



ANGENOMMENE TEXTE

P10_TA(2026)0286

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

Entschließung des Europäischen Parlaments vom 15. September 2026 zu den 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 Demokratie¹,
- unter Hinweis auf die gemeinsame Mitteilung 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),
- unter Hinweis auf den Vertrag über die Europäische Union (EUV), insbesondere auf Artikel 2 zu den Grundwerten der EU, Artikel 5 zu den Zuständigkeiten der EU, Artikel 10 zum demokratischen Leben und Artikel 21 zum auswärtigen Handeln,
- unter Hinweis 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 Vereinten Nationen,
- unter Hinweis auf die Bestimmungen über das Recht auf freie Meinungsäußerung in Artikel 19 der Allgemeinen Erklärung der Menschenrechte, Artikel 19 des Internationalen Pakts über bürgerliche und politische Rechte, Artikel 10 der Europäischen

¹ ABl. C, C/2025/1981, 11.4.2025, ELI:
<http://data.europa.eu/eli/C/2025/1981/oj>.

Menschenrechtskonvention (EMRK) und Artikel 11 der Charta der Grundrechte der Europäischen Union,

- 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 Stiftungen²,
- 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 Terrorismusfinanzierung⁴,
- 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 (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 (Richtlinie gegen SLAPP-Klagen),
- unter Hinweis auf die Verordnung (EU) 2024/900 des Europäischen Parlaments und des Rates vom 13. März 2024 über die Transparenz

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>.

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>.

und das Targeting politischer Werbung⁷ (Verordnung über die Transparenz und das Targeting politischer Werbung),

- 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 Union⁸ (Cybersicherheitsverordnung),
- 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) 2019/1937⁹ (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 Rates¹⁰ (Richtlinie über die Resilienz kritischer Einrichtungen),
- 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

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 31.5.2001, 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>.

Sektor und zur Änderung der Richtlinien (EU) 2019/1937 und (EU) 2020/1828 (Gesetz über digitale Märkte)¹³,

- unter Hinweis auf die Verordnung (EU) 2024/1252 des Europäischen Parlaments und des Rates vom 11. April 2024 zur Schaffung eines Rahmens zur Gewährleistung einer sicheren und nachhaltigen Versorgung mit kritischen Rohstoffen und zur Änderung der Verordnungen (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1724 und (EU) 2019/1020¹⁴ (europäische Verordnung zu kritischen Rohstoffen),
- unter Hinweis auf die gemeinsame Mitteilung der Kommission und der Hohen Vertreterin der Union für Außen- und Sicherheitspolitik vom 3. Dezember 2025 mit dem Titel „Stärkung der wirtschaftlichen Sicherheit der EU“ (JOIN(2025)0977),
- 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 Rates¹⁵,
- 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 melden¹⁶,
- 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)¹⁷,
- 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 Ukraine¹⁸ untergraben oder bedrohen, und auf die Verordnung (EU) Nr. 269/2014 des Rates vom 17. März 2014

¹³ ABl. L 265 vom 12.10.2022, S. 1, ELI:
<http://data.europa.eu/eli/reg/2022/1925/oj>.

¹⁴ ABl. L, 2024/1252, 3.5.2024, ELI:
<http://data.europa.eu/eli/reg/2024/1252/oj>.

¹⁵ ABl. L 156 vom 5.5.2021, S. 1, ELI:
<http://data.europa.eu/eli/reg/2021/692/oj>.

¹⁶ ABl. L 305 vom 26.11.2019, S. 17, ELI:
<http://data.europa.eu/eli/dir/2019/1937/oj>.

¹⁷ ABl. L 95 vom 15.4.2010, S. 1, ELI:
<http://data.europa.eu/eli/dir/2010/13/oj>.

¹⁸ ABl. L 78 vom 31.5.2001, S. 16, ELI:
[http://data.europa.eu/eli/dec/2014/145\(1\)/oj](http://data.europa.eu/eli/dec/2014/145(1)/oj).

über restriktive Maßnahmen angesichts von Handlungen, die die territoriale Unversehrtheit, Souveränität und Unabhängigkeit der Ukraine untergraben oder bedrohen¹⁹,

- 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 Ukraine²⁰ 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 Ukraine²¹,
- 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 Ukraine²² destabilisieren, 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 destabilisieren²³,
- 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 Gebiete²⁴ 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 kontrollierten Gebiete der ukrainischen Regionen Donezk und Luhansk und die Entsendung russischer Streitkräfte in diese Gebiete²⁵,
- unter Hinweis auf den Beschluss (GASP) 2024/2643 des Rates vom 8. Oktober 2024 über restriktive Maßnahmen angesichts der destabilisierenden Aktivitäten Russlands²⁶ und die Verordnung (EU) Nr. 2024/2642 des Rates vom 8. Oktober 2024 über restriktive

¹⁹ ABl. L 78 vom 17.3.2014, S. 6, ELI:
<http://data.europa.eu/eli/reg/2014/269/oj>.

²⁰ ABl. L 66 vom 31.5.2001, S. 26, ELI:
[http://data.europa.eu/eli/dec/2014/119\(1\)/oj](http://data.europa.eu/eli/dec/2014/119(1)/oj).

²¹ ABl. L 66 vom 6.3.2014, S. 1, ELI:
<http://data.europa.eu/eli/reg/2014/208/oj>.

²² ABl. L 229 vom 31.5.2001, S. 13, ELI:
<http://data.europa.eu/eli/dec/2014/512/oj>.

²³ ABl. L 229 vom 31.7.2014, S. 1, ELI:
<http://data.europa.eu/eli/reg/2014/833/oj>.

²⁴ ABl. L 42 I vom 23.2.2022, S. 109, ELI:
<http://data.europa.eu/eli/dec/2022/266/oj>.

²⁵ ABl. L 42 I vom 23.2.2022, S. 77, ELI:
<http://data.europa.eu/eli/reg/2022/263/oj>.

²⁶ ABl. L, 2024/2643, 9.10.2024, ELI:
<http://data.europa.eu/eli/dec/2024/2643/oj>.

Maßnahmen angesichts der destabilisierenden Aktivitäten Russlands²⁷,

- unter Hinweis auf den Beschluss 2012/642/GASP des Rates vom 15. Oktober 2012 über restriktive Maßnahmen gegen Belarus²⁸ und auf die Verordnung (EG) Nr. 765/2006 des Rates vom 18. Mai 2006 über restriktive Maßnahmen gegen Präsident Lukaschenka und verschiedene belarussische Amtsträger²⁹,
- 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 Ukraine³⁰ durch Iran 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 Iran³¹,
- 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 Korea³² 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 Korea³³,
- 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 den Vorschlag der Kommission vom 21. Januar 2026 für eine Verordnung des Europäischen Parlaments und des Rates über digitale Netze, zur Änderung der Verordnung (EU) 2015/2120, der Richtlinie 2002/58/EG und der Entscheidung Nr. 676/2002/EG sowie zur Aufhebung der Verordnung (EU) 2018/1971, der Richtlinie (EU) 2018/1972 und des Beschlusses Nr. 243/2012/EU (Verordnung über digitale Netze)

²⁷ ABl. L, 2024/2642, 9.10.2024, ELI:
<http://data.europa.eu/eli/reg/2024/2642/oj>.

²⁸ ABl. L 285 vom 17.10.2012, S. 1, ELI:
<http://data.europa.eu/eli/dec/2012/642/oj>.

²⁹ ABl. L 134 vom 20.5.2006, S. 1, ELI:
<http://data.europa.eu/eli/reg/2006/765/oj>.

³⁰ ABl. L 186 vom 9.6.2023, S. 20, ELI:
<http://data.europa.eu/eli/dec/2023/1532/oj>.

³¹ ABl. L 186 vom 25.7.2023, S. 1, ELI:
<http://data.europa.eu/eli/reg/2023/1529/oj>.

³² ABl. L, 2024/1603, 3.5.2024, ELI:
<http://data.europa.eu/eli/dec/2024/1603/oj>.

³³ ABl. L, 2024/1602, 31.5.2024, ELI:
http://data.europa.eu/eli/reg_impl/2024/1602/oj.

(COM(2026)0016),

- unter Hinweis auf den Vorschlag der Kommission vom 20. Januar 2026 für eine Verordnung des Europäischen Parlaments und des Rates über die Agentur der Europäischen Union für Cybersicherheit (ENISA), den europäischen Rahmen für die Cybersicherheitszertifizierung und die Sicherheit der IKT-Lieferketten sowie zur Aufhebung der Verordnung (EU) 2019/881 (Cybersicherheitsverordnung 2) (COM(2026)0011) (überarbeitete Cybersicherheitsverordnung),
- unter Hinweis auf den Vorschlag der Kommission vom 3. Juni 2026 für eine Verordnung des Europäischen Parlaments und des Rates über einen Rahmen für Maßnahmen zur Stärkung des Halbleiterökosystems der Union und zur Aufhebung der Verordnung (EU) 2023/1781 (Chip-Verordnung 2.0) (COM(2026)0504),
- unter Hinweis auf den Vorschlag der Kommission vom 3. Juni 2026 für eine Verordnung des Europäischen Parlaments und des Rates zur Schaffung eines Rahmens für Maßnahmen zur Stärkung des europäischen Cloud- und KI-Ökosystems (Verordnung über Cloud- und KI-Entwicklung) (COM(2026)0502),
- 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))³⁴,
- unter Hinweis auf seine früheren Entschlüsse zur Russischen Föderation und zu ihrem Angriff auf die Ukraine sowie zu ihren feindseligen Handlungen gegen die Mitgliedstaaten, einschließlich seiner 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 Russland³⁵,
- unter Hinweis auf seine Entschliessung vom 29. April 2026 zu dem Bericht der Kommission über die Rechtsstaatlichkeit 2025³⁶,
- unter Hinweis auf seine Entschliessung vom 7. Mai 2025 zu einem neu gestalteten langfristigen Haushalt für die Union in einer Welt im Wandel³⁷,

³⁴ Angenommene Texte, P10_TA(2025)0306.

³⁵ Angenommene Texte, P10_TA(2025)0230.

³⁶ Angenommene Texte, P10_TA(2026)0147.

³⁷ Angenommene Texte, P10_TA(2025)0090.

- unter Hinweis auf seine Entschlieung vom 23. Januar 2025 zu Desinformation und Geschichtsflschung seitens Russlands zur Rechtfertigung des Angriffskrieges gegen die Ukraine³⁸ und auf seine Entschlieung vom 22. Oktober 2025 zu dem Standpunkt des Rates zum Entwurf des Gesamthaushaltsplans der Europischen Union fr das Haushaltsjahr 2026³⁹, in der das Projekt des Baus einer Gedenksttte in Brssel erwhnt wird,
- unter Hinweis auf seine Entschlieung vom 13. Juli 2023 zu Empfehlungen fr die Reform der Vorschriften des Europischen Parlaments zu Transparenz, Integritt, Rechenschaftspflicht und Korruptionsbekmpfung⁴⁰,
- unter Hinweis auf seine Entschlieung vom 13. November 2025 zu Manahmen gegen die lnderbergreifende Unterdrckung von Menschenrechtsverteidigern⁴¹,
- unter Hinweis auf seine Entschlieung vom 21. Januar 2026 zu der Bekmpfung der Straflosigkeit mittels EU-Sanktionen, auch mittels der globalen Sanktionsregelung der EU im Bereich der Menschenrechte (sogenannte Magnitski-Verordnung der EU)⁴²,
- unter Hinweis auf seine Entschlieung vom 1. Juni 2023 zu Einflussnahme aus dem Ausland auf alle demokratischen Prozesse in der Europischen Union, einschlielich Desinformation⁴³,
- unter Hinweis auf seine Entschlieung vom 15. Dezember 2022 zum Korruptionsverdacht gegen Katar und zu der umfassenderen Notwendigkeit von Transparenz und Rechenschaftspflicht in den Organen der EU⁴⁴,
- unter Hinweis auf seine Entschlieung vom 23. November 2022 zur Einstufung der Russischen Fderation als dem Terrorismus Vorschub leistender Staat⁴⁵,

³⁸ ABl. C, C/2025/2147, 23.4.2025, ELI:
<http://data.europa.eu/eli/C/2025/2147/oj>.

