte in

kritischen Sektoren wie Feuerwehrleute, Gesundheitsfachkräfte und öffentliche Bedienstete, sondern auch für Akteure der Zivilgesellschaft und die breite Öffentlichkeit zu verbessern;

BK. in der Erwägung, dass technologische Souveränität und sichere digitale Ökosysteme, einschließlich Projekten wie IRIS² und dem europäischen System für kritische Kommunikation, von entscheidender Bedeutung sind, um die Kontrolle über wesentliche Kommunikationskanäle zu behalten und kritische Infrastruktur zu stärken;

BL. in der Erwägung, dass die Vorsorge von einer reibungslosen Zusammenarbeit zwischen den Organen, Einrichtungen und sonstigen Stellen der EU, den Mitgliedstaaten und internationalen Partnern abhängt, die durch gemeinsame Übungen und Schulungen, gemeinsame Plattformen zur Lageerfassung und einen raschen Informationsaustausch unterstützt wird;

BM. in der Erwägung, dass der Aufbau einer belastbaren Resilienz und die Erreichung eines ausreichenden Maßes an ziviler und militärischer Vorsorge massive Investitionen erfordern, um die technologische und industrielle Basis Europas zu stärken und strategische Abhängigkeiten zu verringern; in der Erwägung, dass für diese Bemühungen neue gezielte Finanzierungsmechanismen erkundet werden müssen;

Einleitung

1. begrüßt die gemeinsame Mitteilung der Kommission und der Hohen Vertreterin der Union für Außen- und Sicherheitspolitik zur Einrichtung des Europäischen Schutzschilds für die Demokratie und die anhaltenden Bemühungen, auf der bereits im Rahmen des Europäischen Aktionsplans für Demokratie und des Pakets zur Verteidigung der Demokratie geleisteten Arbeit aufzubauen; ist der Ansicht, dass die Kernaufgabe des Europäischen Schutzschilds für die Demokratie darin bestehen sollte, die europäische Demokratie vor externen Bedrohungen zu schützen und letztlich zum Schutz der europäischen Lebensweise, der Rechtsstaatlichkeit und der in Artikel 2 EUV verankerten Werte beizutragen;

2. nimmt mit Besorgnis die zunehmend komplexe und sich wandelnde Bedrohungslage zur Kenntnis, mit der die EU und ihre Mitgliedstaaten konfrontiert sind und die durch ausländische Informationsmanipulation und Einmischung, hybride Angriffe und Desinformationskampagnen böswilliger Akteure aus Drittländern gekennzeichnet ist; betont, dass es sich hierbei um feindselige Handlungen handelt, mit denen die demokratischen Grundlagen der EU ausgehöhlt werden, indem Spaltung geschürt, das Vertrauen der Öffentlichkeit in die Organe geschmälert und gesellschaftliche Schwachstellen ausgenutzt werden, wobei häufig fortschrittliche digitale Technologien zum Einsatz kommen;

3. betrachtet Russland als die größte externe Bedrohung für die demokratische Integrität Europas; bekräftigt seine Auffassung, dass Russland ein dem Terrorismus Vorschub leistender Staat ist; betont, dass dringend eine umfassende, kohärente und zukunftsorientierte Strategie erforderlich ist, um diese Herausforderungen wirksam anzugehen und die europäische Demokratie zu schützen;

4. bekräftigt mit Überzeugung, dass die in der Initiative „Europäischer Schutzschild für die Demokratie“ dargelegten politischen Prioritäten – darunter die Bekämpfung von

ausländischer Informationsmanipulation und Einmischung und hybriden Bedrohungen, die Stärkung der Resilienz bei Wahlen, die Verbesserung der Cybersicherheit, die Unterstützung der Zivilgesellschaft und die Förderung eines unabhängigen und investigativen Journalismus – fest im kommenden MFR verankert und mit ausreichenden Mitteln ausgestattet werden müssen;

Europäisches Zentrum für demokratische Resilienz

5. begrüßt den Vorschlag der Kommission für ein Europäisches Zentrum für demokratische Resilienz (im Folgenden „Zentrum“) als notwendigen und logischen Schritt hin zu einer verstärkten Koordinierung der Bemühungen, sich entwickelnden gemeinsamen Bedrohungen standzuhalten, insbesondere ausländischer Informationsmanipulation und Einmischung sowie Desinformation; nimmt seinen Ansatz einer schrittweisen Einführung von Funktionen und Operationen, einschließlich einer schrittweisen Zunahme der Beteiligung der Mitgliedstaaten, zur Kenntnis; begrüßt die Zusicherung der Kommission, dass sie bereits an der Einrichtung des Zentrums unter der Leitung des für Demokratie, Justiz, Rechtsstaatlichkeit und Verbraucherschutz zuständigen Mitglieds der Kommission arbeitet und ausdrücklich das Ziel verfolgt, dass es im Laufe des Jahres 2026 seine Arbeit aufnehmen kann; begrüßt die Zusage der Kommission, das Parlament regelmäßig über die Umsetzung des Europäischen Schutzschildes für die Demokratie und des Zentrums zu unterrichten und in diesen Prozess einzubeziehen;

6. weist jedoch darauf hin, dass es dem Vorschlag an ausreichenden operativen Details, klaren Mittelzuweisungen, einer spezifischen Verwaltungsstruktur, einem konkreten Mandat und einem Zeitplan mangelt; stellt fest, dass das Zentrum in der gemeinsamen Mitteilung über den Europäischen Schutzschild für die Demokratie nicht ausdrücklich mit einer der darin dargelegten Maßnahmen verknüpft wird, die in unterschiedlichen Verwaltungsrahmen innerhalb der Kommission und des EAD verbleiben; bringt seine Besorgnis darüber zum Ausdruck, dass die Fähigkeit der EU, das gesamte Spektrum der derzeit verfügbaren Instrumente effizient zu nutzen, weiter eingeschränkt und die in der gemeinsamen Mitteilung festgestellten Mängel, einschließlich geringerer Reaktionsfähigkeit, Fragmentierung und knapper Haushaltsmittel, verstärkt werden könnten, wenn das Zentrum nur eine weitere zentrale Stelle, ein weiteres Netzwerk, eine weitere Plattform oder ein weiterer Rahmen unter vielen bleibt;

7. begrüßt, dass die gemeinsame Mitteilung eine umfassende Bestandsaufnahme der bestehenden Rahmen, Strukturen, Instrumente, Initiativen und Programme zur Bekämpfung von ausländischer Informationsmanipulation und Einmischung und von Desinformation sowie zur Stärkung der Resilienz enthält und darin die Maßnahmen aufgelistet sind, zu deren Umsetzung sich die Kommission und der EAD verpflichtet haben; fordert die Kommission und den EAD auf, einen klaren Zeitplan für ihre schrittweise Einführung und Integration in das Zentrum vorzuschlagen, wobei diese Integration im Jahr 2026 abgeschlossen sein soll; fordert, dass diese Integration einschlägige Aufsichts- und Durchsetzungsmechanismen für das Gesetz über digitale Dienste umfasst, insbesondere im Hinblick auf die Ermittlung und Minimierung systemischer Risiken, die Koordinierung der Bemühungen zur Bekämpfung von Informationsmanipulationskampagnen, die Sicherstellung der operativen Verantwortung für ein verbessertes Schnellwarnsystem (RAS) und die Pflege und den Betrieb einer einheitlichen Informationsdatenbank zur ausländischen Informationsmanipulation und

Einmischung sowie die Entwicklung der Ressource EUvsDisinfo, des ECNE und der Taskforce der Kommission für Desinformation und strategische Kommunikation;

8. begrüßt, dass die Kommission die Notwendigkeit anerkannt hat, mit den Mitgliedstaaten und dem Parlament über das Mandat, die Struktur und die Arbeitsmethoden des Zentrums zu beraten, und fordert die Kommission auf, den Prozess einzuleiten, indem sie bis zum ersten Quartal 2027 eine Rechtsgrundlage für die Einrichtung des Zentrums als EU-Einrichtung mit einer klaren institutionellen Satzung und einer klaren Positionierung, einer klaren Verwaltungsstruktur und klaren parlamentarischen Kontrollmechanismen vorschlägt; betont, dass institutionelle Klarheit unerlässlich ist, damit das Zentrum entschlossen handeln und gleichzeitig rechenschaftspflichtig bleiben kann;

9. fordert die Kommission auf, das Zentrum mit einem klaren Mandat und Entscheidungsmechanismen auszustatten, damit es als unabhängiges Exzellenzzentrum für die Aufdeckung und Analyse von ausländischer Informationsmanipulation und Einmischung und von Desinformationsoperationen, als Plattform für den Kapazitätsaufbau zur Festlegung gemeinsamer Definitionen, Standards, Schulungen und technischer Instrumente in der gesamten EU und als operatives Rückgrat für die Echtzeitkoordinierung der technischen Unterstützung bei der Bekämpfung aktiver Informationsmanipulationskampagnen fungieren kann;

10. fordert die Kommission auf, sich dafür einzusetzen, dass das Zentrum mit der Aufgabe betraut wird, die Integrität demokratischer Prozesse auf EU-Ebene zu wahren; bekräftigt, dass die operativen Strukturen der Mitgliedstaaten eine erste Verteidigungslinie darstellen; betont jedoch, dass ihre vorrangige Verantwortung nicht die legitimen Interessen der EU im Hinblick auf die Bekämpfung von ausländischer Informationsmanipulation und Einmischung sowie von Desinformation erschöpft; fordert, dass die Kommission klarstellt, dass das Zentrum zwei sich gegenseitig verstärkende Ziele verfolgen muss, nämlich die Koordinierung der Aktivitäten der Mitgliedstaaten in diesem Bereich und die Verbesserung ihrer operativen Fähigkeiten sowie den Schutz der demokratischen Interessen der EU;

11. fordert die Mitgliedstaaten auf, die über keine speziellen operativen Strukturen verfügen, mit Unterstützung des Zentrums spezielle nationale Einrichtungen zur Aufdeckung und Bekämpfung von ausländischer Informationsmanipulation und Einmischung einzurichten oder erheblich zu stärken; fordert die Kommission auf, einen Fahrplan für den Aufbau von Fähigkeiten in den Mitgliedstaaten zu erstellen;

12. fordert die Kommission auf, die Durchführbarkeit einer Befugnisübertragung an das Zentrum zur Verwaltung und Vergabe von zweckgebundenen EU-Finanzhilfen im Rahmen einschlägiger EU-Programme, darunter das Programm „Digitales Europa“, die Fazilität „Connecting Europe“, Horizont Europa, das Programm „Bürgerinnen und Bürger, Gleichstellung, Rechte und Werte“ (CERV) und das vorgeschlagene Programm „AgoraEU“, zu prüfen und das Zentrum zu ermächtigen, Aufforderungen zur Einreichung von Vorschlägen zu veröffentlichen und Projekte in Bereichen seines Mandats auszuwählen, zu überwachen und zu bewerten, insbesondere im Bereich der EDMO, der Initiativen zur Medienkompetenz und anderer einschlägiger europäischer, regionaler und grenzüberschreitender Initiativen, die der Bekämpfung von ausländischer

Informationsmanipulation und Einmischung, der Stärkung der demokratischen Resilienz und der Förderung der Informationsintegrität gewidmet sind;