³⁹ ABl. C, C/2026/2114, 29.4.2026, ELI:
<http://data.europa.eu/eli/C/2026/2114/oj>.

⁴⁰ ABl. C, C/2024/4011, 17.7.2024, ELI:
<http://data.europa.eu/eli/C/2024/4011/oj>.

⁴¹ ABl. C, C/2026/1664, 22.4.2026, ELI:
<http://data.europa.eu/eli/C/2026/1664/oj>.

⁴² Angenommene Texte, P10 TA(2026)0015.

⁴³ ABl. C, C/2023/1226, 21.12.2023, ELI:
<http://data.europa.eu/eli/C/2023/1226/oj>.

⁴⁴ ABl. C 177 vom 17.5.2023, S 109.

⁴⁵ ABl. C 167 vom 11.5.2023, S. 18.

- unter Hinweis auf seine Entschlieung vom 9. Mrz 2022 zu Einflussnahme aus dem Ausland auf alle demokratischen Prozesse in der Europischen Union, einschlielich Desinformation⁴⁶,
- unter Hinweis auf seine Entschlieung vom 8. Mrz 2022 zum schrumpfenden Handlungsspielraum fr die Zivilgesellschaft in der EU⁴⁷,
- unter Hinweis auf seine Entschlieung vom 20. Oktober 2021 zu Europas Medien in der digitalen Dekade: Ein Aktionsplan zur Untersttzung der Erholung und des Wandels⁴⁸,
- unter Hinweis auf seine Entschlieung vom 23. November 2016 zu dem Thema „Strategische Kommunikation der EU, um gegen sie gerichteter Propaganda von Dritten entgegenzuwirken“⁴⁹,
- unter Hinweis auf seine Empfehlung vom 15. Juni 2023 an den Rat und die Kommission nach der Prfung von behaupteten Versten gegen das Unionsrecht und Missstnden bei der Anwendung desselben im Zusammenhang mit dem Einsatz von Pegasus und hnlicher berwachungs- und Sphsoftware⁵⁰,
- unter Hinweis auf seine Empfehlung vom 23. November 2022 an den Rat, die Kommission und den Vizeprsidenten der Kommission und Hohen Vertreter der Union fr Auen- und Sicherheitspolitik zu der neuen Strategie der EU fr die Erweiterung⁵¹,
- unter Hinweis auf seine Empfehlung vom 13. Mrz 2019 an den Rat und die Vizeprsidentin der Kommission und Hohe Vertreterin der Union fr Auen- und Sicherheitspolitik zu der Bestandsaufnahme der Folgemanahmen, die zwei Jahre nach dem Bericht des Europischen Parlaments ber das Thema „Strategische Kommunikation der EU, um gegen sie gerichteter Propaganda von Dritten entgegenzuwirken“ durch den EAD ergriffen wurden⁵²,
- unter Hinweis auf die Folgemanahmen der Kommission zu den Empfehlungen des Parlaments in seinen Entschlieungen,
- unter Hinweis auf die Mitteilung der Kommission vom 12. November 2025 mit dem Titel „EU-Strategie fr die Zivilgesellschaft“ (COM(2025)0790),

⁴⁶ ABl. C 347 vom 9.9.2022, S. 61.

⁴⁷ ABl. C 347 vom 9.9.2022, S. 2.

⁴⁸ ABl. C 184 vom 5.5.2022, S. 71.

⁴⁹ ABl. C 224 vom 27.6.2018, S. 58.

⁵⁰ ABl. C, C/2024/494, 23.1.2024, ELI:
<http://data.europa.eu/eli/C/2024/494/oj>.

⁵¹ ABl. C 167 vom 27.1.2023, S. 105.

⁵² ABl. C 23 vom 21.1.2021, S. 152.

- unter Hinweis auf die Mitteilung der Kommission vom 3. Juni 2026 zur technologischen Souveränität und einer Open-Source-Strategie der EU (COM(2026)0503),
- unter Hinweis auf die Mitteilung der Kommission vom 3. Juni 2026 mit dem Titel „Strategischer Fahrplan für Digitalisierung und KI im Energiesektor“ (COM(2026)0501),
- 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 im November 2025 veröffentlichte nationale Sicherheitsstrategie der Vereinigten Staaten von Amerika und die im Januar 2026 veröffentlichte nationale Verteidigungsstrategie der USA,
- 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 die am 6. Februar 2026 bekannt gegebene vorläufige Feststellung der Kommission, wonach TikTok gegen das Gesetz über digitale Dienste verstößt, da die Risikobewertungen seines Empfehlungssystems und seine suchterzeugende Gestaltung bemängelt wurden,
- unter Hinweis auf den Verhaltenskodex zur Bekämpfung von Desinformation (2018 vorgelegt als Verhaltenskodex für den Bereich der Desinformation und 2022 gestärkt), der von der Kommission und dem Europäischen Gremium für digitale Dienste am 13. Februar 2025 als Verhaltenskodex gemäß Artikel 45 des Gesetzes über digitale Dienste gebilligt wurde und dessen Umwandlung am 1. Juli 2025 wirksam wurde,
- 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 Parlament⁵³,
- 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 Entscheidungsprozessen⁵⁴,

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

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

- 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 Infrastruktur⁵⁵,
- unter Hinweis auf den Beschluss (GASP) 2023/855 des Rates vom 24. April 2023 über eine Partnerschaftsmission der Europäischen Union in Moldau (EUPM Moldova)⁵⁶,
- 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,
- 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-Register⁵⁷,

⁵⁵ ABl. C 20 vom 20.1.2023, S. 1.

⁵⁶ ABl. L 110 vom 25.4.2023, S. 30, ELI:
<http://data.europa.eu/eli/dec/2023/855/oj>.

⁵⁷ ABl. L 207 vom 11.6.2021, S. 1, ELI:
http://data.europa.eu/eli/agree_interinstitut/2021/611/oj.

- 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 Demokratie“, die im Oktober 2025 von der Generaldirektion Bürgerrechte, Justiz und

institutionelle Angelegenheiten des Europäischen Parlaments veröffentlicht wurde⁵⁸,

- unter Hinweis auf die im Februar 2026 veröffentlichte Eurobarometer-Umfrage des Parlaments vom Herbst 2025, in der Bedenken der Öffentlichkeit hinsichtlich Sicherheitsrisiken skizziert wurden,
- unter Hinweis auf die im Mai 2025 veröffentlichte Eurobarometer-Sonderumfrage 568 der Kommission zum Thema Schutz und Förderung der Demokratie,
- unter Hinweis auf den ersten, den zweiten und den dritten Bericht des Europäischen Auswärtigen Dienstes (EAD) über Bedrohungen durch ausländische Informationsmanipulation und Einmischung,
- unter Hinweis auf den Bericht des Europarats von 2024 mit dem Titel „Press Freedom in Europe: Time to Turn the Tide – Annual assessment of press freedom in Europe by the partner organisations of the Safety of Journalists Platform“ (Pressefreiheit in Europa: Zeit für einen Wandel – Jährliche Bewertung der Pressefreiheit in Europa durch die Partnerorganisationen der Plattform zur Förderung des Schutzes journalistischer Tätigkeiten und der Sicherheit von Journalisten),
- 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 die Studie der Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung (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 in der EU – Neue Formen schwerer und organisierter Kriminalität) (Leitstudie EU-SOCTA), die 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),

⁵⁸ 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 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),
- unter Hinweis auf den gemeinsamen Ratgeber zu Cybersicherheit der US-amerikanischen Agentur für Cyber- und Infrastruktursicherheit, der Nationalen Sicherheitsagentur der Vereinigten Staaten (National Security Agency – NSA), der zentralen Sicherheitsbehörde der Vereinigten Staaten (Federal Bureau of Investigation – 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 ein weltumspannendes Spionagenetz aufzubauen),
- 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 am 1. November 2025 veröffentlichten Artikel des Zentrums für Medienpluralismus und -freiheit am Europäischen Hochschulinstitut mit dem Titel „Influencers as news creators:

implications for media regulation“ (Influencer als neue Urheber: Auswirkungen für die Regulierung der Medien),

- 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 Einrichtungen: 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 künstliche Intelligenz im Westen mit russischer Propaganda infiziert),
- unter Hinweis auf den Bericht von Media Freedom Rapid Response mit dem Titel „Mapping Media Freedom – Monitoring Report 2025“ (Medienfreiheit kartografieren – Monitoring-Bericht 2025), der im Februar 2026 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“ (Der 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 Pressemitteilung der Kommission vom 18. Dezember 2023 über die Einleitung eines förmlichen Verfahrens gemäß dem Gesetz über digitale Dienste gegen die Plattform X zur Bewertung möglicher Verstöße gegen ihre Verpflichtungen, insbesondere im Hinblick auf die Eindämmung systemischer Risiken im Zusammenhang mit der Gestaltung und Funktionsweise ihrer Empfehlungssysteme, sowie gegen ihre Verpflichtungen im Zusammenhang mit der Risikobewertung, der Moderation von Inhalten, der Transparenz der Werbung und dem Zugang von Forschenden zu Daten,
- unter Hinweis auf mehrere wissenschaftliche und investigative Studien zu Empfehlungssystemen in den sozialen Medien im Zusammenhang mit der Bundestagswahl in Deutschland, wonach es zu algorithmischer Voreingenommenheit und zur Verstärkung polarisierender oder parteiischer Inhalte kam, was das politische Informationsumfeld der Nutzer prägte,
- unter Hinweis auf die Pressemitteilung der Kommission vom 30. April 2024 über die Einleitung eines förmlichen Verfahrens gemäß dem Gesetz über digitale Dienste gegen Meta-Plattformen, insbesondere in Bezug auf den Umgang mit politischen Inhalten auf ihren Online-Plattformen,
- 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 Hochrisikoanbietern), worin vor den Risiken für die Energiesouveränität Europas aufgrund unregulierter und ferngesteuerter Funktionen von PV-Wechselrichtern von Hochrisikoanbietern aus Drittstaaten gewarnt wurde,
- unter Hinweis auf das am 19. März 2025 vorgestellte Weißbuch zur europäischen Verteidigung – Bereitschaft 2030 und die Verordnung

(EU) 2025/1106 des Rates vom 27. Mai 2025 zur Festlegung des Instruments „Sicherheitsmaßnahmen für Europa (SAFE) durch die Stärkung der europäischen Verteidigungsindustrie“⁵⁹,

- unter Hinweis auf die Schlussfolgerungen des Ratsvorsitzes vom 28. November 2025 zum Zugang zu zuverlässigen Nachrichten im Rahmen des Europäischen Schutzschilds für die Demokratie,
 - gestützt auf die Artikel 55 und 213 seiner Geschäftsordnung,
 - unter Hinweis auf den Bericht des Sonderausschusses für den Europäischen Schutzschild für die Demokratie (A10-0199/2026),
- 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; in der Erwägung, dass diese Initiative eine einzigartige Gelegenheit bietet, ein wirksames, gesamtgesellschaftliches Konzept für den Schutz der Demokratie, der Freiheit und des Wohlstands in Europa zu entwickeln; in der Erwägung, dass die demokratische Resilienz und die Sicherheit Europas zunehmend untrennbar miteinander verbunden sind;
- B. in der Erwägung, dass Armut, sozioökonomische Deprivation und Marginalisierung bestimmte Teile der Gesellschaft besonders verwundbar und anfällig für Einflussnahme von außen und feindselige Informationsmaßnahmen machen können;
- C. in der Erwägung, dass die von Russland ausgehende Bedrohung der Sicherheit und der demokratischen Integrität Europas weiterhin so hoch ist wie nie zuvor; in der Erwägung, dass auch durch andere Akteure wie China und Iran große Herausforderungen bestehen; in der Erwägung, dass der Grundsatz der Informationsabschreckung angewandt werden muss und erforderlichenfalls restriktive Maßnahmen gegen Akteure ergriffen werden müssen, die für ausländische Informationsmanipulation und Einmischung verantwortlich sind;
- D. in der Erwägung, dass die gemeinsame Mitteilung über den Europäischen Schutzschild für die Demokratie mehrere sinnvolle Empfehlungen und Vorschläge enthält, wie die Einrichtung eines Europäischen Zentrums für demokratische Resilienz, die Ausweitung des Geltungsbereichs des Schutzschilds auf Beitrittsländer und die Nachbarschaft der EU und die vollständige Durchsetzung wichtiger EU-Rechtsvorschriften; in der Erwägung, dass beide

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

Sonderausschüsse des Parlaments zu Einflussnahme aus dem Ausland auf alle demokratischen Prozesse in der Europäischen Union, einschließlich Desinformation (INGE und INGE 2), bereits gefordert hatten, dass eine EU-Einrichtung zur Bekämpfung von ausländischer Informationsmanipulation und Einmischung sowie von Desinformation geschaffen wird, die dem vorgeschlagenen Europäischen Zentrum für demokratische Resilienz entspricht; in der Erwägung, dass eine solche Einrichtung bestehende Instrumente, Fähigkeiten und Kompetenzen nicht ein zweites Mal bereitstellen, sondern in einer einzigen Stelle mit einer klaren Zielvorstellung, einem klaren Mandat, echten Befugnissen und einer Finanzausstattung konsolidieren sollte;

- E. in der Erwägung, dass aus den jüngsten Berichten des EAD über Angriffe im Wege ausländischer Informationsmanipulation und Einmischung hervorgeht, dass die Methoden böswilliger Akteure, die technische Infrastruktur und die angestrebten Narrative zunehmend besser verstanden werden, dass sich dieses Bewusstsein über die Lage jedoch noch nicht in nachhaltigen operativen Mechanismen niedergeschlagen hat, die es den Mitgliedstaaten und der EU ermöglichen, vorausschauend zu handeln, vorzubeugen, aufzudecken und rechtzeitig koordinierte Gegenmaßnahmen zu ergreifen; in der Erwägung, dass Wahlen auf nationaler und auf EU-Ebene vorrangiges Ziel feindseliger Kampagnen zur Informationsmanipulation und anderer Formen böswilliger Angriffe sind; in der Erwägung, dass mit diesen Kampagnen bestimmte Kandidaten oder politische Parteien verunglimpft werden, versucht wird, den Wahlprozess an sich zu diskreditieren, polarisierende Themen instrumentalisiert werden und der Versuch unternommen wird, traditionelle Medien zu diskreditieren; in der Erwägung, dass auch die Organe der EU und Behörden der Mitgliedstaaten massiv angegriffen werden; in der Erwägung, dass es in der EU kein gemeinsames Konzept zur Bekämpfung von ausländischer Informationsmanipulation und Einmischung sowie von Desinformation gibt, die Unterschiede zwischen den einzelnen Mitgliedstaaten im Hinblick auf ihre Kapazitäten beträchtlich sind und es keinen übergeordneten strategischen Rahmen oder funktionierenden transnationalen oder europäischen Kooperationsmechanismus gibt, durch den die operativen Reaktionen und die Informationen über Bedrohungen zueinander in Beziehung gesetzt werden;
- F. in der Erwägung, dass das Europäische Kooperationsnetz für Wahlen (ECNE), das Schnellwarnsystem und die Europäische Beobachtungsstelle für digitale Medien (EDMO) zwar wichtige Elemente der allgemeinen Resilienz der EU gegenüber ausländischer Informationsmanipulation und Einmischung sowie Desinformation sind, ihre Wirksamkeit 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, mit denen nationale operative Kapazitäten mit der Koordinierung auf EU-Ebene verknüpft werden könnten;

- G. 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 und den demokratischen Prozessen in ihren Mitgliedstaaten schadet; in der Erwägung, dass letztlich hauptsächlich die europäischen Bürgerinnen und Bürger unter diesen Praktiken leiden, da ihr Zugang zu verlässlichen Informationen und ihre Möglichkeiten, sich eine unabhängige Meinung zu bilden und konstruktiv am demokratischen Leben teilzuhaben, unmittelbar geschwächt werden, während gleichzeitig die öffentliche Sicherheit und die gesellschaftliche Stabilität gefährdet sind;
- H. in der Erwägung, dass einige Mitgliedstaaten, die in spezielle operative Strukturen mit klaren Statuten und Mandaten sowie ausreichender Finanz- und Personalausstattung investiert haben, aufzeigen, was machbar ist, wobei in diesem Zusammenhang insbesondere der französische Dienst VIGINUM und die schwedische Agentur für psychologische Verteidigung erwähnt werden können, die faktenbasiert, technisch und unparteiisch vorgehen; in der Erwägung, dass diese Einrichtungen zwar auf Anfrage oder aus eigener Initiative wertvolle Erkenntnisse beisteuern, jedoch nicht hinreichend miteinander vernetzt sind;
- I. 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 und traditionelle Lösungen wie Transparenz- oder Sorgfaltspflicht obsolet werden; in der Erwägung, dass ohne ein koordiniertes Vorgehen der EU und ohne klare operative Kapazitäten und Forschungsmöglichkeiten zunehmend die Angreifer und nicht die Verteidiger technologisch im Vorteil sein werden, wodurch der Kern unserer Demokratien bedroht ist; in der Erwägung, dass manche KI-Unternehmen die Sicherheitsmaßnahmen, mit denen sie der Verbreitung und Generierung von Desinformation über ihre Dienste entgegenwirken, nicht erhöht, sondern zurückgefahren haben; in der Erwägung, dass KI zwar Desinformationskampagnen erleichtert, aber auch Instrumente bietet, um solche Kampagnen besser aufzuspüren, zu analysieren und ihnen entgegenzuwirken;

- J. in der Erwägung, dass der Grundsatz, wonach Unternehmen einen finanziellen Beitrag zur Bewältigung externer Effekte, die mit ihren Tätigkeiten verbunden sind, leisten sollten, sowohl im Unionsrecht als auch in der Praxis fest verankert ist; in der Erwägung, dass gewisse Erzeuger im Rahmen der erweiterten Herstellerverantwortung die Entsorgung der Abfälle bezahlen müssen, die durch ihre Erzeugnisse entstehen, wobei hier das Verursacherprinzip unmittelbar zum Tragen kommt; in der Erwägung, dass alle in der Bankenunion tätigen Banken im Rahmen des einheitlichen Abwicklungsmechanismus jährlich Beiträge an den einheitlichen Abwicklungsfonds entrichten, sodass die systemischen Risiken im Zusammenhang mit ihren Aktivitäten nicht vom Steuerzahler getragen werden müssen; in der Erwägung, dass Pharmaunternehmen verpflichtet sind, Unbedenklichkeitsstudien nach der Zulassung zu finanzieren, da diejenigen, die Gewinne mit dem Inverkehrbringen eines Produkts erzielen, zur Überwachung der möglicherweise von dem Produkt verursachten Schäden beitragen müssen; in der Erwägung, dass diese Logik auf große Anbieter von Diensten der Informationsgesellschaft angewandt werden sollte, die Nutzen aus dem Informationsökosystem ziehen und gleichzeitig systemische Risiken für die demokratische Integrität schaffen;
- K. in der Erwägung, dass die EU mehrfach erfolgreich rechtlich umstrittene und neu aufkommende Politikfelder mithilfe strukturierter vorbereitender Instrumente bewältigt hat; in der Erwägung, dass hier beispielhaft insbesondere das Grünbuch über das Urheberrecht und die technologische Herausforderung aus dem Jahr 1988, die hochrangige Expertengruppe für künstliche Intelligenz und der Konsultationsprozess im Vorfeld des Erlasses der Datenschutz-Grundverordnung⁶⁰ zu nennen sind; in der Erwägung, dass ausländische Informationsmanipulation und Einmischung sowie Desinformation eine ähnliche Herausforderung im Zusammenhang mit Technologie, internationalen Beziehungen und Geschäftsmodellen darstellen, die sich im Zusammenspiel mit gesellschaftlichen und rechtlichen Phänomenen weiterentwickeln und gleichzeitig mit verfassungsrechtlichen Überlegungen konkurrieren; in der Erwägung, dass ein maßgeschneiderter, disziplinenübergreifender Vorbereitungsprozess unabdingbar für einen soliden und gerichtsfesten Rechtsrahmen für ausländische Informationsmanipulation und Einmischung sowie Desinformation sein könnte, wobei die Zuständigkeiten der Mitgliedstaaten und die Befugnisse der EU-Organen uneingeschränkt geachtet werden

⁶⁰ Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1, ELI: <http://data.europa.eu/eli/reg/2016/679/oj>).

müssen;

- L. 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 unauthentische Nutzung sozialer Medien über automatisierte Softwareprogramme, gefälschte Social-Media-Konten und den Einsatz von Trollfabriken, botbasierter Verstärkung und Steuerung, b) Astroturfing und Informationsüberflutung zur Beeinflussung der öffentlichen Debatte im Internet, c) Personalisierung, Tracking und Microtargeting von Einzelpersonen, d) Websites, die amtlichen Quellen nachempfunden sind, e) die künstliche Verstärkung und Monetarisierung spaltender Inhalte, f) die Verwendung synthetischer Inhalte wie Deepfakes und anderer KI-generierter Inhalte, g) Empfehlungssysteme, mit denen durch Polarisierung das Nutzerverhalten manipuliert werden soll, sowie h) das Grooming von Großen Sprachmodellen (LLM) und andere Techniken zur Verfälschung von Daten, bei denen voreingenommene, irreführende oder falsche Narrative böswillig in KI-Systeme eingespeist werden, um deren Training zu beeinflussen; in der Erwägung, dass zwar Instrumente zur Bekämpfung dieser Techniken und negativen Phänomene entwickelt wurden, diese jedoch weitgehend unzureichend sind;
- M. in der Erwägung, dass Online-Plattformen dadurch, dass sie Einblicke in die Präferenzen und Schwachstellen jedes einzelnen Nutzers haben, einen größeren Einfluss auf die öffentliche Debatte ausüben als traditionelle Medien; in der Erwägung, dass es Anzeichen dafür gibt, dass die Algorithmen von Plattformen von ihren Eigentümern und Anteilseignern manipuliert werden können, damit bestimmte politische Inhalte bevorzugt werden, wodurch das Informationsumfeld verzerrt wird und die Möglichkeiten der Nutzer, zutreffende und pluralistische Informationen zu erhalten, eingeschränkt werden; in der Erwägung, dass sehr große Online-Plattformen (VLOP) und sehr große Suchmaschinen (VLOSE) zu De-facto-Gatekeepern des öffentlichen Raums geworden sind und dadurch einen erheblichen Einfluss darauf ausüben, welche Informationen die Bürgerinnen und Bürger vorfinden, wie diese Informationen priorisiert sind und unter welchen Bedingungen sie verbreitet werden;
- N. in der Erwägung, dass die EU und ihre Mitgliedstaaten kürzlich eine Reihe umfassender Rechtsakte angenommen haben, um für Sicherheit und Transparenz im Internet zu sorgen, darunter das Gesetz über digitale Dienste, das Gesetz über digitale Märkte, die Verordnung über die Transparenz und das Targeting politischer Werbung, das Europäische Medienfreiheitsgesetz sowie die Verordnung über künstliche Intelligenz; in der Erwägung, dass diese