13. fordert die Kommission auf, eine eigene EU-Haushaltslinie für die Tätigkeiten des Zentrums mit einer klaren Trennung zwischen operativer Finanzierung und allgemeinen Koordinierungskosten bereitzustellen; fordert die Kommission auf, ausreichende personelle Ressourcen sicherzustellen und die Finanzierung aus den bestehenden Haushalten zu überbrücken, um die vorbereitenden Arbeiten vor dem MFR 2028-2034 zu ermöglichen;

14. fordert die Kommission auf, die Durchführbarkeit der Einrichtung eines Finanzierungsmechanismus zur Ergänzung der speziellen Haushaltslinie für die Tätigkeiten des Zentrums auf der Grundlage von Beiträgen sehr großer Online-Plattformen zu prüfen; weist darauf hin, dass der Bankensektor Mechanismen für die Abwicklung von Banken finanziert, Pharmaunternehmen die Sicherheitsüberwachung unterstützen und umweltschädliche Industriezweige Umweltkosten tragen; fordert einen Mechanismus, durch den Social-Media-Plattformen proportional zu der Infrastruktur beitragen, die erforderlich ist, um negativen externen Einflüssen und systemischen Risiken im Zusammenhang mit ihren Diensten entgegenzuwirken, sowohl in Bezug auf ausländische Informationsmanipulation und Einmischung und auf Desinformation als auch auf den Aufbau von Resilienz; betont, dass solche Beiträge nicht nur im Einklang mit den etablierten europäischen Grundsätzen der Verantwortung und Rechenschaftspflicht stehen, sondern auch sicherstellen würden, dass die Kosten für den Schutz des demokratischen Diskurses von denjenigen getragen werden, die am meisten vom digitalen Informationsökosystem profitieren;

Digitale Resilienz

15. fordert die vollständige Umsetzung wichtiger Rechtsvorschriften im digitalen Raum in allen Mitgliedstaaten, darunter das Gesetz über digitale Dienste, die Verordnung über die Transparenz und das Targeting politischer Werbung und die Verordnung über künstliche Intelligenz; vertritt den Standpunkt, dass bei der weiteren Umsetzung der Rechtsvorschriften im digitalen Bereich ein stärkerer Schwerpunkt auf die Bekämpfung von Desinformation im Internet, die Gewährleistung der Informationsintegrität und den Schutz des demokratischen Diskurses während des Wahlkampfs gelegt werden sollte; zeigt sich in diesem Zusammenhang besorgt darüber, dass verzögerte Leitlinien und technische Standards ein Hindernis für die rechtzeitige Umsetzung der Verordnung über künstliche Intelligenz darstellen; begrüßt, dass die Kommission in ihrem Vorschlag für das Omnibus-Paket für den Digitalbereich zur Vereinfachung der KI-Rechtsvorschriften versucht, dieses Problem anzugehen, indem sie den Zeitplan für die Umsetzung der Vorschriften für Hochrisiko-KI-Systeme an die Verfügbarkeit von Normen oder anderen Unterstützungsinstrumenten knüpft;

16. begrüßt die offizielle Aufnahme des freiwilligen Verhaltenskodex zur Bekämpfung von Desinformation in den Rahmen des Gesetzes über digitale Dienste; ist der Ansicht, dass die unehrliche Nutzung sozialer Medien, z. B. durch Bots, Scheinkonten, polarisierende Algorithmen sowie künstliche Steuerung und Verstärkung, zu den größten Risiken für einen freien und offenen Diskurs im Internet gehört, insbesondere während des Wahlkampfs; fordert alle in der EU tätigen sehr großen Online-Plattformen und sehr

großen Online-Suchmaschinen nachdrücklich auf, den Kodex uneingeschränkt einzuhalten, und fordert die Plattform X nachdrücklich auf, ihm wieder beizutreten;

17. begrüßt die Zusage der Kommission, ein Protokoll über Vorfälle und Krisen im Zusammenhang mit dem Gesetz über digitale Dienste auszuarbeiten, um weiter gegen größere Vorfälle und Störungen im Informationsumfeld vorzugehen; ist der Ansicht, dass mit diesem Protokoll unter anderem gegen die Einflussnahme auf Wahlen durch koordiniertes unehrliches Verhalten im Online-Raum vorgegangen werden sollte, insbesondere durch botbasierte Verstärkung und Steuerung, die einen echten öffentlichen Diskurs wirksam verzerren;

18. nimmt zur Kenntnis, dass die Kommission ihre Untersuchung bezüglich der Verletzung der Transparenzpflichten gemäß dem Gesetz über digitale Dienste durch die Plattform X abgeschlossen und anschließend eine Geldbuße in Höhe von 120 Mio. EUR verhängt hat; fordert die Kommission nachdrücklich auf, die verbleibenden Untersuchungen in Bezug auf mutmaßliche Verstöße gegen die EU-Rechtsvorschriften im digitalen Bereich zu beschleunigen, einschließlich solcher, bei denen es um Einflussnahme auf Wahlen, algorithmische Undurchsichtigkeit oder die Verbreitung gefälschter Konten und Bots geht; fordert die Kommission insbesondere auf, die Untersuchungen zur Einhaltung des Gesetzes über digitale Dienste durch TikTok im Zusammenhang mit der rumänischen Präsidentschaftswahl 2024 rasch abzuschließen, einschließlich seiner Verpflichtung, systemische Risiken für demokratische Prozesse zu mindern;

19. fordert die Kommission und die zuständigen Regulierungsbehörden auf, verdeckte Desinformationskampagnen, die darauf abzielen, generative KI-Systeme auszunutzen, beispielsweise die Aktivitäten des in Moskau ansässigen Netzwerks „Prawda“, zu untersuchen und öffentlich aufzudecken; fordert Anbieter von KI-Systemen nachdrücklich auf, dieses Phänomen durch ihre KI-Risikomanagementsysteme angemessen anzugehen und zu mindern; fordert darüber hinaus, dass die Festlegung von Sicherheitsstandards für Anbieter großer Sprachmodelle (LLM) auf internationaler Ebene koordiniert wird, um eine verbesserte Transparenz hinsichtlich der Datenquellen für das Training zu gewährleisten;

20. fordert die Kommission auf, ihre Bewertung der Nutzerbasis und Funktionalität von Telegram dringend abzuschließen, um seine Einstufung als sehr große Online-Plattform im Rahmen des Gesetzes über digitale Dienste zu bestimmen; fordert die Kommission und die zuständigen Behörden nachdrücklich auf, die potenzielle Rolle von Telegram bei der Erleichterung krimineller Aktivitäten, der Einflussnahme bei Wahlen und der Verbreitung von Desinformation in der EU zu untersuchen; fordert die Plattform zudem nachdrücklich auf, sich dem freiwilligen Verhaltenskodex gegen Desinformation anzuschließen und die EU-Vorschriften in Bezug auf Transparenz, die Moderation von Inhalten und Datenzugang vollständig einzuhalten, um gleiche Wettbewerbsbedingungen zu gewährleisten und das Vertrauen der Bürgerinnen und Bürger in den digitalen Informationsraum zu wahren;

21. empfiehlt, die Rolle von Influencern, einschließlich Nano- und Mikro-Influencern, bei der Gestaltung der öffentlichen Debatte und der Einflussnahme auf Wahlen weiter zu untersuchen, sowohl diejenigen, die sich bewusst oder unbewusst gegen ausländische Desinformationskampagnen stellen, als auch diejenigen, die sich daran beteiligen;

betont in diesem Zusammenhang, dass strenge Standards für Transparenz und Informationsintegrität für Ersteller politischer Online-Inhalte erforderlich sind, insbesondere für Influencer, die in einer Grauzone zwischen kommerzieller Werbung und politischer Meinungsäußerung agieren; begrüßt die bestehenden Verhaltenskodizes, Schulungen und andere Initiativen, die entwickelt wurden, um die sozialen Medien und Influencer verantwortungsvoller und transparenter zu machen;

22. ist der Ansicht, dass eine digitale Infrastruktur der EU, einschließlich sicherer lokaler Rechenzentren und souveräner Cloud- und Edge-Computing-Kapazitäten der EU, eine strategische Säule der digitalen Resilienz ist, mit der sichergestellt wird, dass sensible Daten der europäischen Bevölkerung nicht in ausländischen Rechenzentren gespeichert werden; fordert die Kommission auf, im geplanten EU-Rechtsakt über Cloud- und KI-Entwicklung eine Definition der souveränen Cloud und ihres Anwendungsbereichs vorzuschlagen; fordert die Kommission auf, sich mit den erfolglosen Diskussionen über das EU-System für die Cybersicherheitszertifizierung für Cloud-Dienste auseinanderzusetzen und im Rahmen der Überarbeitung des Rechtsakts zur Cybersicherheit eine konkrete Lösung vorzuschlagen, die den Bedenken hinsichtlich der Cybersicherheit und Souveränität im Zusammenhang mit einer Machtkonzentration Rechnung trägt; fordert nachdrücklich die Entwicklung von Reallaboren und Finanzierungsmechanismen zur Unterstützung von Innovationen durch EU-Start-ups im Technologiebereich, insbesondere in Sektoren mit kritischen Abhängigkeiten; unterstützt ferner die langfristige Vision von EU-Social-Media-Plattformen, die im Einklang mit den EU-Werten Transparenz, Datenschutz, Meinungsfreiheit und demokratische Rechenschaftspflicht gestaltet sind;

23. fordert die Kommission, die digitalen Regulierungsbehörden der EU und Online-Plattformen auf, für Transparenz bei Programmen zur Umverteilung von Einnahmen zu sorgen, die es Akteuren in Bezug auf ausländische Informationsmanipulation und Einmischung oder sogar Einrichtungen, die auf der Sanktionsliste stehen, ermöglichen könnten, Einnahmen zu erzielen; ist der Ansicht, dass die Monetarisierung von Aktivitäten in Bezug auf ausländische Informationsmanipulation und Einmischung im Rahmen solcher Programme als Teil der Verpflichtungen zur Risikobewertung und Risikominderung gemäß dem Gesetzes über digitale Dienste angegangen werden sollte;

24. nimmt mit Besorgnis die Feststellungen der niederländischen Datenschutzbehörde zur Kenntnis, wonach KI-Chatbots voreingenommene und unzuverlässige Wahlempfehlungen geben können, wodurch die Integrität von Wahlen gefährdet wird; fordert die Kommission auf, ihrer Verpflichtung nachzukommen, Leitlinien für den Einsatz von KI in Wahlprozessen zu erstellen, um einen verantwortungsvollen Umgang mit KI sicherzustellen;

Redefreiheit

25. betont, dass der Europäische Schutzschild für die Demokratie die Meinungs- und Informationsfreiheit als ein Grundrecht schützen und wahren muss, das sowohl im Online- als auch im Offline-Bereich gilt; betont, dass Menschenrechte in der EU im weltweiten Vergleich zu den am stärksten geschützten zählen und dass Unternehmen, die in der EU tätig sein und europäische Kunden anziehen möchten, eine gemeinsame Verantwortung für den Schutz dieser Rechte tragen; betont jedoch, dass die Meinungs- und Informationsfreiheit so konzipiert wurde, dass sie den Menschen schützt, und nicht

Maschinen oder Software, die unehrliches Verhalten zeigen, wie KI und botbasierte Verstärkung und Steuerung sowie automatisierte Softwareprogramme, die repetitive Aufgaben über ein Netzwerk ausführen, um echte Nutzer nachzuahmen;