Rechtsakte zwar einen großen Fortschritt darstellen, wenn es gilt, Online-Plattformen zur Rechenschaft zu ziehen und demokratische Prozesse zu schützen, die Transparenz zu stärken, die Meinungsfreiheit zu wahren und so zu umfassenden Schutzmechanismen gegen ausländische Informationsmanipulation und Einmischung beizutragen, ihre Wirksamkeit jedoch davon abhängt, dass sie umfassend, rasch und kohärent durchgesetzt werden, wobei diese Durchsetzung derzeit herausfordernd ist und schleppend verläuft, sodass Schwachstellen entstehen; in der Erwägung, dass deshalb eine strukturierte Unterstützung für die Mitgliedstaaten diesbezüglich besonders wichtig ist; in der Erwägung, dass die EU und ihre Mitgliedstaaten außerdem weitere nichtlegislative Maßnahmen, gemeinsame Konzepte und Methoden konzipieren sollten, um ausländische Informationsmanipulation und Einmischung zu verhindern und die Demokratie zu schützen; in der Erwägung, dass das Parlament eine wichtige Rolle spielt, wenn es darum geht, die Digitalvorschriften der EU zu überwachen und zu stärken, und dass diese Bemühungen im Interesse ihrer Wirksamkeit durch regelmäßige Prüfungen der Arbeitsmethoden des Parlaments ergänzt werden sollten;

- O. in der Erwägung, dass es Belege dafür gibt, dass die auf dem Nutzerverhalten beruhenden Empfehlungssysteme sehr großer Online-Plattformen, darunter X, TikTok und Instagram, strukturell von der Aufmerksamkeitsökonomie bestimmt werden, sodass spaltende, polarisierende oder irreführende Inhalte verstärkt werden, was wiederum Risiken für den gesellschaftlichen Diskurs und die Integrität von Wahlen birgt, wie bei Wahlen in der ganzen EU beobachtet werden konnte, als extremistische politische Inhalte verstärkt wurden; in der Erwägung, dass diese Systeme die Sichtbarkeit redaktionell unabhängiger und pluralistischer Medien schwächen und der raschen Verbreitung von AI-generierten Deepfakes und künstlichen oder manipulierten Inhalten Vorschub leisten und es somit den Nutzern und insbesondere benachteiligten Gruppen immer schwerer machen, zwischen wahren und falschen Informationen zu unterscheiden; in der Erwägung, dass mit der Verordnung über künstliche Intelligenz eine obligatorische Kennzeichnung AI-generierter Inhalte eingeführt wurde; in der Erwägung, dass sehr große Online-Plattformen gemäß den Artikeln 34 und 35 des Gesetzes über digitale Dienste verpflichtet sind, systemische Risiken zu bewerten und zu mindern; in der Erwägung, dass mit dem Gesetz über digitale Dienste außerdem wichtige neue Vorschriften mit Blick auf eine stärkere Transparenz und Rechenschaftspflicht hinsichtlich der Algorithmen eingeführt wurden, wozu unter anderem die Möglichkeit für die Nutzer gehört, sich für nicht personalisierte Feeds zu entscheiden, sodass die Abhängigkeit von einer intransparenten algorithmischen Kuratierung sinkt; in der Erwägung, dass es nach wie vor Herausforderungen im Zusammenhang mit der Umsetzung und dem Nutzererlebnis gibt; in der Erwägung, dass eine wirksame Durchsetzung des Gesetzes über

digitale Dienste und der Verordnung über künstliche Intelligenz, die mit aktuellen Leitlinien und einer unabhängigen Überwachung einhergeht, unerlässlich ist, um Manipulation zu bekämpfen und demokratische Prozesse zu schützen;

- P. in der Erwägung, dass die US-Regierung gezielte Sanktionen, Zollandrohungen, Visumsperren und persönliche Sanktionen gegen EU-Akteure, die an der Ausarbeitung und der Durchsetzung des Gesetzes über digitale Dienste und anderer Digitalvorschriften beteiligt sind, gerichtet hat und somit der Integrität der Beschlussfassung in der EU und der Rechtsstaatlichkeit schadet; in der Erwägung, dass die EU als offener und auf Regeln beruhender Binnenmarkt ihr souveränes Recht aufrechterhalten muss, im Einklang mit demokratischen Werten, internationalen Verpflichtungen und dem Schutz der Grundrechte einschließlich der Meinungsfreiheit – bei der es sich um einen grundlegenden Wert handelt, der auch von den Vereinigten Staaten und anderen gleich gesinnten Partnern in der gesamten demokratischen Welt geteilt wird – legislativ tätig zu werden; in der Erwägung, dass unbegründete Zensurvorfälle diese gemeinsamen Werte untergraben und von tatsächlichen schwerwiegenden Verstößen gegen die Meinungsfreiheit in Ländern wie Russland, China oder Iran ablenken; in der Erwägung, dass die Durchsetzung der Digitalvorschriften der EU insbesondere dann, wenn große Technologie-Plattformen Lobbyarbeit betreiben, keinen Verzögerungen oder Einschränkungen aufgrund geopolitischer Erwägungen unterliegen darf; in der Erwägung, dass Druck von außen – etwa geoökonomische Zwangsmaßnahmen, strategische Übernahmen und die Unterstützung extremistischer Bewegungen durch öffentliche oder private Akteure aus Drittstaaten – die Souveränität der Beschlussfassung und die demokratische Resilienz der EU zusätzlich bedroht; in der Erwägung, dass sich die Durchsetzung der Digitalvorschriften der EU auch künftig ausschließlich am Unionsrecht und am Schutz demokratischer Interessen orientieren muss und keinerlei ungebührlichem Einfluss aufgrund von politischem, handelspolitischem oder externem Druck unterliegen darf; in der Erwägung, dass in diesem Zusammenhang die Einigkeit der EU-Mitgliedstaaten und ihre politische Abstimmung unabdingbar sind;
- Q. in der Erwägung, dass KI Innovation, den Zugang zu Wissen, Produktivität und neue Digitalbranchen vorantreibt und somit neue Möglichkeiten eröffnet, wie zum Beispiel eine bessere Wahlleitung und -beaufsichtigung, indem ungewöhnliche Online-Aktivitäten und koordiniertes manipulatives Verhalten aufgespürt werden; in der Erwägung, dass der Einsatz von KI, einschließlich generativer Modelle und Deepfakes, außerdem mit beträchtlichen Herausforderungen für die Informationsintegrität und Wahlprozesse einhergeht, sodass es rasch wirksamer Schutzmaßnahmen für die Demokratie und einer Regulierungsaufsicht bedarf; in der Erwägung,

dass in seriösen Berichten die Tätigkeiten eines in Moskau ansässigen Desinformationsnetzwerks namens „Pravda“ aufgedeckt wurden, das LLM gezielt mit kremlfreundlichen Narrativen infiltriert, die neutralen und faktenbasierten Meldungen nachempfunden sind; 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 verbindlich wirkenden Sprache unmerklich falsche oder irreführende geopolitische Botschaften zu verbreiten, und der demokratische Diskurs und das Vertrauen in Digitaltechnologien unterhöhlt werden; in der Erwägung, dass diese Form der algorithmischen Manipulation das Vertrauen der Öffentlichkeit in KI-Technologien zu untergraben, den demokratischen Diskurs zu verzerren und die Gefahr von Desinformation in der gesamten EU und weltweit zu verschärfen droht; in der Erwägung, dass daran ersichtlich wird, dass es besserer KI-Kompetenzen in der Bildung, im Berufsleben und in der Gesellschaft generell, mehr Transparenz beim Training von LLM und einer angemessenen Forschungsfinanzierung bedarf; in der Erwägung, dass von KI hervorgebrachte Ergebnisse Verzerrungen widerspiegeln können, die bei der Konzeption der Systeme eingebaut wurden;

- R. in der Erwägung, dass Online-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, faktenbasierte Inhalte zu fördern oder zu einer echten politischen Debatte beizutragen; in der Erwägung, dass sich gleichzeitig immer mehr Bürgerinnen und Bürger, insbesondere Minderjährige und junge Erwachsene, im Übermaß auf Ersteller von Inhalten und Influencer auf den sozialen Medien, Gaming-Dienste und Dienste zum Teilen von Videos und Inhalten verlassen, und zwar auch für Nachrichten und Aktuelles, sodass sie sich selbst Gefahren aufgrund von suchterzeugender Gestaltung, schädlichen Inhalten und manipulativen Praktiken aussetzen; in der Erwägung, dass Persönlichkeiten und Influencer im Internet in erheblichem Maße in der Lage sein können, die öffentliche Meinung und den Informationsfluss zu beeinflussen, ohne dass sie Rechenschaftsstandards unterliegen, die mit denen vergleichbar sind, die für Medien gelten;
- S. 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 und zur Verzerrung des Wahlkampfs hinweisen; in der Erwägung, dass TikTok – eine der von jungen Wählerinnen und 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; in der Erwägung, dass es Hinweise auf zwei wesentliche operative Muster gibt, nämlich die koordinierte Manipulation von Empfehlungsalgorithmen durch Netze synchronisierter Konten, die künstlichen Traffic und Trendverstärkung erzeugen, und die verdeckte Instrumentalisierung von Erstellern von Inhalten, wobei beide Muster zeigen, wie die technische Dynamik der Plattformen instrumentalisiert werden und demokratische Sicherheitsvorkehrungen umgehen kann;

- T. in der Erwägung, dass Telegram – ein Messaging-Dienst mit immer mehr Nutzern in der EU – verstärkt als Kanal für Desinformation, Einflussnahme aus dem Ausland und illegale Aktivitäten, einschließlich der Verbreitung extremistischer Inhalte, der Anwerbung für Sabotage, politische Propaganda und Desinformation im Zusammenhang mit den Rechtsvorschriften der EU und der Mitgliedstaaten, angeführt wird; in der Erwägung, dass die Ursprünge von Telegram in Russland, die undurchsichtigen Eigentumsverhältnisse und das Fehlen einer bedeutenden Moderation von Inhalten anhaltende Bedenken hinsichtlich seiner Rolle bei der Unterhöhlung des demokratischen Diskurses hervorgerufen haben; 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 jungen Menschen, ausnutzen, um Spionage- und Sabotageaktionen 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; in der Erwägung, dass die Kommission in ihrer langwierigen Bewertung noch nicht zu einer Schlussfolgerung gelangt ist;
- U. in der Erwägung, dass der zunehmende Einfluss von Technologieunternehmen aus Drittstaaten – insbesondere Unternehmen mit Sitz in den Vereinigten Staaten und China – die strategischen Abhängigkeiten der EU in kritischen Bereichen wie Dateninfrastruktur, Satellitenkommunikation, Cloud-Diensten,

Online-Plattformen, Bezahldiensten und IT-Software etwa in Bereichen wie der Verteidigung deutlich gemacht hat; in der Erwägung, dass die Förderung heimischer Innovationen, die Gewährleistung fairer und wettbewerbsorientierter digitaler Märkte, die Durchsetzung des digitalen Regelwerks, die Förderung europäischer Start-ups und Investitionen in die souveräne digitale Infrastruktur wichtige Schritte sind, wenn es gilt, ein wettbewerbsfähiges, sicheres, robustes und unabhängiges digitales Ökosystem der EU aufzubauen und gleichzeitig die Möglichkeiten der feindlichen Einmischung, der Informationsmanipulation und wirtschaftlicher Zwangsmaßnahmen einzuschränken; 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; in der Erwägung, dass KI die Globalisierung umgestaltet und beschleunigt, indem sie eine neue Phase des strategischen Wettbewerbs einläutet; in der Erwägung, dass die digitale Souveränität der EU besonders schwer zu erreichen ist, wenn sehr große Online-Plattformen und sehr große Online-Suchmaschinen de facto als Oligopole agieren;