26. würdigt, wie wichtig wirksame Schutzmaßnahmen für Nutzer bei der Ausübung ihrer demokratischen Rechte sind, darunter die Möglichkeit, Entscheidungen der Plattformen zur Moderation von Inhalten anzufechten, und die Verpflichtung der Plattformen, Nutzer zu informieren, wenn ihre Inhalte entfernt oder eingeschränkt werden; weist erneut darauf hin, dass Plattformen gemäß dem Gesetz über digitale Dienste verpflichtet sind, zu diesem Zweck einen gesonderten Mechanismus für die Bearbeitung von Beschwerden bereitzustellen; betont, dass der Schutz der Grundrechte einzelner Nutzer auch die Durchführung gründlicher Bewertungen und die Minderung systemischer Risiken umfasst, die die Integrität des Informationsraums beeinträchtigen;

Medien- und Informationsintegrität

27. ist der Ansicht, dass Maßnahmen zur Förderung freier und redaktionell unabhängiger Medien ein zentraler Bestandteil der Verwirklichung der Ziele des Europäischen Schutzschildes für die Demokratie sind; begrüßt in diesem Zusammenhang die bahnbrechenden gemeinsamen Mindeststandards für Medienfreiheit und -pluralismus, die durch die Annahme des Europäischen Medienfreiheitsgesetzes eingeführt wurden; weist jedoch darauf hin, dass die Bedeutung der Verordnung nur anhand ihrer Umsetzung in der Praxis beurteilt werden kann, und betont daher die Bedeutung einer strikten Durchsetzung; begrüßt die neuen Verpflichtungen im Bereich Medienförderung, die im Rahmen des Programms für Medienresilienz angekündigt wurden, und fordert entsprechende langfristige Verpflichtungen im kommenden MFR;

28. betont, dass die potenziellen Auswirkungen der EU-Rechtsvorschriften auf den Journalismus und die redaktionellen Medien sorgfältig geprüft werden müssen, insbesondere im Hinblick auf die Sicherung der Nachhaltigkeit und Rentabilität der Geschäftsmodelle von Medienunternehmen;

29. betont in Bezug auf Medienunternehmen, die Abonnements über Apps verkaufen, dass das Gesetz über digitale Märkte vollständig umgesetzt werden muss; nimmt in diesem Zusammenhang den Nichteinhaltungsbeschluss der Kommission vom 23. April 2025 in Bezug auf Apple und Meta zur Kenntnis; nimmt die Untersuchung der Kommission zu einem potenziellen Verstoß gegen das Gesetz über digitale Märkte durch Google in Form der Herabstufung der Inhalte von Medienverlagen in den Suchergebnissen zur Kenntnis;

30. begrüßt, dass die gemeinsame Mitteilung neue Unterstützungsmaßnahmen zur Förderung der digitalen Kompetenz und der Medienkompetenz umfasst, wie das Programm für Medienresilienz, die Initiative zur Förderung von Grundkompetenzen für Schulen und die Stärkung der Expertengruppe für Medienkompetenz, einschließlich der Einrichtung eines neuen Expertennetzes für Medienkompetenz, sowie aktualisierte Leitlinien für Lehrkräfte und pädagogische Fachkräfte; betont, dass bei der bevorstehenden Überarbeitung der Richtlinie über audiovisuelle Mediendienste die Bestimmungen über Mindestanforderungen für die Arbeit der Mitgliedstaaten im Bereich der Medienkompetenz gestärkt werden sollten;

31. begrüßt die angekündigte Aktualisierung der Empfehlung der Kommission zur Sicherheit von Journalisten[52] und die bevorstehende Überprüfung der Empfehlung zur Bekämpfung von SLAPP-Klagen[53]; betont, dass bei diesen Aktualisierungen und Überprüfungen berücksichtigt werden muss, wie sich Bedrohungen, Gewalt, Sabotage und andere Maßnahmen, die darauf abzielen, die journalistische Arbeit zu behindern, auf den Schutz, die Sicherheit und die Handlungskompetenz von Journalisten und anderen Medienschaffenden in der EU auswirken;

32. betont, dass Journalisten vor missbräuchlichen Klagen geschützt werden müssen; begrüßt in diesem Zusammenhang die Annahme der Richtlinie zur Bekämpfung von SLAPP-Klagen[54] und die angekündigte Erneuerung des Mandats und der Zusammensetzung der Expertengruppe gegen SLAPP-Klagen; fordert die Mitgliedstaaten auf, den laufenden Umsetzungsprozess ambitioniert voranzutreiben, und fordert die Kommission auf, weiterhin Unterstützung zu leisten; fordert die Kommission auf, einen umfassenden Evaluierungsbericht über die Erfolge der Umsetzung auszuarbeiten;

33. begrüßt die vorläufige Einigung über die Verordnung über ausländische Direktinvestitionen[55], insbesondere die Bestimmungen, nach denen die Medienbranche als ein Faktor einbezogen wird, der bei der Feststellung, ob es wahrscheinlich ist, dass sich eine Investition negativ auf die Sicherheit oder die öffentliche Ordnung auswirkt, zu berücksichtigen ist; bedauert jedoch, dass die Medienbranche nicht im verbindlichen Anwendungsbereich im Anhang der Verordnung aufgeführt ist;

34. fordert die Kommission und die Mitgliedstaaten auf, die Folgen des veränderten Zugangs der US-Regierung zur Beihilfepolitik im Zusammenhang mit Medienpluralismus und unabhängigem Journalismus sorgfältig zu analysieren und erforderlichenfalls tätig zu werden, um die auf den Medienmärkten sowohl innerhalb der EU als auch in den Grenzregionen entstandene Lücke zu schließen; begrüßt die Soforthilfe der EU für RFE/RL; fordert die Ausarbeitung einer Lösung, um RFE/RL mit einer stabilen, langfristigen Finanzierung auszustatten;

35. betont, dass gesellschaftsbasierte Faktenprüfnetze bei der Aufdeckung und Bekämpfung von Desinformationskampagnen mitwirken und wertvolle Erkenntnisse für Risikobewertungen im Rahmen der Verordnung über digitale Dienste liefern können; hält fest, dass unabhängige Faktenprüforganisationen für ihre Arbeit stabile

---

[52] Empfehlung (EU) 2021/1534 der Kommission vom 16. September 2021 zur Gewährleistung des Schutzes, der Sicherheit und der Handlungskompetenz von Journalisten und anderen Medienschaffenden in der Europäischen Union (ABl. L 331 vom 20.9.2021, S. 8, ELI: http://data.europa.eu/eli/reco/2021/1534/oj).
[53] Empfehlung (EU) 2022/758 der Kommission vom 27. April 2022 zum Schutz von Journalisten und Menschenrechtsverteidigern, die sich öffentlich beteiligen, vor offenkundig unbegründeten oder missbräuchlichen Gerichtsverfahren („Strategische Klagen gegen öffentliche Beteiligung“) (ABl. L 138 vom 17.5.2022, S. 30, ELI: http://data.europa.eu/eli/reco/2022/758/oj).
[54] Richtlinie (EU) 2024/1069 des Europäischen Parlaments und des Rates vom 11. April 2024 über den Schutz von Personen, die sich öffentlich beteiligen, vor offensichtlich unbegründeten Klagen oder missbräuchlichen Gerichtsverfahren („strategische Klagen gegen öffentliche Beteiligung“) (ABl. L, 2024/1069, 16.4.2024, ELI: http://data.europa.eu/eli/dir/2024/1069/oj).
[55] Verordnung (EU) 2019/452 des Europäischen Parlaments und des Rates vom 19. März 2019 zur Schaffung eines Rahmens für die Überprüfung ausländischer Direktinvestitionen in der Union (ABl. L 79I vom 21.3.2019, S. 1, ELI: http://data.europa.eu/eli/reg/2019/452/oj).

Bedingungen benötigen; ist der Ansicht, dass das von der Kommission 2025 angekündigte Europäische Netz von Faktenprüfern ein Instrument sein könnte, um das zu erreichen; betont, dass Faktenprüforganisationen strenge Standards hinsichtlich politischer Neutralität, Unabhängigkeit und methodischer Objektivität einhalten müssen, um vertrauenswürdig und erfolgreich zu sein;

Zivilgesellschaft

36. betont, dass die Zivilgesellschaft bei der Verteidigung unserer Demokratie eine entscheidende Rolle spielt, und zwar nicht nur indem sie Manipulationsversuche demokratischer Prozesse aus dem Ausland als wachsame Instanz aufdeckt und aktiv bekämpft, sondern auch als elementare Kraft bei den langfristigen Bemühungen um den Aufbau stärkerer und widerstandsfähigerer Gesellschaften; hebt insbesondere hervor, dass die Zivilgesellschaft einen wichtigen Beitrag zur Wahrung der in Artikel 2 EUV verankerten Werte leistet;

37. begrüßt die EU-Strategie für die Zivilgesellschaft der Kommission, die zusammen mit der Mitteilung über den Europäischen Schutzschild für die Demokratie veröffentlicht wurde; begrüßt den Ansatz der Kommission, diese Strategie mit ihrer Arbeit am Schutzschild zu verknüpfen und damit das bürgerschaftliche Engagement weiter zu stärken;

38. fordert die Kommission auf, ihre Anstrengungen im Bereich des zivilen Dialogs zu intensivieren und neue Instrumente dafür zu schaffen; begrüßt in diesem Zusammenhang die Zusage der Kommission, bis 2026 eine funktionsfähige Plattform der Zivilgesellschaft einzurichten, um einen systematischeren Ansatz voranzutreiben, der zur Stärkung des Dialogs im Einklang mit den Werten der EU genutzt wird; ist der Ansicht, dass die angekündigte Online-Wissensplattform zum zivilgesellschaftlichen Raum zur Koordinierung der Aktivitäten von Organisationen der Zivilgesellschaft im Bereich des Schutzes der Demokratie und der Bekämpfung von hybriden Bedrohungen und von Informationsmanipulation und Einflussnahme aus dem Ausland beitragen und das Situationsbewusstsein verbessern könnte;

39. betont, dass konkreten Finanzierungsprogrammen wie dem Programm „Bürgerinnen und Bürger, Gleichstellung, Rechte und Werte“ große Bedeutung zukommt; begrüßt die Idee der Kommission, das Programm „Bürgerinnen und Bürger, Gleichstellung, Rechte und Werte“ beizubehalten und in das neue Programm AgoraEU für den Zeitraum 2028-2034 aufzunehmen; fordert die Kommission auf, dafür Sorge zu tragen, dass die Mittel für diesen Aktionsbereich von AgoraEU den Bedürfnissen der Organisationen der Zivilgesellschaft entsprechen und in direkter Mittelverwaltung durch die Kommission ausgeführt werden;

40. hebt hervor, dass es in Bezug auf die Finanzierung von Organisationen der Zivilgesellschaft im Allgemeinen und hinsichtlich der Unterstützung durch Drittländer im Besonderen mehr finanzieller Transparenz bedarf; weist darauf hin, dass Organisationen der Zivilgesellschaft von böswilligen Akteuren aus Drittländern als Instrumente zur unrechtmäßigen Einflussnahme auf demokratische Prozesse in der EU und ihren Mitgliedstaaten genutzt werden können und bereits genutzt wurden; betont, dass das Parlament als Organ angesichts des sogenannten Katargate-Skandals eine besondere Verantwortung dafür trägt, zu Reformen in diesem Bereich beizutragen; hebt

jedoch hervor, dass Maßnahmen zur Bewältigung dieser Frage so konzipiert sein sollten, dass sie nicht dazu missbraucht werden können, die rechtmäßigen Aktivitäten der Zivilgesellschaft als solche zu stigmatisieren;