- V. 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 und der Mitgliedstaaten trotz regulatorischer Maßnahmen weiterhin zu destabilisieren; in der Erwägung, dass die Tatsache, dass Online-Werbung intransparent ist, dazu führt, dass große Geldbeträge von rechtmäßigen Marken auf Desinformationsseiten weitergeleitet werden können, polarisierende Inhalte finanziert werden können und Qualitätsjournalismus beeinträchtigt werden kann; in der Erwägung, dass Meta das einzige große Technologieunternehmen ist, das eingeschränkt Monetarisierungsdaten veröffentlicht, während andere große Technologieunternehmen nach wie vor gänzlich intransparent sind;
- W. in der Erwägung, dass in einer Umfrage, die im Vorfeld der Parlamentswahl 2025 in den Niederlanden durchgeführt wurde, jeder zehnte Befragte angab, dass er wahrscheinlich KI um Rat für die Wahlentscheidung bitten werde, während weitere 13 % angaben, dass sie vielleicht auf KI zurückgreifen würden; in der Erwägung, dass mehr als ein Drittel der jüngsten Befragten in den Niederlanden

angab, KI wahrscheinlich oder vielleicht für Hilfe bei der Wahlentscheidung zu nutzen; 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; in der Erwägung, dass Investitionen in die Entwicklung quelloffener LLM eine Möglichkeit bieten, Bedenken im Hinblick auf versteckte Voreingenommenheit, Hintertüren oder Datenmissbrauch in KI-Chatbots auszuräumen;

- X. 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 zunichtezumachen sowie die Nachrichten echter Personen mit unauthentischen Inhalten zu fluten;
- Y. in der Erwägung, dass das Grundrecht auf die Freiheit der Meinungsäußerung und die Informationsfreiheit, das in Artikel 19 der Allgemeinen Erklärung der Menschenrechte sowie 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;
- Z. in der Erwägung, dass die Freiheit der Meinungsäußerung und die Informationsfreiheit Grundrechte sind, deren Ziel es ist, Menschen zu schützen und nicht etwa Maschinen, Algorithmen, Bots oder KI;
- AA. in der Erwägung, dass autoritäre Regime Plattformen der sozialen Medien nutzen, um die Meinungsfreiheit zu unterdrücken; in der Erwägung, dass die Nutzer Transparenz, ein ordnungsgemäßes Verfahren und den Schutz der Meinungsfreiheit erwarten, die gemäß den Anforderungen des Gesetzes über digitale Dienste aufrechterhalten werden müssen; in der Erwägung, dass deshalb die Digitalvorschriften der EU umfassend durchgesetzt werden müssen,

damit diese Grundsätze gewahrt werden;

- AB. in der Erwägung, dass die Freiheit der Meinungsäußerung und die Informationsfreiheit sowie die Freiheit und der Pluralismus der Medien, die in Artikel 11 Absatz 2 der Charta der Grundrechte der Europäischen Union und in Artikel 10 der Europäischen Menschenrechtskonvention verankert sind, Eckpfeiler demokratischer und resilienter Gesellschaften sind; in der Erwägung, dass redaktionell unabhängiger, hochwertiger, faktenbasierter, gut finanzierter und gewerblich tragfähiger Journalismus – auch von Journalisten im Exil – ein wichtiger Schutz vor ausländischer Informationsmanipulation und Einmischung sowie vor Desinformation und ein grundlegendes Instrument für die sachkundige Entscheidungsfindung ist;
- AC. in der Erwägung, dass der Begriff „Informationsintegrität“ zwar regelmäßig von den EU-Organen in politischen und Arbeitsdokumenten verwendet wird, es jedoch keine offizielle oder gemeinsam vereinbarte Bestimmung dieses Begriffs auf EU-Ebene gibt; in der Erwägung, dass diese fehlende Begriffsbestimmung dazu führen kann, dass der Begriff möglicherweise uneindeutig ausgelegt und angewendet wird;
- AD. in der Erwägung, dass das EMFA ein Meilenstein ist, wenn es darum geht, eine unabhängige und pluralistische Medienlandschaft in Europa zu fördern; in der Erwägung, dass die Medien eine demokratische Funktion erfüllen, die sich von der Funktion gewöhnlicher gewerblicher Unternehmen unterscheidet; in der Erwägung, dass solide Schutzvorkehrungen erforderlich sind, um die redaktionelle Unabhängigkeit zu schützen, was insbesondere in Fällen von Eigentumskonzentration, Übernahmen oder Änderungen in Bezug auf die Kontrolle gilt, und um Transparenz, Rechenschaftspflicht mit Blick auf die Quellen und Berufsstandards zu gewährleisten; in der Erwägung, dass sich die Kommission darum bemühen sollte, die Bewerberländer besser in die Medienpolitik der EU einzubeziehen; in der Erwägung, dass sich hierzu auch die Bewerberländer selbst entsprechend bemühen sollten;
- AE. in der Erwägung, dass das Ökosystem der Digitalwerbung zwar neue Möglichkeiten für die Reichweite von Medien eröffnet, jedoch auch zu Marktkonzentration und unlauterem Wettbewerb führt, da wenige große Online-Plattformen einen unverhältnismäßig hohen Anteil der Werbeeinnahmen auf sich vereinen; in der Erwägung, dass Medienorganisationen, die in Nachrichteninhalte und audiovisuelle Produktion investieren, einem Bericht der französischen Regulierungsbehörde für audiovisuelle und digitale Kommunikation (Arcom) und des französischen Kulturministeriums aus dem Jahr 2023 zufolge 2022 lediglich 40 % der Werbeeinnahmen erhalten haben, wobei dieser Wert 2012 noch 65 % betrug und bis 2030 voraussichtlich auf 29 % sinken wird; in der Erwägung, dass dies

häufig zulasten professioneller europäischer Medienunternehmen und der Nachhaltigkeit des unabhängigen Journalismus erfolgt;

- AF. in der Erwägung, dass missbräuchliche Praktiken beherrschender Akteure auf dem Online-Werbemarkt – wie etwa die Praktiken, die dazu geführt haben, dass die Kommission aufgrund von Verstößen gegen Wettbewerbsregeln im Online-Werbegeschäft eine Geldstrafe in Höhe von 2,95 Mrd. EUR gegen Google verhängt hat – deutlich machen, dass es zusätzlicher struktureller Maßnahmen bedarf, mit denen für einen fairen Wettbewerb, mehr Transparenz, Rechenschaftspflicht und Schutzmechanismen gesorgt wird, um den Medienpluralismus, die redaktionelle Unabhängigkeit und die Integrität demokratischer Prozesse zu schützen; in der Erwägung, dass strukturelle Schwachstellen im Online-Werbemarkt von böswilligen Akteuren ausgenutzt werden können, was anhand der sogenannten Doppelgänger-Kampagne, bei der Werbung auf sozialen Medien dazu genutzt wurde, um Nutzer gezielt zu beeinflussen, und der russischen Online-Kampagnen, mit denen ukrainische Männer von einer Meldung für das Militär abgehalten werden sollen, deutlich wird;
- AG. in der Erwägung, dass das Gesetz über digitale Märkte wesentlich ist, wenn es darum geht, für faire digitale Märkte und Medienpluralismus zu sorgen; in der Erwägung, dass es bei seiner Umsetzung noch Herausforderungen gibt; in der Erwägung, dass App-Entwickler im Rahmen des Gesetzes über digitale Märkte Kunden unentgeltlich über Angebote außerhalb von App-Stores informieren können; in der Erwägung, dass die Kommission derzeit einen potenziellen Verstoß gegen das Gesetz über digitale Märkte durch Google in Form der Herabstufung der Inhalte von Medienverlagen untersucht; in der Erwägung, dass die Kommission am 3. Juli 2025 ihre erste Überprüfung des Gesetzes über digitale Märkte eingeleitet hat;
- AH. in der Erwägung, dass mit der Richtlinie über audiovisuelle Mediendienste audiovisuelle Mediendienste reguliert werden, wodurch der Verbraucherschutz auf dem Markt für audiovisuelle Medien gewährleistet und weiteren Zielen von öffentlichem Interesse auf diesem Markt Rechnung getragen wird; in der Erwägung, dass die Mitgliedstaaten gemäß der Richtlinie über audiovisuelle Mediendienste verpflichtet sind, Maßnahmen zur Entwicklung von Medienkompetenzen zu ergreifen und alle drei Jahre über ihre Bemühungen Bericht zu erstatten; in der Erwägung, dass die Kommission derzeit die Richtlinie bewertet und im November 2025 eine Aufforderung zur Einreichung von Beiträgen veröffentlicht hat, um die für 2026 geplante erneute Bewertung vorzubereiten;
- AI. in der Erwägung, dass Kindern Kompetenzen vermittelt werden müssen, damit sie gegen Desinformation gefeit sind; in der

Erwägung, dass feindselige Akteure in diesem Zusammenhang möglicherweise verstärkt Bildungssysteme ins Visier nehmen, um den Bemühungen um die Verbesserung der Digitalkompetenzen entgegenzuwirken; in der Erwägung, dass bestimmte Gruppen aus unterschiedlichen Gründen besonders anfällig für Falschinformationen sind, was unter anderem für Kinder und Jugendliche gilt, die digitale Plattformen verstärkt nutzen; in der Erwägung, dass Medienkompetenz und kritisches Denken von frühester Kindheit an gefördert werden müssen;

- AJ. in der Erwägung, dass die Europäische Beobachtungsstelle für digitale Medien (EDMO) eine wichtige Rolle bei der Überwachung und Bekämpfung von Desinformation spielt; in der Erwägung, dass das Mandat der EDMO ausgeweitet wurde, damit sie ihre wichtige Arbeit fortsetzen kann; in der Erwägung, dass die Ausweitung ihres Mandats nicht mit einer entsprechenden Erhöhung ihrer finanziellen Mittel einhergeht, was die Möglichkeiten der EDMO, ihre Ziele zu verwirklichen, möglicherweise einschränkt;
- AK. in der Erwägung, dass die Tatsache, dass das Programm für Medienresilienz befristet ist, eine Chance dafür bieten könnte, neue innovative Konzepte für die Unterstützung unabhängiger lokaler und regionaler Medien zu prüfen;
- AL. in der Erwägung, dass der Krisenreaktionsmechanismus für Verstöße gegen die Presse- und Medienfreiheit 2025 1 481 Verstöße gegen die Pressefreiheit dokumentiert hat, von denen 2 377 mit Medien verbundene Personen oder Einrichtungen in 36 europäischen Ländern betroffen waren, wobei die Verstöße rechtliche, physische und psychische Drohungen sowie verschiedene Formen der Zensur beinhalteten; in der Erwägung, dass diese Zahl zwar einen leichten Rückgang gegenüber 2024 (1 548 verzeichnete Verstöße) darstellt, jedoch nach wie vor alarmierend hoch und eine deutliche Steigerung gegenüber 2023 ist, wodurch deutlich wird, dass die Medienfreiheit in Europa anhaltend und systemisch bedroht ist; in der Erwägung, dass die Morde an Investigativjournalisten wie Ján Kuciak, Giorgos Karaivaz, Peter R. de Vries und Daphne Caruana Galizia große Empörung in der Öffentlichkeit ausgelöst haben;
- AM. 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;
- AN. 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 im Anschluss an die Reform der Auslandshilfepolitik der Vereinigten Staaten Soforthilfe in Höhe von 5,5 Mio. EUR für seine Arbeit bewilligt hat; in der Erwägung, dass eine dauerhafte Finanzierungslösung für RFE/RL und andere

unabhängige Medien konzipiert werden muss, zumal sie unabdingbar sind, wenn es gilt, die demokratische Resilienz in Nachbarländern zu stärken;