41. begrüßt den Vorschlag der Kommission für eine Richtlinie über die Interessenvertretung im Auftrag von Drittländern, die einen wichtigen Bestandteil des Pakets zur Verteidigung der Demokratie darstellt und mit der harmonisierte Anforderungen für Wirtschaftstätigkeiten im Zusammenhang mit der Interessenvertretung im Auftrag einer Einrichtung aus Drittländern festgelegt werden sollen; betont, dass gemeinsame diesbezügliche Vorschriften eine wichtige Komponente der Schaffung von mehr Transparenz in Bezug auf die Einflussnahme von Drittstaaten wären; fordert die gesetzgebenden Organe auf, das Gesetzgebungsverfahren unverzüglich abzuschließen;

42. erachtet die Beteiligung der Bürgerinnen und Bürger an demokratischen Prozessen als äußerst wichtig; appelliert an die Kommission, in Zusammenarbeit mit den Mitgliedstaaten für eine klare und wirksame Kommunikation über die Initiativen, die sie zur Förderung und Ausweitung der Nutzung ihrer Instrumente zur Bürgerbeteiligung erarbeitet, zu sorgen; begrüßt, dass die Kommission diese Instrumente – insbesondere die Europäische Bürgerinitiative, die europäischen Bürgerforen und die Plattform für Bürgerbeteiligung – stärkt und vorgeschlagen hat, das Netz der nationalen Behörden für die Bürgerbeteiligung auszubauen;

Schutz kritischer Infrastruktur

43. vertritt den Standpunkt, dass der Schutz der EU und ihrer Mitgliedstaaten vor physischen und digitalen Sabotageakten gegen kritische Infrastruktur ein wesentlicher Aspekt der Wahrung der demokratischen Resilienz ist; fordert solide Präventivmaßnahmen, eine verstärkte grenzüberschreitende Zusammenarbeit und eine verbesserte Fähigkeit der EU, derartige feindselige Aktivitäten aufzudecken, zu verhindern und auf sie zu reagieren;

44. verurteilt aufs Schärfste das insbesondere von Russland und Belarus ausgehende und oft zu Eskalationen führende Eindringen von unter anderem Drohen in den Luftraum, das kritische Infrastruktur wie zivile Flughäfen, Militärstützpunkte und Energieanlagen in der gesamten EU und deren Störung zum Ziel hat; fordert die Mitgliedstaaten auf, koordiniert, geeint und angemessen auf jede Verletzung ihres Luftraums zu reagieren, unter anderem durch den Abschuss von Flugzeugen, Drohnen und anderen Fluggeräten, die eine Bedrohung darstellen;

45. betont, dass mehrere hybride Aktivitäten Russlands gegen die EU staatlich gefördertem Terrorismus gleichkommen, auch wenn die Schwelle zu einem bewaffneten Angriff noch nicht überschritten ist; hebt daher hervor, dass die verfügbaren rechtlichen Rahmenregelungen zur Terrorismusbekämpfung auf die feindseligen Handlungen Russlands angewandt werden müssen, zumal diese die territoriale Unversehrtheit der EU-Mitgliedstaaten verletzen, die Integrität ihrer Institutionen schwächen und die Sicherheit der Zivilbevölkerung unmittelbar gefährden; betont, dass die EU dringend von einem Verteidigungsmodus zur aktiven Abschreckung übergehen muss; fordert die Mitgliedstaaten nachdrücklich auf, den rechtlichen und operativen Rahmen für verhältnismäßige Offensivmaßnahmen, die auf die logistische und digitale Infrastruktur hinter den destabilisierenden Aktivitäten Moskaus abzielen, zu bewerten;

46. fordert die Kommission und die Mitgliedstaaten auf, eine gemeinsame Auslegung des Seerechtsübereinkommens der Vereinten Nationen (SRÜ) durch die EU zu begründen, um für ein koordiniertes Vorgehen gegen hybride Aktivitäten und Sabotage in den Meeresgebieten der EU, insbesondere in der Ostsee, zu sorgen; ist der Ansicht, dass die grenzübergreifende Koordinierung sowohl auf operativer als auch auf finanzieller Ebene weiter verbessert werden kann; betont, dass die EU ihre Reaktion auf hybride Bedrohungen in Meeresgebieten verstärken muss, einschließlich solcher, die von der russischen „Schattenflotte“ ausgehen; unterstreicht, dass zur Bewältigung dieser Herausforderungen zweckgebundene und ausreichende EU-Mittel notwendig sind;

47. nimmt mit Besorgnis zur Kenntnis, dass bei der digitalen Infrastruktur der EU strukturelle Abhängigkeiten durch Marktkonzentration und ausländische Kontrolle bestehen, unter anderem bezüglich Betriebssystemen, Rechenzentren, Halbleitern, KI, Cybersicherheit, Cloud-Computing und verschiedenen digitalen Plattformen und Diensten, die allesamt ein hohes Risiko für Demokratie, Freiheit und Sicherheit in der EU und für die Wettbewerbsfähigkeit der EU bergen; fordert die Kommission und die Mitgliedstaaten auf, eine souveräne digitale Infrastruktur der EU mit Technologien, mit denen die Privatsphäre gewahrt bleibt, und einem auf Programmierschnittstellen (API) basierenden Ökosystem der EU als Unterbau einzurichten, indem ambitionierte, zielgerichtete Maßnahmen zur Steigerung der Investitionen in EU-Unternehmen und von deren Marktanteil ergriffen werden, und sich beim Aufbau von Rechenzentren und Cloud-Infrastruktur – unter anderem durch marktorientierte Initiativen wie Joint Ventures oder dem Verbund aus Netzwerken in Bereichen wie KI-Gigafabriken oder Cloud-Dienste – die europäische Versorgung mit sauberer Energie zu Nutze zu machen;

48. betont, dass für eine stärkere Integration zwischen digitaler Infrastruktur, Cybersicherheit und Verteidigungspolitik gesorgt werden muss, um die strategische Autonomie der EU voranzubringen, und dass Infrastruktur mit doppeltem Verwendungszweck wie resiliente Rechenzentren, die verstreut auf dem Gebiet der EU bestehen, wirksam eingesetzt werden müssen, um die Betriebskontinuität angesichts hybrider oder kriegsbedingter Bedrohungen sicherzustellen; hebt ferner hervor, dass die Investitionen in militärische Mobilität und sichere Kommunikationswege erhöht werden müssen, unter anderem in den dringlichen und vorrangigen Einsatz weltraumgestützter Fähigkeiten wie IRIS², um verschlüsselte Dienste für die öffentliche Nutzung und für Verteidigungszwecke bereitzustellen;

49. betont, dass Cybersicherheitsrahmen wie die NIS-2-Richtlinie, die Cyberresilienz-Verordnung[56] und die Cybersolidaritätsverordnung[57] aufeinander abgestimmt funktionieren müssen, um Standards zu unterstützen, die dem Prinzip „Sicherheit durch Design“ folgen, und um eine regulatorische Fragmentierung zu vermeiden; fordert in diesem Zusammenhang eine Überarbeitung der einschlägigen Rechtsvorschriften im Bereich Cybersicherheit und unterstreicht, dass bestehende Strukturen wie die ENISA

[56] Verordnung (EU) 2024/2847 des Europäischen Parlaments und des Rates vom 23. Oktober 2024 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnungen (EU) Nr. 168/2013 und (EU) 2019/1020 und der Richtlinie (EU) 2020/1828 (Cyberresilienz-Verordnung) (ABl. L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).
[57] Verordnung (EU) 2025/38 des Europäischen Parlaments und des Rates vom 19. Dezember 2024 über Maßnahmen zur Stärkung der Solidarität für und der Kapazitäten in der Union für die Erkennung von, Vorsorge für und Bewältigung von Cyberbedrohungen und Sicherheitsvorfällen und zur Änderung der Verordnung (EU) 2021/694 (Cybersolidaritätsverordnung) (ABl. L, 2025/38, 15.1.2025, ELI: http://data.europa.eu/eli/reg/2025/38/oj).

und das Europäische Kompetenzzentrum für Cybersicherheit gestärkt werden müssen;

50. weist darauf hin, dass die NIS-2-Richtlinie nur in geringem Maße umgesetzt wurde; bedauert, dass die Kommission nach Ablauf der Frist am 17. Oktober 2024 Aufforderungsschreiben an nicht weniger als 23 Mitgliedstaaten senden musste, weil diese die Richtlinie nicht vollständig umgesetzt hatten; fordert die Mitgliedstaaten dringend auf, die Umsetzung der Richtlinie so bald als möglich abzuschließen, zumal sie Ende 2025 – mehr als ein Jahr nach Ablauf der Frist – in zehn Mitgliedstaaten noch ausstand; begrüßt in diesem Zusammenhang die Zusage der Kommission, eng mit den Mitgliedstaaten zusammenzuarbeiten, um eine rasche und kohärente Umsetzung des horizontalen Cybersicherheitsrahmens gemäß der NIS-2-Richtlinie sowie der Cyberresilienz-Verordnung und der Cybersolidaritätsverordnung sicherzustellen, wie es in der Strategie für die innere Sicherheit „ProtectEU“ vorgesehen ist;

Zusammenarbeit in den Bereichen Justiz und Inneres

51. ist der Ansicht, dass alle auf Ebene der Mitgliedstaaten und der EU verfügbaren strafrechtlichen Instrumente angewandt und nötigenfalls weiterentwickelt werden sollten, um rechtswidriges Verhalten, das die Aushöhlung demokratischer Institutionen und Prozesse zum Ziel hat, zu verhindern und zu bekämpfen; befürwortet insbesondere das Bekenntnis der Kommission zur einer ambitionierten Überarbeitung des Mandats von Europol, um die Agentur zu einem wirklich operativen Polizeiamt zu machen, das die Mitgliedstaaten besser unterstützt;

52. begrüßt, dass in der gemeinsamen Mitteilung der positive Beitrag anerkannt wird, der dank der justiziellen Zusammenarbeit und der Kooperation im Bereich der Strafverfolgung bei der Bekämpfung von Informationsmanipulation und Einflussnahme aus dem Ausland und Desinformation erzielt wird; fordert die Kommission auf, bei der Vorbereitung der geplanten Überarbeitung der Mandate von Europol und Eurojust sorgfältig die rechtlichen Lücken zu beurteilen, die die Agenturen derzeit daran hindern, den mit hybriden Bedrohungen konfrontierten Mitgliedstaaten uneingeschränkte Unterstützung zu leisten, und Möglichkeiten zu prüfen, diese Lücken zu schließen;

53. nimmt mit Besorgnis zur Kenntnis, dass es zunehmend Beispiele dafür gibt, dass böswillige Akteure aus Drittländern Kriminalität als Dienstleistung und kriminelle Organisationen als Stellvertreter innerhalb der EU nutzen, um Personen und Organisationen, die sie als politische Gegner einstufen, ins Visier zu nehmen, was eine ernsthafte Bedrohung für die innere Sicherheit der EU darstellt; betont, dass solche Praktiken ein nicht hinnehmbarer Akt der Einflussnahme aus dem Ausland sind, der sich potenziell destabilisierend auf unsere Gesellschaften auswirkt; unterstreicht in diesem Zusammenhang, dass die Koordinierung auf EU-Ebene in den Bereichen Strafgerichtsbarkeit und Strafverfolgung weiter intensiviert werden muss;