- AO. in der Erwägung, dass neue Technologien wie KI die Arbeitsbedingungen und -methoden von Journalisten zwar verbessern können, sie aber auch neuen Bedrohungen aussetzen können, beispielsweise schnellen und billigen Nachbildungen bestehender Medien (Doppelgänger-Kampagnen), der massenhaften Schaffung von Desinformationskanälen und koordinierten Angriffen auf Journalisten; in der Erwägung, dass jede Nachahmung bestehender Medien auf Identitätsdiebstahl hinausläuft und von den Justizbehörden angemessen bekämpft werden sollte; in der Erwägung, dass KI-Modelle mit dem Urheberrecht der Union im Einklang stehen müssen, damit der Schutz der Rechteinhaber und die Rechtssicherheit gewährleistet sind; in der Erwägung, dass die Nachrichtenmedienbranche mit Herausforderungen aufgrund des zunehmenden Einflusses von KI-Systemen konfrontiert ist, da dieser Einfluss das Vertrauen der Öffentlichkeit, die Werbeeinnahmen und den Urheberrechtsschutz beeinträchtigt; in der Erwägung, dass die Entwicklungen im Bereich der generativen KI im Zusammenhang mit der bevorstehenden Überprüfung der Urheberrechtsrichtlinie⁶¹ der EU durch die Kommission erörtert werden sollten und ergänzend ein Bericht über die wichtigsten Erkenntnisse ausgearbeitet werden sollte; in der Erwägung, dass es im Zusammenhang mit der Medienpolitik mehr Transparenz bei den Daten, mit denen KI trainiert wird, bedarf;
- AP. in der Erwägung, dass sich der Umbau der US-amerikanischen Entwicklungshilfebehörde USAID auf etliche europäische Medien auswirkt; in der Erwägung, dass dies deutlich macht, dass die europäische Medienlandschaft gestärkt werden muss; in der Erwägung, dass die EU ihre Gelder verstärkt Initiativen gewähren sollte, die die größte öffentliche Wirkung erzielen, und dass die Finanzierung grundlegende operative Unterstützung umfassen sollte;
- AQ. in der Erwägung, dass die von der letzten, von der Fidesz-Partei geführten ungarischen Regierung ergriffenen Maßnahmen die Kommission veranlasst haben, ein Vertragsverletzungsverfahren gegen Ungarn zu eröffnen, weil es das EMFA und die Richtlinie über audiovisuelle Medien nicht eingehalten hatte;
- AR. in der Erwägung, dass der andauernde Angriffskrieg Russlands gegen die Ukraine verdeutlicht, dass die Zivilgesellschaft eine

⁶¹ Richtlinie (EU) 2019/790 des Europäischen Parlaments und des Rates vom 17. April 2019 über das Urheberrecht und die verwandten Schutzrechte im digitalen Binnenmarkt und zur Änderung der Richtlinien 96/9/EG und 2001/29/EG (ABl. L 130 vom 17.5.2019, S. 92, ELI: <http://data.europa.eu/eli/dir/2019/790/oj>).

entscheidende Funktion übernimmt, wenn Gemeinschaften in Krisensituationen geraten, was insbesondere dann der Fall ist, wenn es darum geht, humanitäre Hilfe zu leisten, die Grundbedürfnisse zu decken, die Weiterführung des Alltags der betroffenen Bevölkerungsgruppen sicherzustellen und auf die Androhungen von Sabotage und Spionage zu reagieren;

- AS. in der Erwägung, dass die Zivilgesellschaft außerdem eine wesentliche Rolle spielt, wenn es darum geht, zur Politikgestaltung beizutragen, Dienste für die Gesellschaft und für die Gemeinschaft zu erbringen, das Bewusstsein für wichtige soziale Fragen zu schärfen, die Resilienz zu stärken, verschiedene Gruppen in prekärer Lage zu vertreten und die Grundrechte der Bürgerinnen und Bürger zu fördern und zu schützen sowie durch öffentliche und demokratische Kontrolle dafür zu sorgen, dass Regierungen stets transparent agieren und Rechenschaft ablegen;
- AT. 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 bekräftigt wird, dass die Plattform der Zivilgesellschaft, 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;
- AU. in die Erwägung, dass die Mittel für die demokratische Resilienz aufgestockt und koordiniert und wirksam verwendet werden sollten, damit die größtmögliche Wirkung erzielt wird, wobei gleichzeitig die Unabhängigkeit der betreffenden Einrichtungen geachtet werden muss; 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 ein wichtiger Schritt hin zur Stärkung der EU-Unterstützung für Kultur, Medien und Zivilgesellschaft ist;
- AV. in der Erwägung, dass die Gesellschaften, in denen effektiv in das Humankapital und die Bildung investiert wird, zu den wettbewerbsfähigsten, widerstandsfähigsten und wirtschaftlich solidesten gehören; in der Erwägung, dass Programme wie Erasmus+ die europäischen Werte fördern und das demokratische

Engagement der Jugend sowie die gesellschaftliche Resilienz in der gesamten EU stärken;

- AW. in der Erwägung, dass böswillige Akteure aus Drittstaaten danach streben, das Parlament zu behindern und es in unbotmäßiger Weise zu beeinflussen, indem sie etwa auf illegale Lobbyarbeit und Korruption zurückgreifen, was anhand von Fällen wie dem sogenannten Katargate offenkundig wird; in der Erwägung, dass diese Entwicklungen deutlich machen, dass die Resilienz und die Integrität der Beschlussfassungsverfahren in der EU weiter gestärkt werden müssen;
- AX. in der Erwägung, dass das französische Innenministerium einen Bericht über die Muslimbruderschaft veröffentlicht hat, in dem es Bedenken mit Blick auf verdeckte Einflussnahme und Entrismus geäußert hat; in der Erwägung, dass ähnliche Bedenken auch hinsichtlich anderer religiöser Akteure wie der Russisch-Orthodoxen Kirche (Moskauer Patriarchat) geäußert wurden;
- AY. in der Erwägung, dass hybride Angriffe auf kritische Infrastruktur in der EU immer häufiger vorkommen, wobei die Vorfälle von denselben böswilligen Drittstaatsakteuren wie Russland, Belarus und China, aber auch von Iran und Nordkorea ausgehen; in der Erwägung, dass die EU in einem zunehmend unbeständigen geopolitischen Umfeld auch auf hybride Bedrohungen vorbereitet sein muss, die von anderen als diesen Akteuren ausgehen; in der Erwägung, dass diese Angriffe häufig gegen essenzielle Systeme, Netzwerke und Einrichtungen gerichtet sind, die für das Funktionieren einer Gesellschaft – unter anderem für die öffentliche Sicherheit und die wirtschaftliche Stabilität – von entscheidender Bedeutung sind; 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; in der Erwägung, dass derartige Angriffe zeigen, dass Schwachstellen dringend beseitigt werden müssen;
- AZ. in der Erwägung, dass Angriffe auf die Eisenbahninfrastruktur das Leben und die Sicherheit von Bürgerinnen und Bürgern gefährden und strategische Logistiknetzwerke bedrohen, was anhand des beispiellosen Sabotageakts gegen die polnische Eisenbahninfrastruktur auf der strategisch wichtigen Strecke Warschau-Lublin deutlich wurde, mit dem ein katastrophaler Unfall ausgelöst werden sollte und der zahlreiche Todesopfer hätte fordern können; in der Erwägung, dass der russische Militärgeheimdienst (GRU) eine fortwährende Kampagne mit physischen Sabotageakten in allen EU-Mitgliedstaaten führt, wobei hier auch die Explosion eines Munitionsdepots in Vrbětice (Tschechien) im Jahr 2014 und die

gezielten Angriffe kubanischer Staatsangehöriger, die vor Kurzem für Sabotageoperationen angeworben worden waren, auf kritische Infrastruktur in Litauen zu nennen sind;

- BA. 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 elf Kabelschäden verzeichnet wurden, was auf koordinierte Sabotage hindeutet; in der Erwägung, dass im Vorschlag für eine Verordnung über digitale Netze verbindliche Resilienzverpflichtungen auf EU-Ebene für Betreiber von Unterseekabeln enthalten sind, einschließlich der verbindlichen Einhaltung von Sicherheitsanforderungen in den Lieferketten für Informations- und Kommunikationstechnologie (IKT) im Rahmen des Vorschlags für die Überarbeitung des Rechtsakts zur Cybersicherheit; in der Erwägung, dass Finnland gemeinsam mit Verbündeten im baltischen Raum und der Kommission die Einrichtung eines neuen Zentrums für die Seeüberwachung in der Ostsee leitet, das darauf ausgerichtet ist, kritische Unterseeinfrastruktur zu schützen; in der Erwägung, dass die Präsenz russischer Schiffe in irischen Gewässern seit Beginn der groß angelegten Invasion in der Ukraine durch Russland im Jahr 2022 deutlich zugenommen hat, was Bedenken hinsichtlich der Sicherheit der wichtigen Verbindungskabel zwischen Irland und dem Vereinigten Königreich aufwirft;
- BB. in der Erwägung, dass der Schutz wichtiger Meerengen zur demokratischen Resilienz beiträgt, da hybride Angriffe auf solche Knotenpunkte zu schwerwiegenden wirtschaftlichen, sozialen und sicherheitspolitischen Störungen führen können; in der Erwägung, dass chinesische Unternehmen mit engen Verbindungen zur Kommunistischen Partei Chinas derzeit Anteile an mehr als 30 europäischen Seehafenterminals halten, von denen sich viele in unmittelbarer Nähe zu europäischen Marinestützpunkten befinden; in der Erwägung, dass sich die Kommission und die Vizepräsidentin der Kommission und Hohe Vertreterin der Union für Außen- und Sicherheitspolitik im gemeinsamen Weißbuch zur europäischen Verteidigung – Bereitschaft 2030 verpflichtet haben, die bestehenden EU-Rechtsvorschriften zu überprüfen und strengere Vorschriften über Eigentum und Kontrolle kritischer Verkehrsinfrastruktur einzuführen;
- BC. in der Erwägung, dass in den letzten Monaten mehrere Verletzungen des Luftraums und ein unbefugtes Eindringen von Drohnen über mehreren EU-Mitgliedstaaten und benachbarten NATO-Verbündeten gemeldet wurden, unter anderem über Polen, den baltischen Staaten, Rumänien, Dänemark, Schweden, Deutschland, Belgien und Norwegen; 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, darunter „Schmuggelballone“ für illegale grenzüberschreitende Tätigkeiten, nach wie vor untersucht werden, jedoch weithin der starke Verdacht besteht, dass sie Teil desselben Musters hybrider Einschüchterung und Destabilisierung sind, das sich gegen Europa richtet;

- BD. in der Erwägung, dass mehrere europäische Länder, darunter Frankreich, Estland, Deutschland, Polen, Tschechien und Norwegen, zuletzt mit schweren Cyberangriffen und Sabotageakten konfrontiert waren, die gegen Regierungssysteme, kritische Infrastruktur und private Unternehmen gerichtet waren und feindlich gesinnten Drittländern, einschließlich der militärischen Nachrichtendienste Russlands und mit dem chinesischen Staat verbundenen Akteuren, zugeschrieben werden; in der Erwägung, dass diese Angriffe deutlich machen, dass die kollektive Cyberresilienz und die Fähigkeiten der EU zur Zuordnung von Cyberangriffen dringend gestärkt werden müssen;
- BE. 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 und die strategische Autonomie Europas darstellt;
- BF. in der Erwägung, dass die EU nach wie vor stark von Technologie und Finanzdiensten aus den USA abhängig ist, wodurch europäische Daten und digitale Infrastruktur Risiken ausgesetzt sind, die sich aus US-amerikanischen Rechtsvorschriften wie dem CLOUD Act, dem Foreign Intelligence Surveillance Act und dem Patriot Act ergeben, die den US-amerikanischen Behörden umfangreichen Zugang zu Daten gewähren, über die US-amerikanische Unternehmen verfügen, auch wenn diese Daten in der EU gespeichert sind; in der Erwägung, dass die Kommission im Juli 2023 den Datenschutzrahmen EU-USA angenommen hat, der den freien Verkehr personenbezogener Daten zwischen der EU und den Vereinigten Staaten mit angemessenen Schutzvorschriften ermöglicht und einen Mechanismus vorsieht, mit dem EU-Bürger Zugang zu einem unabhängigen und unparteiischen Beschwerdemechanismus im Zusammenhang mit der Erhebung und Nutzung ihrer Daten durch US-Nachrichtendienste haben; in der Erwägung, dass Microsoft selbst gegenüber dem französischen Senat eingeräumt hat, dass es in der EU befindliche Daten nicht vor einer Überwachung durch die Vereinigten Staaten schützen kann;
- BG. in der Erwägung, dass Spanien Huawei damit beauftragt hat, gerichtlich genehmigte Abhöraktionen für Strafverfolgungsbehörden und Nachrichtendienste zu verwalten und zu speichern; in der Erwägung, dass die Kommission Huawei aufgrund von