54. verurteilt aufs Schärfste, dass Migration als Waffe gegen die EU eingesetzt und instrumentalisiert wird; vertritt den Standpunkt, dass dieses Phänomen einen inakzeptablen Versuch böswilliger Drittländer darstellt, politischen Druck auf die Mitgliedstaaten an den Außengrenzen und die EU auszuüben; begrüßt die spezifischen Bestimmungen zur Instrumentalisierung der Migration, die kürzlich in wichtige EU-Rechtsvorschriften zum Grenzmanagement und zur Migration aufgenommen wurden;

betont, dass die von derartigen Bedrohungen betroffenen Mitgliedstaaten sich auf die Unterstützung spezialisierter EU-Agenturen verlassen können müssen; fordert, dass das Mandat von Frontex gestärkt wird, damit die Agentur über die Rechtsgrundlage und die personellen, finanziellen und technischen Ressourcen verfügt, die sie braucht, um die Mitgliedstaaten bei der Bewältigung derartiger hybrider Bedrohungen ordnungsgemäß zu unterstützen; hebt in diesem Zusammenhang hervor, dass die Fähigkeit der EU, durch ausreichende Investitionen im Rahmen des MFR 2028-2034 zu den Grenzschutzbemühungen der Mitgliedstaaten beizutragen, weiter verbessert werden muss;

Externe Dimension

55. betont, dass der Europäische Schutzschild für die Demokratie eine solide externe Dimension haben muss; begrüßt, dass spezifische Maßnahmen in die gemeinsame Mitteilung aufgenommen wurden, mit denen Ländern außerhalb der EU-Grenzen unterstützt werden, indem insbesondere der Kapazitätsaufbau gefördert wird, damit Bewerberländer und potenzielle Bewerberländer widerstandfähiger gegenüber Informationsmanipulation und Einflussnahme aus dem Ausland und hybrider Einmischung werden, und indem unabhängige Medien und unabhängiger Journalismus unterstützt werden und deren Fähigkeit gestärkt wird, Desinformation in den sozialen Medien vor und während Wahlen im Blick zu behalten;

56. befürwortet die Idee, diplomatische Kanäle zu nutzen, um die Kapazitäten in vorrangigen Regionen auszubauen; ist der Ansicht, dass den EU-Delegationen und den Botschaften der EU-Mitgliedstaaten eine Schlüsselrolle zukommt, wenn es darum geht, ein besseres Verständnis der lokalen Gegebenheiten zu erlangen, die zu Einflussnahme aus dem Ausland führen können, und angepasst zu reagieren; stellt fest, dass die EU-Delegationen und die Botschaften der Mitgliedstaaten die Organisation von Sensibilisierungskampagnen in den Gastländern unterstützen können; betont, dass Missionen und Operationen im Rahmen der Gemeinsamen Sicherheits- und Verteidigungspolitik (GSVP) in die in der gemeinsamen Mitteilung vorgesehenen Maßnahmen einbezogen werden müssen; fordert die Mitgliedstaaten und den EAD auf, Maßnahmen zum Kapazitätsaufbau und Schulungen zu hybriden Bedrohungen in die einzelnen Mandate von Missionen und Operationen aufzunehmen, damit die nationalen Partner besser gewappnet sind;

57. fordert die Ausarbeitung einer umfassenden Strategie, mit der die EU-Delegationen und die GSVP-Missionen und -Operationen in enger Abstimmung mit den diplomatischen Vertretungen der EU-Mitgliedstaaten wirksamer als erste Verteidigungslinie gegen hybride Angriffe agieren können, was unter anderem Cyberoperationen und Operationen im Bereich Informationsmanipulation und Einflussnahme aus dem Ausland umfasst; ist der Ansicht, dass verstärkte Kapazitäten für strategische Kommunikation und öffentliche Diplomatie innerhalb der EU-Delegationen von entscheidender Bedeutung sind und der Schwerpunkt dabei darauf liegen sollte, faktenbasierte Narrative, bürgerschaftliches Engagement und Vertrauensbildung, insbesondere bei jungen Menschen und Lehrkräften, zu befördern; fordert die Vizepräsidentin der Kommission und Hohe Vertreterin der Union für Außen- und Sicherheitspolitik und den Rat auf, Teams für die Überwachung von und die Reaktion auf Desinformation in GSVP-Missionen aufzunehmen, für Schulungen im Bereich Informationsmanipulation und Einflussnahme aus dem Ausland für das gesamte Missionspersonal zu sorgen und

die Koordinierung zwischen zivilen und militärischen Operationen zu stärken, um hybriden Einflüssen entgegenzuwirken;

58. begrüßt das verstärkte Bekenntnis zum Aufbau von Offensivkapazitäten für Informationsoperation, das in der gemeinsamen Mitteilung zum Ausdruck kommt; stellt fest, dass angesichts eines derartigen Bekenntnisses zweckgebundene Ressourcen und langfristige Planung notwendig sind; betont, dass das Ziel unter anderem darin bestehen sollte, dass die EU in ihrer Nachbarschaft proaktive Informationsmaßnahmen stärkt, um Russlands Destabilisierungsanstrengungen entgegenzuwirken; unterstreicht, dass Menschen, die unter autoritären Regimen und insbesondere in Russland leben, sachliche und vertrauenswürdige Informationen zur Verfügung gestellt werden müssen, um die destruktiven Governance-Praktiken der Regierenden aufzudecken, zumal diese die Freiheit und den Frieden nicht nur in den Nachbarländern, sondern in erster Linie innerhalb ihres eigenen Landes gefährden; fordert, dass der digitale Raum und der Cyberspace sowie die Tatsache, dass sie nicht an Grenzen gebunden sind, in jeder erdenklichen Weise genutzt werden, um dieses Ziel zu erreichen;

59. stellt fest, dass die unmittelbaren Nachbarn der EU, darunter der Westbalkan, die Republik Moldau und die Ukraine, erheblicher Einflussnahme aus dem Ausland ausgesetzt sind; fordert die Finanzierung regionaler Koordinierungszentren für die Bekämpfung von Informationsmanipulation und Einflussnahme aus dem Ausland, eine verstärkte Unterstützung für investigativen Journalismus und Medienregulierungsbehörden und die Ausweitung der faktengestützten strategischen Kommunikation mithilfe der EU-Delegationen, um gegen die EU gerichteter Desinformation entgegenzutreten; unterstreicht, dass ein besonderer Schwerpunkt auf unterstützenden Maßnahmen für die Integrität von Wahlen in den Ländern, die EU-Beitrittskandidaten sind, liegen muss;

60. fordert die Kommission auf, Medienkompetenzprogramme zu einem festen Bestandteil der Heranführungshilfe und des Europäischen Nachbarschaftsinstruments zu machen und dabei spezielle EU-Finanzhilfen zur Unterstützung von investigativem Journalismus in gefährdeten Regionen vorzusehen;

61. fordert, dass die derzeitigen Bemühungen der EU verstärkt werden, die Partnerländer in ihrer Nachbarschaft sowie in vorrangigen Ländern in Subsahara-Afrika, im asiatisch-pazifischen Raum und in Lateinamerika beim Aufbau ihrer Resilienz gegenüber Informationsmanipulation und Einflussnahme aus dem Ausland, bei der Stärkung demokratischer Prozesse und bei der Sicherstellung der Integrität von Wahlen zu unterstützen; betont insbesondere, dass das Leitprojekt EUvsDisinfo weiterentwickelt werden muss;

62. würdigt die Einrichtung der EUPM Moldova als erfolgreiches Beispiel dafür, wie die EU eine entscheidende Rolle bei der Unterstützung der Krisenmanagementstrukturen eines Partnerlandes und der Stärkung seiner Resilienz gegenüber hybriden Bedrohungen, Cyberbedrohungen und Bedrohungen durch Informationsmanipulation und Einflussnahme aus dem Ausland spielen kann; ist der Ansicht, dass die EUPM Moldova als Vorbild dienen sollte, was die Einbeziehung der Abwehr hybrider Bedrohungen in das Mandat bestehender Missionen bzw. die Einrichtung ähnlicher Missionen in anderen Partnerländern betrifft; nimmt die Parlamentswahl in der

Republik Moldau vom 28. September 2025 und den klaren Sieg der proeuropäischen Partei Aktion und Solidarität (PAS) zur Kenntnis;

63. begrüßt die Entsendung von EU-Teams für die rasche Reaktion auf hybride Bedrohungen, zumal sie – wie das jüngste Beispiel der Republik Moldau zeigt – ein nützliches Instrument für den auf dem spezifischen Know-how und der Expertise der EU und ihrer Mitgliedstaaten gründenden Aufbau von Kapazitäten und Resilienz in Ländern sind, die Ziel von hybriden Angriffen, Cyberangriffen und Informationsmanipulation und Einflussnahme aus dem Ausland sind;

64. erachtet es als äußerst wichtig, den Grundsätzen und Zielen des Europäischen Schutzschilds für die Demokratie in der internationalen Zusammenarbeit mit gleichgesinnten Partnern wie der G7, der NATO, den Vereinten Nationen, der Organisation für Sicherheit und Zusammenarbeit in Europa und dem Europarat Vorrang einzuräumen; begrüßt die Schritte, die bereits im Rahmen des bilateralen und multilateralen Engagements unternommen wurden, insbesondere den Verhaltenskodex der Vereinten Nationen für die Informationsintegrität auf digitalen Plattformen, die Zusage der Mitgliedstaaten des Europarats in der Erklärung von Reykjavik, Wahlsysteme vor ausländischer Einflussnahme zu schützen, die Sicherheits- und Verteidigungspartnerschaften und die anhaltenden Bemühungen im Rahmen des Krisenreaktionsmechanismus der G7, kollektive Reaktionen auf Informationsmanipulation und Einflussnahme aus dem Ausland vorzusehen und auszuarbeiten;

65. begrüßt die Einrichtung einer Sicherheits- und Verteidigungspartnerschaft zwischen der EU und dem Vereinigten Königreich im Mai 2025; bewertet es als positiv, dass ihr Schwerpunkt unter anderem auf der Zusammenarbeit bei der Bekämpfung von Cyberbedrohungen, hybriden Bedrohungen und Informationsmanipulation und Einflussnahme aus dem Ausland sowie auf dem Schutz kritischer Infrastruktur liegt;

Wahlsysteme und Resilienz bei Wahlen

66. betont, dass es ein Kernziel des Europäischen Schutzschilds für die Demokratie sein sollte, die Integrität von Wahlen auf lokaler, regionaler, nationaler und EU-Ebene zu schützen; fordert die Kommission und die Mitgliedstaaten auf, unter uneingeschränkter Achtung des Subsidiaritätsprinzips bei der Umsetzung von Reformen zusammenzuarbeiten, die darauf abzielen, die Resilienz von Wahlprozessen in Europa zu stärken, und dabei einen besonderen Schwerpunkt auf Maßnahmen zur Verhinderung ausländischer Einflussnahme zu legen;

67. fordert die Mitgliedstaaten auf, ihre Anstrengungen zur Umsetzung der Empfehlungen der Kommission für inklusive, belastbare und stabile Wahlverfahren in der EU zu verstärken; betont insbesondere, dass es wichtig ist, nationale Wahlnetzwerke einzurichten, um die nationalen Behörden und Fachstellen dabei zu unterstützen, sich in ihrer Arbeit aufeinander abzustimmen;

68. fordert die Mitgliedstaaten auf, dafür Sorge zu tragen, dass Wahlbehörden bzw. andere entsprechende Stellen, die für gut funktionierende, freie und faire Wahlen zuständig sind, ausreichend finanziert und mit den geeigneten Instrumenten ausgestattet sind, um ihre Aufgaben wahrnehmen zu können, sei es in Bezug auf die Schulung des Personals

und die erforderlichen digitalen Instrumente oder in Bezug auf die Sicherstellung ausreichender Investitionen in Wahlgremien und Wahlinfrastruktur;