Sicherheitsbedenken aus 5G-Netzen in der gesamten EU ausgeschlossen hat;

- BH. in der Erwägung, dass alle US-amerikanischen Bundesbehörden den Anforderungen des Konzepts „Buy American“ unterliegen, wonach dem Kauf von in den Vereinigten Staaten hergestellten Produkten Vorrang eingeräumt wird; in der Erwägung, dass der EU-Rahmen für die Vergabe öffentlicher Aufträge anders aufgebaut ist und in manchen Fällen zu Abhängigkeiten von Produkten aus Drittländern und den damit verbundenen Risiken für europäische Unternehmen beitragen kann; in der Erwägung, dass das Europäische Parlament und andere EU-Organe trotz der Tatsache, dass in vielen Fällen angemessene europäische Alternativen zur Verfügung stehen, weiterhin außerhalb von Europa entwickelte bzw. hergestellte Software- und Hardwareprodukte erwerben;
- BI. in der Erwägung, dass die Kommission am 20. Januar 2026 einen Vorschlag zur Überarbeitung des Rechtsakts zur Cybersicherheit vorgelegt hat, in dem verbindliche Sicherheitsanforderungen in Bezug auf IKT-Lieferketten im Bereich der kritischen Infrastruktur vorgeschlagen werden, wobei systematische Risikobewertungen und Beschränkungen für risikoreiche Anbieter aus Ländern mit erhöhten Sicherheitsrisiken vorgesehen sind; in der Erwägung, dass dieser neue Rahmen über das freiwillige Instrumentarium für die 5G-Cybersicherheit von 2020 hinausgeht, indem vorgeschlagen wird, den Mitgliedstaaten verbindliche Verpflichtungen zur Einhaltung der Vorgaben aufzuerlegen; in der Erwägung, dass das operative Mandat und der Haushalt der ENISA durch den Vorschlag zur Überarbeitung des Rechtsakts zur Cybersicherheit erheblich ausgeweitet bzw. aufgestockt werden könnten, nämlich um mehr als 80 %, sodass auch die Koordinierung im Zusammenhang mit Cybervorfällen in Echtzeit, Frühwarnsysteme und der Austausch von Erkenntnissen über Bedrohungen zwischen den Mitgliedstaaten erfasst würden;
- BJ. in der Erwägung, dass mit dem von der Kommission am 21. Januar 2026 vorgeschlagenen Rechtsakt über digitale Netze eine Aufsicht auf EU-Ebene über die Frequenzzuweisung, auch in Bezug auf Anbieter von Satellitendiensten, eingeführt wird, wobei vorgeschrieben wird, dass Anbietern, die die Anforderungen des Vorschlags zur Überarbeitung des Rechtsakts zur Cybersicherheit an die Sicherheit der IKT-Lieferkette nicht erfüllen, das Recht zur Bereitstellung von Netzen und Diensten entzogen wird; in der Erwägung, dass neben anderer kritischer Infrastruktur die Wahlinfrastruktur zunehmend von digitalen Netzen und vielfältigen Kommunikationswegen abhängt, damit einzelne Schwachstellen vermieden werden;
- BK. in der Erwägung, dass fossilfreie Energiequellen einen entscheidenden Eckpfeiler für die Energiesouveränität Europas darstellen; in der Erwägung, dass laut der Analyse von Wood

Mackenzie aus dem Jahr 2025 neun der zehn weltweit größten Anbieter von Solarwechselrichtern ihren Sitz in China hatten; in der Erwägung, dass in Solarwechselrichtern, die in China hergestellt und in Europa und den Vereinigten Staaten verwendet werden, versteckte Kommunikationsgeräte entdeckt wurden; in der Erwägung, dass nach Angaben des tschechischen Amts für Cybersicherheit Solarwechselrichter mit Datenschutzrisiken und in Extremfällen mit dem Risiko der Fernmanipulation behaftet sind; in der Erwägung, dass Solarkraftwerke, die über ein dichtes dezentrales Netz miteinander verbunden sind, anfälliger für Cyberangriffe sind und daher angemessene Cybersicherheitsschutzmaßnahmen erfordern;

BL. in der Erwägung, dass hybride Angriffe eine anerkannte Sicherheitsbedrohung für die EU und ihre Mitgliedstaaten darstellen und sich erheblich auf die Demokratie auswirken; in der Erwägung, dass die innere Sicherheit nach wie vor in die Zuständigkeit der Mitgliedstaaten fällt, dass der grenzüberschreitende, vernetzte und mehrdimensionale Charakter dieser Angriffe jedoch eine verstärkte Zusammenarbeit, einen systematischen Informationsaustausch und koordinierte Maßnahmen auf EU-Ebene erfordert, die durch eine angemessene Finanzierung unterstützt werden; in der Erwägung, dass in der Europäischen Strategie für die innere Sicherheit vom April 2025 betont wird, dass das Strafrecht der EU bereits bestimmte Formen von ausländischer Informationsmanipulation und Einmischung und Desinformationstätigkeiten abdeckt und dass eine verstärkte Zusammenarbeit der EU dazu beitragen kann, dieser Art von Verhalten wirksamer entgegenzuwirken; in der Erwägung, dass strafrechtliche Instrumente zum Europäischen Schutzschild für die Demokratie beitragen können, soweit die betreffenden Tätigkeiten im Einklang mit dem geltenden Recht Straftaten darstellen;

BM. 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; in der Erwägung, dass zunehmend neue Strategien, die von terroristischen und kriminellen Organisationen entwickelt wurden, zur Einflussnahme aus dem Ausland sowie zu deren Finanzierung genutzt werden, einschließlich der Nutzung von Kryptowerten und der Kommunikation über verschiedene digitale Kanäle, einschließlich Videospiele oder Online-Shops, um Sanktionen zu umgehen und illegal Geld zu transferieren; in der Erwägung, dass die Strafjustiz und die Strafverfolgungsbehörden daher angemessen im Hinblick auf moderne Ermittlungsmethoden und -technologien sowie die gesamte Wertschöpfungskette der Manipulation und Einflussnahme geschult werden müssen, damit sie Beweismittel in Strafverfahren ordnungsgemäß erheben, verarbeiten, verwahren und verwenden

können; in der Erwägung, dass Übermittlungen personenbezogener Daten an Drittländer oder internationale Organisationen, die für die Zwecke der polizeilichen Zusammenarbeit, der Zusammenarbeit in Strafsachen oder der Zusammenarbeit beim Grenzmanagement erforderlich sind, besonderen Bedingungen nach dem Unionsrecht unterliegen und nur erfolgen sollten, wenn die Integrität und Sicherheit dieser Daten gewährleistet werden kann;

BN. in der Erwägung, dass Europol in seinem 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 Angriffen, unter anderem Desinformationskampagnen, 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 in seinem Mandat in Bezug auf neue Sicherheitsbedrohungen, insbesondere Sabotage, hybride Bedrohungen und Informationsmanipulation; in der Erwägung, dass in der gemeinsamen Mitteilung über den Europäischen Schutzschild für die Demokratie angekündigt wurde, dass bei der Überarbeitung der Mandate sowohl von Europol als auch der Agentur der Europäischen Union für justizielle Zusammenarbeit in Strafsachen (Eurojust) Möglichkeiten ausgelotet würden, wie die Bemühungen zur Bekämpfung von ausländischer Informationsmanipulation und Einmischung und Desinformationsaktivitäten weiter verstärkt werden können;

BO. 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 Strafverfolgungsbeamte ausgeprägtes Wissen um die destabilisierenden Auswirkungen haben, die ausländische Informationsmanipulation und Einmischung und Desinformationskampagnen auf die betroffenen Gemeinschaften haben können; in der Erwägung, dass sie daher wichtige Partner für den Schutz demokratischer Einrichtungen sein können; in der Erwägung, dass der rechtliche, berufliche und ethische Rahmen, der für die Wahrnehmung dieser Rolle erforderlich ist, besser definiert und in der gesamten EU weiter harmonisiert werden sollte;

BP. in der Erwägung, dass 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;

BQ. in der Erwägung, dass die Lage an den Außengrenzen der

Mitgliedstaaten zu Russland und Belarus aufgrund anhaltender hybrider Bedrohungen nach wie vor Anlass zur Sorge gibt; in der Erwägung, dass den EU-Agenturen im Bereich Justiz und Inneres in Zusammenarbeit mit den nationalen Behörden eine Schlüsselrolle bei der Schaffung und Aufrechterhaltung eines gemeinsamen Lagebewusstseins für die mit solchen Bedrohungen verbundenen Risiken und bei der Unterstützung der Mitgliedstaaten an den Außengrenzen in Krisensituationen zukommt; in der Erwägung, dass die Kommission die Stärkung der Europäischen Agentur für die Grenz- und Küstenwache (Frontex) in ihre Leitinitiativen für die Wahlperiode 2024-2029 aufgenommen hat; in der Erwägung, dass weitere Initiativen wie der sogenannte Schutzschild für die Ostflanke dazu beitragen können, den Schutz der Außengrenzen zu stärken und die Resilienz gegenüber hybriden Bedrohungen zu erhöhen;

- BR. in der Erwägung, dass die transnationale Unterdrückung die systematische Einschüchterung und Schikanierung von Journalisten und Aktivisten, Menschenrechtsverteidigern, politischen Gegnern und Mitgliedern der in der EU ansässigen Diasporagemeinschaften durch drittstaatliche Behörden oder ihre Stellvertreter umfasst, wie im Fall der rechtlichen Schikanen ukrainischer Journalisten durch Russland, der türkischen und aserbaidzhanischen Versuche, die Opposition zum Schweigen zu bringen, und der geplanten Angriffe auf die belarussische Diaspora in Litauen; in der Erwägung, dass die zunehmende Überwachung von Menschenrechtsverteidigern als eine Form der transnationalen Unterdrückung betrachtet werden sollte; in der Erwägung, dass solche Praktiken nicht nur die Sicherheit und die Grundrechte der Betroffenen verletzen, sondern auch die Souveränität und Sicherheit der EU und der Mitgliedstaaten, die demokratischen Freiheiten und die Rechtsstaatlichkeit beeinträchtigen; in der Erwägung, dass Opfer transnationaler Unterdrückung in der EU weiterhin Schutz erhalten sollten;
- BS. in der Erwägung, dass die Bewerberländer und die Nachbarländer der EU, insbesondere die Ukraine, Moldau, Armenien, Georgien und der Westbalkanländer, nach wie vor stark von ausländischer Informationsmanipulation und Einmischung sowie hybriden Bedrohungen betroffen sind; in der Erwägung, dass insbesondere die Republik Moldau mit anhaltenden, koordinierten und staatlich initiierten Desinformationskampagnen konfrontiert ist, mit denen demokratische Einrichtungen, die Integrität von Wahlen und ihr Weg zum EU-Beitritt untergraben werden sollen; in der Erwägung, dass diese Länder Unterstützung durch die EU benötigen, um zivilgesellschaftliche und institutionelle Resilienz aufzubauen und ausländische Informationsmanipulation und Einmischung und hybride Bedrohungen zu bekämpfen, unter anderem im Rahmen der Mechanismen zur finanziellen Unterstützung der Ukraine-Fazilität, der Reform- und Wachstumsfazilität für den Westbalkan und der Reform- und Wachstumsfazilität für Moldau; in der Erwägung, dass die EU die Rückmeldungen und Erfahrungen dieser Länder

berücksichtigen sollte, da sie seit vielen Jahren mit hybriden Angriffen aus Russland konfrontiert sind; in der Erwägung, dass die Wirksamkeit der Bemühungen der EU zur Stärkung der institutionellen Resilienz in den Bewerberländern von ihrer Bereitschaft abhängt, einschlägige Maßnahmen zu ergreifen, notwendige Reformen umzusetzen und wirksam zusammenzuarbeiten;