69. ist der Ansicht, dass Hasskampagnen und Gewalt, die es Kandidaten erschweren, sich an der öffentlichen Debatte zu beteiligen oder mit Wählern zu interagieren, eine Bedrohung für die Demokratie darstellen; betont, dass solche Bedrohungen durch Versuche von Drittländern, die EU zu destabilisieren, verstärkt werden können; begrüßt in diesem Zusammenhang die Zusage der Kommission, Empfehlungen zur Sicherheit in der Politik vorzulegen; fordert die Mitgliedstaaten auf, ihre Bemühungen um den Schutz von Kandidaten, die sich zur Wahl stellen, und von gewählten Vertretern zu verstärken;

70. unterstreicht, dass das Europäische Kooperationsnetz für Wahlen eine wesentliche Funktion übernimmt, wenn es darum geht, den Austausch bewährter Verfahren hinsichtlich der Resilienz bei Wahlen in der EU und ihren Mitgliedstaaten zu gewährleisten; stellt jedoch fest, dass seine Tätigkeiten derzeit eingeschränkt sind; begrüßt die Zusage der Kommission, das ECNE zu stärken, einschließlich Reformen wie der Einrichtung eines Speichers gemeinsamer Referenzen und Standards für Wahlprozesse;

71. fordert die Kommission auf, sich stärker um Reformen des ECNE zu bemühen, unter anderem durch eine Überprüfung hinsichtlich seiner Ressourcen und seines ständigen Personals und durch die Weiterentwicklung des gemeinsamen Mechanismus zur Stärkung der Resilienz bei Wahlen; unterstreicht, dass konkrete Maßnahmen umgesetzt werden müssen, um die Beteiligung der Bewerberländer an den Tätigkeiten des ECNE zu forcieren; fordert die Kommission auf, im Rahmen des ECNE eine ständige Überwachungsgruppe einzurichten, die für die Aufsicht über die Umsetzung der Empfehlungen der Kommission zu inklusiven und stabilen Wahlverfahren in der EU und der künftigen Empfehlungen zur Sicherheit politischer Akteure zuständig ist; vertritt die Auffassung, dass es außerdem in den Aufgabenbereich dieser Überwachungsgruppe fallen sollte, Vorschläge für künftige Aktualisierungen dieser Empfehlungen auszuarbeiten;

72. fordert die Kommission auf, das Parlament und die Behörde für europäische politische Parteien und europäische politische Stiftungen (APPF) als ständige Partner in alle Sitzungen des ECNE einzubeziehen;

73. begrüßt das Ziel der Kommission, den Schutz von wahlbezogener Infrastruktur durch bestehende Rechtsvorschriften und Instrumente auszubauen; fordert die Kommission auf, diese Bemühungen durch eine gezielte Überarbeitung der Richtlinie über die Resilienz kritischer Einrichtungen zu ergänzen, damit die Wahlinfrastruktur in die Liste der wesentlichen Dienste im Bereich der öffentlichen Verwaltung gemäß der Richtlinie aufgenommen wird;

74. fordert die Kommission und die Mitgliedstaaten auf, sich mit dem Problem der Einmischung ausländischer Akteure in die parteipolitische Landschaft in Europa auseinanderzusetzen; nimmt mit Besorgnis verschiedene Beispiele für die Finanzierung extremistischer Bewegungen innerhalb der EU durch Drittstaaten zur Kenntnis; ist der Ansicht, dass finanzielle Transparenz ein wichtiges Instrument ist, um dieses Problem zu beleuchten, und fordert in diesem Zusammenhang einen verstärkten Austausch zwischen privaten und öffentlichen Einrichtungen; betont insbesondere, dass gegen

verdeckte politische Kommunikation, einschließlich undurchsichtiger Finanzierungsstrukturen und heimlicher Geldgeber, vorgegangen werden muss, um die demokratische Integrität zu wahren und Transparenz für die Bürgerinnen und Bürger zu gewährleisten;

75. nimmt mit Besorgnis die sich verdichtenden Beweise für Einflussnahme und Spionage aus dem Ausland im politischen System Europas zur Kenntnis; begrüßt die Ermittlungsbemühungen in den Mitgliedstaaten, die zu Verurteilungen und laufenden Verfahren im Zusammenhang mit Bestechung, Spionage und der Förderung fremder Staatsinteressen geführt haben; hebt die ernsthaften Risiken hervor, die durch unzureichende Sicherheitsmaßnahmen bei der Rekrutierung von Mitarbeitern und Partnern mit engen Verbindungen zu autoritären Regimen entstehen;

76. begrüßt die vor Kurzem angenommene überarbeitete Fassung der Verordnung über das Statut und die Finanzierung europäischer politischer Parteien und europäischer politischer Stiftungen; nimmt die Bestimmungen über die Finanzierung und Beteiligung von Parteien aus Drittländern zur Kenntnis; fordert die gesetzgebenden Organe auf, für ihre vollumfängliche und wirksame Durchsetzung zu sorgen;

77. stellt fest, dass die Entwicklungen im Bereich der Kryptowährungen eine potenzielle Sicherheitslücke schaffen, die sich aus einem Mangel an Transparenz und an Kontrollierbarkeit der Finanzierung politischer Parteien und Bewegungen in Europa ergibt; nimmt das Vorhaben der Kommission zur Kenntnis, unter dem Dach des Europäischen Kooperationsnetzes für Wahlen und in enger Zusammenarbeit mit anderen EU-Netzen und Interessenträgern nationale Sachverständige zusammenbringen, um zu diesem Thema bewährte Verfahren auszutauschen, mögliche Leitlinien auszuarbeiten und gemeinsame Maßnahmen zu fördern; fordert die Kommission auf, die Umsetzung des Pakets zur Bekämpfung der Geldwäsche und der Verordnung über Märkte für Kryptowerte weiterhin zu überwachen und etwaige Lücken, die noch in den Rechtsvorschriften bestehen, zu schließen;

Die Rolle von Sanktionen beim Schutz der Demokratie

78. ist der Ansicht, dass Sanktionen gegen fremde Staaten oder ausländische Einrichtungen bzw. Einzelpersonen, deren Handlungen darauf abzielen, die demokratische Integrität der EU oder ihrer Mitgliedstaaten zu schädigen, eine wichtige Komponente der Ziele des Europäischen Schutzschilds für die Demokratie darstellen; betont ferner, dass wirksame Sanktionen einen umfangreichen Maßnahmenkatalog umfassen müssen, darunter das Einfrieren und die Einziehung von Vermögenswerten, Zuweisung und Aufdeckung von Verantwortung, Erhöhungen von Kosten und Einschränkungen von Einnahmen, Einfuhr- und Ausfuhrverbote, Einreiseverbote und andere einschlägige restriktive Maßnahmen;

79. fordert die Kommission und die Mitgliedstaaten auf, verhängte Sanktionen regelmäßig und sorgfältig im Hinblick auf optimale Effizienz und eine eventuelle neuerliche Ausweitung zu bewerten, einschließlich sekundärer Sanktionen gegen Einrichtungen, die an der Umgehung von Sanktionen beteiligt sind; ist der Ansicht, dass die EU insbesondere im Bereich der hybriden Bedrohungen und destabilisierenden Aktivitäten Russlands ihre Sanktionsregelung weiter ausweiten sollte, indem sie die finanziellen und technischen Hilfsstrukturen wie Kryptobörsen, Werbenetze und Hosting-Anbieter

ins Visier nimmt, auf die sich Desinformation, Cyberangriffe und Wahleinmischung stützen, und gleichzeitig gegen die Proxy-Netzwerke Russlands in Drittländern, insbesondere in Afrika und im Nahen Osten, vorgeht und Sanktionen gegen Medienunternehmen, Logistikzentren und mit Wagner in Verbindung stehende Gruppen verhängt, die EU-feindliche Narrative verbreiten; ist der Ansicht, dass die EU, um die Kosten hybrider Aggressionen weiter zu erhöhen, Sekundärsanktionen auf Unternehmen aus Drittländern – und insbesondere aus China – ausweiten sollte, die russische Operationen erleichtern, und dass sie russischen Cybersöldnern die Nutzung von in der EU ansässigen Diensten wie Hosting-, Domain- und Cloud-Diensten untersagen und EU-Politiker oder -Lobbyisten, die verdeckt von Moskau finanziert werden, öffentlich bekannt machen und mit Sanktionen belegen sollte;

80. ist der Ansicht, dass die Identifizierung und Bekanntmachung von Herkunftsländern anstelle von Einzelpersonen oder Unternehmen ein wichtiger Schritt sein könnte, um das Problem der klar/eindeutig systematischen, vielschichtigen und oft staatlich finanzierten Einflussnahme anzuerkennen, an der Länder wie Russland oder Iran in ganz Europa beteiligt sind; begrüßt den Beschluss der Kommission, Russland gemäß dem EU-Rechtsrahmen zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung als Drittland mit hohem Risiko einzustufen, um die Integrität des Finanzsystems der EU zu wahren; weist darauf hin, dass mit der neuen Verordnung zur Bekämpfung der Geldwäsche eine zusätzliche Rechtsgrundlage für die Ermittlung gefährlicher Länder geschaffen wird, einschließlich solcher, die an der Verbreitung von Massenvernichtungswaffen beteiligt sind;

81. betont, dass die Wirksamkeit und Glaubwürdigkeit der EU-Sanktionen von einer strengen und konsequenten Durchsetzung abhängen; hebt hervor, dass die angekündigte Überarbeitung des Mandats der Europäischen Staatsanwaltschaft (EUStA) eine Gelegenheit bietet, ihre Rolle zu stärken und auf die Untersuchung und Strafverfolgung von Verstößen gegen Sanktionen auszuweiten;

82. verurteilt den politisch motivierten Einsatz „schwarzer Listen“ durch Russland, die sich gegen EU-Bürgerinnen und -Bürger, Vertreter von staatlichen Behörden und Handelsorganisationen, Journalisten, Akteure der Zivilgesellschaft und politische Amtsträger, einschließlich demokratisch gewählter Mitglieder des Europäischen Parlaments, richten; fordert eine besser koordinierte und entschlossenere Reaktion der EU auf diese willkürlichen Maßnahmen, um den Schutz und die Sicherheit der auf einer schwarzen Liste stehenden Personen sicherzustellen und ihnen Solidarität und die erforderliche Unterstützung entgegenzubringen; bekundet seine uneingeschränkte Unterstützung für alle betroffenen Personen;

Krisenvorsorge der EU

83. begrüßt die EU-Strategie für eine Union der Krisenvorsorge und betont, dass die in der Strategie festgelegten Ziele eng mit denen des Europäischen Schutzschilds für die Demokratie verknüpft sind; hebt ferner hervor, dass die Funktionsfähigkeit von Gesellschaften unter außerordentlichen oder disruptiven Bedingungen eine Voraussetzung für die demokratische Resilienz ist und dass Reformen zur Stärkung der Krisenvorsorge daher einen integralen Bestandteil des Europäischen Schutzschilds für die Demokratie bilden sollten;

84. fordert die rasche Entwicklung und Einführung einer EU-weiten, interoperablen Krisenwarn-App, die den Bürgerinnen und Bürgern in Notfällen zuverlässige und mehrsprachige Informationen in Echtzeit zur Verfügung stellt; empfiehlt, dass diese App in nationale und EU-Frühwarnsysteme integriert wird, für schutzbedürftige Gruppen zugänglich gemacht und regelmäßig entsprechend dem technologischen Fortschritt und den bewährten Verfahren des Krisenmanagements aktualisiert wird;

85. begrüßt die Initiativen in mehreren Mitgliedstaaten, eine Informationsbroschüre zur Notfallvorsorge von Haushalten mit klaren, praktischen Leitlinien zur Verfügung zu stellen, die auf die unterschiedlichen sozialen und geografischen Gegebenheiten Europas zugeschnitten sind, um die Bürgerinnen und Bürger bei der Vorsorge für Notfälle zu unterstützen; fordert die Kommission auf, eine Broschüre auf EU-Ebene zu erstellen, die an den grenzüberschreitenden und multinationalen Kontext angepasst ist und Empfehlungen zur Notfallbevorratung, praktische Anweisungen zur Selbstversorgung für mindestens 72 Stunden, grundlegende Hinweise zu Erster Hilfe und spezifische Empfehlungen für schutzbedürftige Gruppen, einschließlich älterer Menschen, Menschen mit Behinderungen und Familien mit Kindern, beinhaltet;

86. fordert die Organisation regelmäßiger groß angelegter, von der EU koordinierter Übungen zur Krisenvorsorge, an denen die EU-Organe, die Mitgliedstaaten, regionale und lokale Behörden, der Privatsektor und die Zivilgesellschaft beteiligt sind; empfiehlt für diese Übungen Simulationen von komplexen, realistischen Szenarien, einschließlich Cyberangriffen, Störungen kritischer Infrastruktur, koordinierter Desinformation und hybrider Krisen, die es erlauben, die Reaktionskapazitäten zu bewerten, die Interoperabilität zwischen den Regierungs- und Verwaltungsebenen zu verbessern und eine Krisenvorsorgekultur auf allen Ebenen zu fördern; fordert zu diesem Zweck die Einführung eines Europäischen Tags der Krisenvorsorge; schlägt als Tag für diese Veranstaltung den 24. Februar vor – das Datum der grundlosen groß angelegten militärischen Invasion Russlands in die Ukraine im Jahr 2022, das als Symbol für die Solidarität der EU mit der Ukraine dienen und daran erinnern sollte, dass eine verstärkte zivile und militärische Vorsorge gegen die zunehmenden Bedrohungen durch autoritäre Regime dringend nötig ist;

87. fordert die Kommission auf, die Möglichkeit zu prüfen, Erasmus+ oder ähnliche Programme auf grenzüberschreitende Initiativen zu Krisenvorsorgeschulungen von Beschäftigten in kritischen Sektoren wie Feuerwehrleuten, Gesundheitsfachkräften oder freiwilligen Katastrophenschutzhelfern, öffentlichen Bediensteten und Vertretern zivilgesellschaftlicher Organisationen sowie der breiten Öffentlichkeit auszuweiten; empfiehlt, dass diese Programme den grenzüberschreitenden und sektorübergreifenden Wissensaustausch sowie gemeinsame Übungen und Schulungen zu hybriden Bedrohungen und Notfällen fördern und die lokalen Vorsorgekapazitäten in allen Mitgliedstaaten stärken, wobei gefährdeten Regionen besondere Beachtung geschenkt werden sollte;

88. fordert die beschleunigte Einführung sicherer Kommunikationssysteme wie IRIS² und das Europäische System für kritische Kommunikation; betont, dass mit diesen Initiativen die Resilienz der Telekommunikation, die Kontinuität wesentlicher Dienste in Krisenzeiten, der Abbau externer Abhängigkeiten in strategischen Sektoren und eine verstärkte Cybersicherheit dieser Infrastrukturen sichergestellt werden;

89. fordert eine verstärkte Koordinierung zwischen den Organen, Einrichtungen und sonstigen Stellen der EU, den Mitgliedstaaten und den internationalen Partnern durch gemeinsame Plattformen zur Lageerfassung, gemeinsame Methoden und Mechanismen für einen raschen und sicheren Informationsaustausch; betont, dass diese Instrumente eine kohärente, flexible und koordinierte Reaktion auf hybride Bedrohungen ermöglichen, die Risikoerkennung verbessern und die kollektive Krisenvorsorge und Resilienz der EU stärken;

90. betont, dass die Krisenvorsorge im MFR 2028-2034 durchgängig berücksichtigt werden muss, um eine verlässliche Resilienz aufzubauen und ein ausreichendes Maß an ziviler und militärischer Vorsorge zu erreichen; fordert die Kommission nachdrücklich auf, gezielte Finanzierungsinstrumente zu entwickeln, die einschlägige Instrumente für Verteidigung und zivile Sicherheit, wie die Fazilität zur Verteidigung Europas und die Fazilität zur Sicherung Europas, miteinander kombinieren, um eine ausreichende und stabile Finanzierung für Projekte zur Stärkung der Resilienz, für technologische Innovationen und Fähigkeiten mit doppeltem Verwendungszweck, für Initiativen zur zivilen Vorsorge, für den Schutz kritischer Infrastruktur und für Bemühungen zur Stärkung der industriellen und technologischen Souveränität der EU bereitzustellen; stellt fest, dass in speziellen Finanzierungsströmen auch lokalen Krisenvorsorgemaßnahmen Vorrang eingeräumt werden sollte, insbesondere in den Gebieten, die am stärksten gefährdet und von hybriden Bedrohungen betroffen sind;

91. empfiehlt den Entscheidungsorganen der EU, ihre Strategien und Notfallpläne für den Fall eines offenen militärischen Angriffs gegen einen oder mehrere Mitgliedstaaten und ähnlicher Krisenszenarien zu überprüfen und zu optimieren; betont ferner, dass in allen Organen, Einrichtungen und sonstigen Stellen der EU ein Höchstmaß an Sicherheit und Gefahrenabwehr sichergestellt werden muss, auch im Bereich der Cybersicherheit sowie der Sicherheit und Integrität von Informationen, und dass die in diesem Zusammenhang erforderlichen Voraussetzungen geschaffen werden müssen, darunter die Einrichtung anerkannter sicherer Kommunikationskanäle und angemessener Sitzungssäle für Sitzungen unter Ausschluss der Öffentlichkeit; unterstreicht, dass die Vorschriften über Verstöße gegen die Sicherheit und Vertraulichkeit von Informationen streng durchgesetzt werden müssen, insbesondere vor dem Hintergrund eines erhöhten Risikos von Spionage und Sabotage; betont, dass hybride Bedrohungen auch abseits von offenen militärischen Konflikten nach wie vor wachsende Risiken für das tägliche Funktionieren der EU darstellen;

92. begrüßt die Bemühungen der Kommission, die physische Sicherheit und die Informationssicherheit innerhalb der EU-Organe, Einrichtungen und sonstigen Stelle zu stärken, wie in der Mitteilung des Managementkontrollgremiums vom Oktober 2025 dargelegt ist, einschließlich Pläne für sichere Sitzungssäle, verbesserter Verfahren für die Sicherheitsüberprüfung von Bediensteten, das Verschlusssachen bearbeitet, und der Einrichtung des Sicherheitskollegs, um regelmäßige Aktualisierungen zu Bedrohungsentwicklungen sicherzustellen; stellt fest, dass diese Maßnahmen erhöhten Risiken durch Spionage, Einflussnahme aus dem Ausland und hybride Bedrohungen entgegenwirken, die sich gegen die Entscheidungsprozesse der EU richten; betont jedoch, dass die Verbesserung der physischen Sicherheit durch robuste Cybersicherheitsprotokolle und Spionageabwehrkapazitäten ergänzt werden muss, um dem gesamten Spektrum der Infiltrationsrisiken zu begegnen; fordert die rasche Annahme des Vorschlags der Kommission für eine Verordnung über die

Informationssicherheit in den Organen, Einrichtungen und sonstigen Stellen der Union (COM(2022)0119); weist darauf hin, dass in der Cybersicherheitsverordnung für die Organe, Einrichtungen und sonstigen Stellen der EU ein Cybersicherheitshaushalt in Höhe von 10 % der Gesamtmittel für Informations- und Kommunikationstechnologien für EU-Einrichtungen empfohlen wird;

93. empfiehlt, dass weitere Maßnahmen ergriffen werden, um die Sicherheit und Resilienz des Parlaments gegen Einflussnahme aus dem Ausland sowie seine Krisenvorsorge und Funktionsfähigkeit im Krisenfall zu erhöhen; fordert in diesem Zusammenhang eine verstärkte Unterstützung seiner Mitglieder, einschließlich IT- und Sicherheitskontrollen, Schulungen und spezifischer Briefings im Vorfeld von Dienstreisen sowie verstärkter interdisziplinärer Schulungen und anderer Maßnahmen zur Stärkung der Resilienz, bei denen physische Sicherheit und Informationssicherheit, Gefahrenabwehr und Cybersicherheit miteinander kombiniert werden; fordert weitere gezielte Schulungen für die Bediensteten des Parlaments, um Informationsmanipulation zu verhindern; empfiehlt, sein Cybersicherheitsumfeld im Einklang mit der Cybersicherheitsverordnung zu stärken und seinen operativen Reifegrad zu erhöhen, um seine Resilienz im Bereich der Cybersicherheit weiter zu stärken und seine Kapazitäten zur Erkennung von Bedrohungen vor dem Hintergrund einer dynamischen Bedrohungslage im Bereich der Cybersicherheit und eines sich rasch wandelnden technologischen Umfelds zu verbessern;

94. stellt im Zusammenhang mit der inneren Sicherheit des Parlaments fest, dass die berufliche Nutzung privater Mobiltelefone und anderer Geräte wie Laptops durch Mitglieder und Bedienstete eine Schwachstelle darstellt, die für Angriffe auf das Organ ausgenutzt werden könnte; betont, dass die Mitglieder und die Bediensteten mit den für die Wahrnehmung ihrer Aufgaben erforderlichen IT-Geräten wie Mobiltelefonen und Laptops ausgestattet werden sollten; begrüßt in diesem Zusammenhang die Sicherheitsüberprüfungen, die den Mitgliedern und Bediensteten auf Anfrage angeboten werden, um potenzielle Spähsoftware auf privaten Geräten zu erkennen; fordert die Verwaltung auf, diese Überprüfungen zu systematisieren und auf alle Geräte auszuweiten, die für die Arbeit im Zusammenhang mit dem Parlament verwendet werden; fordert klarere Regeln und systematische und sachgerechte Leitlinien für die Mitglieder und die Bediensteten sowie Schutzmaßnahmen zur Minderung dieser Risiken, insbesondere während Dienstreisen;

95. fordert die Kommission und den EAD auf, das Parlament systematisch in ihre Vorsorgemaßnahmen und Übungen, wie die Übung „EU Integrated Resolve“, einzubeziehen;

°

° °

96. beauftragt seine Präsidentin, diese Entschließung dem Rat, der Kommission, der Vizepräsidentin der Kommission und Hohen Vertreterin der Union für Außen- und Sicherheitspolitik und den Regierungen und den Parlamenten der Mitgliedstaaten zu übermitteln.

BEGRÜNDUNG

Die Europäische Union gründet sich auf die Werte der Demokratie, der Rechtsstaatlichkeit und der Grundrechte, die das Fundament ihrer politischen Ordnung, ihrer institutionellen Legitimität und ihres gesellschaftlichen Zusammenhalts bilden. In den letzten Jahren wurden diese Grundlagen zunehmend zum Ziel von sich rasch intensivierenden feindseligen Aktivitäten. Informationsmanipulation und Einflussnahme aus dem Ausland, hybride Operationen, koordinierte Desinformationskampagnen und andere Formen böswilliger Einflussnahme haben an Umfang, Komplexität und Wirkung zugenommen.

Mit diesen Taktiken werden bewusst gesellschaftliche Brüche ausgenutzt, der öffentliche Diskurs manipuliert und Versuche unternommen, das Vertrauen der Bürgerinnen und Bürger in die Institutionen und demokratischen Prozesse der Union und ihrer Mitgliedstaaten zu zersetzen. Aufgrund ihres zunehmend digitalen Charakters – verstärkt durch undurchsichtige Online-Plattformen und grenzüberschreitende Verbreitungsnetze – wird die Bedrohungslage komplexer und der Umgang damit nur schwer durch einzelne Mitgliedstaaten zu bewältigen. Vor diesem Hintergrund hat die Union erkannt, dass eine besser koordinierte Reaktion mit einer stärker strategischen und vorausschauenden Ausrichtung erforderlich ist. Auf der Grundlage der Arbeit seiner früheren Sonderausschüsse zur Einflussnahme aus dem Ausland auf demokratische Prozesse (INGE und INGE2) beschloss das Europäische Parlament im Dezember 2024, einen Sonderausschuss für den Europäischen Schutzschild für die Demokratie (EUDS) einzusetzen, dessen Aufgabe darin besteht, zu prüfen, wie die Union ihre demokratischen Grundlagen besser verteidigen kann.

Die Gemeinsame Mitteilung über den Europäischen Schutzschild für die Demokratie, die von der Kommission und der HR/VP vorgelegt wurde, stellt einen wichtigen Beitrag zu diesen Bemühungen dar. Sie enthält einen strukturierten Überblick über die derzeitige Bedrohungslage und nennt mehrere Bereiche, in denen weitere Maßnahmen erforderlich sind, um die Union vor Informationsmanipulation und Einflussnahme aus dem Ausland sowie Desinformation zu schützen und die gesellschaftliche Resilienz zu stärken. Der Berichterstatter begrüßt diese Initiative und würdigt ihren Mehrwert, was die Konsolidierung des Verständnisses der Union für die anstehenden Herausforderungen anbelangt.

Allerdings bleiben die Zielvorgaben der Mitteilung, auch wenn sie die richtige Richtung vorgibt, hinter den Anforderungen zurück, die sich angesichts des Ausmaßes der Bedrohungen stellen. Erforderlich ist nicht nur ein Reflexionsrahmen, sondern auch eine konkrete Reformagenda, durch die operative Kapazitäten, Rechenschaftspflicht und langfristige Krisenvorsorge sichergestellt werden können.

Die Union hat ein wachsendes Ökosystem aus Strukturen, Instrumenten und Programmen zur Bekämpfung von Informationsmanipulation und Desinformation aus dem Ausland geschaffen. Es wurden dabei erhebliche Anstrengungen unternommen, einschließlich der Arbeit der einschlägigen Taskforces, Kooperationsnetze und Frühwarnmechanismen. Um diese Arbeit auf die nächste Stufe zu heben, müssen jedoch auch Reformen durchgeführt werden. Der Vorschlag zur Einrichtung eines Europäischen Zentrums für demokratische Resilienz ist eine willkommene und vielversprechende Initiative. Allerdings fehlt es der Initiative, so wie sie in der Mitteilung vorgestellt wurde, an der nötigen operativen Klarheit, ohne die eine solche Einrichtung nicht zu einer erfolgreichen Drehscheibe für Fachwissen und

Maßnahmen werden kann. Der Entwurf eines Berichts enthält konkrete Empfehlungen, wie dieses Ziel erreicht werden kann.

Der digitale Raum wird in vielerlei Hinsicht von böswilligen Akteuren aus Drittländern für die Durchführung ihrer Operationen ausgenutzt. Der Berichterstatter ist der Ansicht, dass die einschlägigen EU-Rechtsvorschriften beibehalten werden müssen und dass die Kommission ihre Durchsetzungsmaßnahmen verstärken muss, insbesondere wenn es Anzeichen für Manipulation im Zusammenhang mit Wahlen, systemische algorithmische Intransparenz, koordiniertes irreführendes Verhalten oder einen groß angelegten Missbrauch von Plattformfunktionen gibt.

Die sich wandelnde Bedrohungslage erfordert auch eine wirksamere Zusammenarbeit der Mitgliedstaaten auf Unionsebene bei der Durchführung von Wahlen. Die Integrität von Wahlprozessen stellt den Kern der demokratischen Resilienz dar. In diesem Zusammenhang wird in dem Entwurf eines Berichts betont, dass das Europäische Kooperationsnetz für Wahlen erheblich ausgebaut werden muss und dass eine umfassende Reform erforderlich ist, um dieses Netz anspruchsvoller und operativ relevanter zu gestalten. Darüber hinaus sollte wahlbezogene Infrastruktur als Teil der kritischen Infrastruktur der Union anerkannt und entsprechend geschützt werden.

Der Berichterstatter begrüßt auch, dass in der Gemeinsamen Mitteilung über den Europäischen Schutzschild für die Demokratie eine auswärtige Dimension vorgesehen ist. Die Ziele des Schutzschilds für die Demokratie können nicht ohne eine enge Zusammenarbeit mit Partnern in der Nachbarschaft der Union erreicht werden, insbesondere mit Bewerberländern, die zunehmend einer intensiven Einflussnahme aus dem Ausland ausgesetzt sind. Die Stärkung ihrer Resilienz – unter anderem durch Kapazitätsaufbau, Schulungen und die Bereitstellung von Fachwissen – ist für den Schutz des weiter gefassten demokratischen Raums Europas unerlässlich. In dem Entwurf eines Berichts wird der EAD aufgefordert, Maßnahmen zur Vorsorge gegen hybride Bedrohungen systematisch in die Mandate von GSVP-Missionen und -Operationen aufzunehmen und so die Fähigkeit der nationalen Partner zu stärken, böswillige Einflussnahme zu erkennen und zu bekämpfen. Im Rahmen der auswärtigen Dimension des Schutzschilds sollte auch eine Überprüfung der einschlägigen Sanktionsinstrumente vorgenommen werden, um sicherzustellen, dass sie optimal auf das Vorgehen gegen Akteure ausgerichtet sind, die die demokratische Integrität Europas gefährden. Die Abstimmung mit gleichgesinnten Partnern ist ebenfalls wichtig, um wirksame gemeinsame Reaktionen sicherzustellen. Der Berichterstatter begrüßt die Nutzung multilateraler und bilateraler Kooperationskanäle, einschließlich der bestehenden Sicherheits- und Verteidigungspartnerschaften der EU.

In dem Entwurf eines Berichts wird ferner betont, dass eine anspruchsvolle Agenda erforderlich ist, um die Gesellschaft resilienter zu machen. Einen wichtigen Bestandteil bilden dabei Reformen zur Unterstützung des Mediensektors zusammen mit Maßnahmen zur Stärkung der Medienkompetenz. Die Zivilgesellschaft und die EU-Strategie für die Zivilgesellschaft stellen einen weiteren wichtigen Aspekt dar: eine starke und unabhängige Zivilgesellschaft ist für die demokratische Resilienz unerlässlich. Der Berichterstatter spricht sich dafür aus, dass solide Programme zur Umsetzung der in der Initiative „Europäischer Schutzschild für die Demokratie“ festgelegten politischen Prioritäten im nächsten mehrjährigen Finanzrahmen für den Zeitraum 2028-2034 berücksichtig werden.

Für die Stärkung der gesellschaftlichen Resilienz ist auch ein verbesserter Schutz kritischer Infrastruktur von entscheidender Bedeutung, der im Hinblick auf die Ziele des Schutzschilds für die Demokratie neu bewertet werden sollte. Dies wiederum erfordert Reformen zur Stärkung der europäischen Souveränität über digitale Infrastruktur, Betriebssysteme, Rechenzentren, Halbleiter, KI, Cybersicherheit, Cloud-Computing und verschiedene digitale Plattformen und Dienste. Die Überarbeitung der Mandate der einschlägigen EU-Agenturen wie Europol und Frontex kann ebenfalls eine wichtige Rolle bei der Verbesserung der Resilienz und des Schutzes vor hybriden Bedrohungen spielen.

Schließlich wird in dem Entwurf eines Berichts betont, dass eine Voraussetzung für den Aufbau demokratischer Resilienz auch darin besteht, dass Gesellschaften auch unter außerordentlichen oder disruptiven Bedingungen weiterhin funktionieren können. Reformen zur Stärkung der Krisenvorsorge – von Krisenmanagementkapazitäten bis hin zur Kontinuität demokratischer Institutionen – müssen daher einen integralen Bestandteil des Europäischen Schutzschilds für die Demokratie bilden. Das Fazit des Entwurfs des Berichts lautet, dass der Schutz und die Stärkung der demokratischen Systeme Europas nicht nur Wachsamkeit und Resilienz auf allen Ebenen der Gesellschaft erfordern, sondern auch eine koordinierte und vorausschauende Strategie der Union, die mit ausreichenden Ressourcen und politischem Engagement einhergeht.

ANLAGE: ERKLÄRUNG ZU BEITRÄGEN

Gemäß Anlage I Artikel 8 der Geschäftsordnung erklärt der Berichterstatter, dass er in seinem Bericht Beiträge zu Angelegenheiten, die den Gegenstand des Dossiers betreffen, aufgenommen hat, die er bei der Vorbereitung des Entwurfs eines Berichts von den folgenden Interessenvertretern, die in den Anwendungsbereich der Interinstitutionellen Vereinbarung über ein verbindliches Transparenz-Register[1] fallen, oder den folgenden Vertretern der Behörden von Drittländern, einschließlich ihrer diplomatischen Vertretungen und Botschaften, erhalten hat:

1. Interessenvertreter, die in den Anwendungsbereich der Interinstitutionellen Vereinbarung über ein verbindliches Transparenz-Register fallen
European Partnership for Democracy
EU DisinfoLab
Schibsted ASA
European Confederation of Police
Reporters sans frontières
TikTok Technology Ltd
Europe MédiaLab
Psychological Defence Research Institute
Civil Society Europe (CSE)
European Fact-Checking Standards Network
Stiftung Mercator
The Foundation for European Progressive Studies (FEPS)
Konrad Adenauer Foundation
Association of Commercial Television in Europe (ACT)
European Association for Local Democracy (ALDA)
Martens Center
2. Vertreter der Behörden von Drittländern, einschließlich ihrer diplomatischen Vertretungen und Botschaften
k. A.

Für die vorstehende Liste ist ausschließlich der Berichterstatter verantwortlich.

Wenn natürliche Personen in der Liste namentlich, mit ihrer Funktion oder mit beidem genannt werden, erklärt der Berichterstatter, dass er den betroffenen natürlichen Personen die Erklärung zum Datenschutz Nr. 484 des Europäischen Parlaments (https://www.europarl.europa.eu/data-protect/index.do) vorgelegt hat, in der die Bedingungen für die Verarbeitung ihrer personenbezogenen Daten und die mit dieser Verarbeitung verbundenen Rechte dargelegt sind.

[1] Interinstitutionelle Vereinbarung vom 20. Mai 2021 zwischen dem Europäischen Parlament, dem Rat der Europäischen Union und der Europäischen Kommission über ein verbindliches Transparenz-Register (ABl. L 207 vom 11.6.2021, S. 1, ELI: http://data.europa.eu/eli/agree_interinstit/2021/611/oj).