- BT. in der Erwägung, dass der Angriffskrieg Russlands gegen die Ukraine und Chinas bestimmende 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 jährliche Budget Russlands für die Verbreitung von Desinformation und Propaganda auf mehrere Milliarden Euro beläuft; in der Erwägung, dass die EU der Desinformationskriegsführung Russlands nicht mit einer angemessenen Finanzierung oder wirksamen Strategie begegnet; 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 europäische 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;
- BU. in der Erwägung, dass bereits im Hinblick auf drei Kandidaten für die Präsidentschaftswahl in Frankreich im Jahr 2027 Vorgänge im Zusammenhang mit Informationsmanipulation festgestellt wurden, die Russland zugeschrieben wurden;
- BV. in der Erwägung, dass der Angriffskrieg Russlands gegen die Ukraine sowie seine umfassendere hybride Kriegsführung gegen Europa und die Einmischung in die demokratischen Prozesse anderer Länder durch die nationalistische imperialistische Ideologie des „Raschismus“ ermöglicht und gerechtfertigt wurden und Teil einer umfassenderen Strategie sind, die sich gegen den Westen und seine Interessen und Werte richtet, einschließlich der regelbasierten internationalen Ordnung, der Rechtsstaatlichkeit, der Demokratie, der Menschenrechte und der gemeinsamen Sicherheit; in der Erwägung, dass das Parlament die Ideologie, die Politik und die Praktiken des derzeitigen Regimes Russlands als unvereinbar mit dem Völkerrecht und den Werten der EU verurteilt hat;
- BW. in der Erwägung, dass sich Russland einer vielschichtigen Kampagne zur hybriden Einflussnahme bedient hat, um die Wahlen in der Republik Moldau 2024 und 2025 zu stören, bei der Desinformation,

Finanzmanipulation, Cyberangriffe und Proxy-Netzwerke kombiniert wurden; in der Erwägung, dass Russland massiv in diese Versuche investiert hat, die dank der Wirksamkeit der Verteidigungspolitik Moldaus und der Unterstützung durch die EU gescheitert sind; in der Erwägung, dass die Partnerschaftsmission der EU in der Republik Moldau (EUPM) am 24. April 2023 mit dem ausdrücklichen Ziel eingerichtet wurde, die moldauischen Behörden bei der Bekämpfung von ausländischer Informationsmanipulation und Einmischung zu unterstützen;

- BX. in der Erwägung, dass am 7. Juni 2026 Parlamentswahlen in Armenien abgehalten wurden, und zwar nach einer Phase verstärkter Einmischung Russlands, wobei unter anderem bestimmte religiöse Akteure und die internationale Diaspora instrumentalisiert wurden, um die demokratischen Institutionen Armeniens zu untergraben, die Friedensgespräche mit Aserbaidschan zum Scheitern zu bringen und den Einfluss Russlands zu bekräftigen; in der Erwägung, dass dem Jahresbericht 2026 Armeniens über externe Sicherheitsrisiken zufolge ausländische Akteure ihre Agenten in Armenien aktivieren;
- BY. in der Erwägung, dass Serbien zu einem zentralen Knotenpunkt für Desinformation und zu einem Verbündeten in puncto Einflussnahme aus Russland und – in geringerem Maße – aus China geworden ist; in der Erwägung, dass nach Urteilen moldauischer Gerichte Serbien und die Republika Srpska in Bosnien und Herzegowina 2024 ein militantes Ausbildungslager in Verbindung mit Russland ausrichteten, in dem Unruhestifter rekrutiert und geschult wurden, um während der Wahl und des Referendums in Moldau für massive Störungen zu sorgen; in der Erwägung, dass die Cyberinfrastruktur Serbiens genutzt wurde, um ausgefeilte Spear-Phishing-Angriffe zu starten, und zwar zur Imitation der Sicherheitskonferenz in Belgrad und gegen Beamte und Diplomaten der EU und der NATO; in der Erwägung, dass Serbien zu einem sicheren Zufluchtsort für Spione und Oligarchen aus Russland geworden ist, die Oppositionelle Russlands überwachen und Wege finden, sich den Sanktionen zu entziehen; in der Erwägung, dass serbische Bürgerinnen und Bürger mit mutmaßlichen Verbindungen zu Russland verhaftet wurden, weil sie in Frankreich und Deutschland mutmaßlich hassmotivierte Handlungen begangen haben, darunter die Verwüstung jüdischer Stätten, um ethnische und religiöse Zwietracht zu säen;
- BZ. in der Erwägung, dass die besorgniserregende Abnahme der Unterstützung der USA für die internationale Demokratie durch den Rückzug aus wichtigen multilateralen und internationalen Rahmen zu einer erheblichen globalen Finanzierungslücke, unter anderem bei der Bekämpfung von Desinformation und autoritärem Einfluss, geführt hat;
- CA. in der Erwägung, dass die nationale Sicherheitsstrategie und die

ationale Verteidigungsstrategie der USA einen Wandel in der langjährigen US-Außenpolitik widerspiegeln, der unter anderem durch den ausdrücklichen Fokus auf die US-Interessen in der westlichen Hemisphäre und das Herunterspielen der von Russland und China ausgehenden Bedrohung gekennzeichnet ist; in der Erwägung, dass die nationale Sicherheitsstrategie auch kritische Verweise auf mutmaßliche demokratische Mängel in einigen EU-Mitgliedstaaten enthält und darin Maßnahmen ankündigt werden, die Einflussnahme aus dem Ausland gleichkommen; in der Erwägung, dass die nationale Strategie globale Entwicklungen weitgehend im Hinblick auf wirtschaftlichen Nationalismus und strategische Interessen abbildet, einen stärker transaktionalen Ansatz gegenüber traditionellen Verbündeten offenbart und somit die Grundsätze infrage stellt, die seit Jahrzehnten die Grundlage der US-Außenpolitik bilden;

- CB. in der Erwägung, dass China im Vergleich zu anderen Akteuren ausgefeiltere Methoden anwendet, um Einfluss in der EU zu gewinnen, unter anderem durch die Kooptierung politischer Eliten, das Ködern ehemaliger Amtsträger mit lukrativen Arbeitsstellen und den Aufbau eines umfassenden Netzes von Studierenden, Forschenden und Wirtschaftsakteuren, die Narrative und politische Maßnahmen zugunsten Chinas vorantreiben sollen; in der Erwägung, dass solche Methoden auch koordinierte Informationsmanipulation und Desinformationsaktivitäten in Drittstaaten umfassen, und zwar hat China den Berichten einer parteiübergreifenden US-amerikanischen Kommission zufolge eine Desinformationskampagne durchgeführt, um französische Rafale-Kampfflugzeuge zu diskreditieren, die von Indien im Konflikt zwischen Indien und Pakistan 2025 gegen chinesische Waffen eingesetzt wurden;
- CC. in der Erwägung, dass im Rahmen internationaler Initiativen, einschließlich der Initiativen der Vereinten Nationen, der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung, des Europarats, gleichgesinnter Länder in Ostasien wie Japan, Südkorea und Taiwan und der G7, allmählich Grundsätze und Rahmenbedingungen für den Schutz der Integrität von Informationen festgelegt werden, die in demokratischen Werten, Medienpluralismus und Menschenrechten verankert sind;
- CD. in der Erwägung, dass Kampagnen zur ausländischen Informationsmanipulation und Einmischung auch von Akteuren in der EU ausgehen können, einschließlich der Mitgliedstaaten; in der Erwägung, dass die Glaubwürdigkeit demokratischer Einrichtungen auch davon abhängt, dass die jeweiligen Regierungen von der Verbreitung unrichtiger, irreführender oder politisch instrumentalisierter Informationen absehen, insbesondere im Fall von Naturkatastrophen, gesundheitlichen Notlagen und humanitären Krisen; in der Erwägung, dass die Glaubwürdigkeit der EU und die Unabhängigkeit ihres Entscheidungsprozesses beeinträchtigt

werden können, wenn ehemalige hochrangige Beamte von EU-Mitgliedstaaten oder EU-Organen bezahlte Positionen oder Beratungsfunktionen annehmen oder wenn es zu anderen Formen der Zusammenarbeit mit autoritären Regimen in Drittstaaten oder deren staatlich kontrollierten Unternehmen kommt;

- CE. in der Erwägung, dass das Phänomen der Informationsmanipulation und Einmischung im innerstaatlichen Kontext sowie dessen Auswirkungen weiter untersucht und verstanden werden sollten insbesondere im Zusammenhang mit ausländischer Informationsmanipulation und Einmischung; in der Erwägung, dass die vorgestellten Maßnahmen zur Bekämpfung von 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, der digitalen Kompetenz und der KI-Kompetenz in allen Altersgruppen; in der Erwägung, dass die wirksame Unterbindung und Bekämpfung von Informationsmanipulation einen sektorübergreifenden Ansatz in der gesamten Gesellschaft erfordert;
- CF. 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;
- CG. in der Erwägung, dass ausländische Informationsmanipulation und Einmischung im Zusammenhang mit Wahlen häufig wiederkehrenden Mustern folgt, darunter Bemühungen, Kandidaten oder politische Akteure zu diskreditieren, das Vertrauen in Wahlprozesse zu untergraben und gesellschaftliche Spaltungen auszunutzen; in der Erwägung, dass bei den Bemühungen um die Sicherstellung der Integrität von Wahlen ein umfassender Ansatz verfolgt werden muss;
- CH. 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 weiter auszubauen;
- CI. 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 ECNE weiter zu verbessern, voneinander zu lernen, wenn sie Bedrohungen ausgesetzt sind, und sich über bewährte Verfahren zur

Bekämpfung dieser Bedrohungen auszutauschen;

- CJ. in der Erwägung, dass es eindeutig notwendig ist, den Schutz der Wahlinfrastruktur und der nationalen politischen Parteien, die ebenfalls Ziel von Cyberangriffen und anderen Formen von ausländischer Informationsmanipulation und Einmischung waren, zu stärken, nicht zuletzt angesichts der groß angelegten Cyberangriffe auf die rumänischen Wahlbehörden im Herbst 2024; in der Erwägung, dass im jährlichen Tätigkeitsbericht der ENISA von 2019 bereits empfohlen wurde, Wahlsysteme, -verfahren und -infrastruktur als kritische Infrastruktur einzustufen, damit die erforderlichen Cybersicherheitsmaßnahmen ergriffen werden;
- CK. in der Erwägung, dass mehrere Berichte und Untersuchungen, darunter Erkenntnisse im Zusammenhang mit sogenannten Doppelgänger-Kampagnen, bei denen sich Akteure als Vertreter etablierter Medien ausgeben, darauf hindeuten, dass Russland wahrscheinlich in die Bundestagswahl 2025 in Deutschland eingegriffen und proeuropäische politische Parteien ins Visier genommen hat; in der Erwägung, dass im Rahmen umfassenderer Einflussnahme, die als Muster in mehreren europäischen Ländern beobachtet wurde, auch andere Akteure aus Drittländern an der Einmischung in diese Wahl beteiligt gewesen sein könnten;
- CL. in der Erwägung, dass die verdeckte Finanzierung politischer Parteien und Bewegungen in der EU durch Drittländer, die durch erfolgte dokumentierte Fälle der Einflussnahme aus dem Ausland durch autoritäre Regime im Wege direkter oder indirekter Finanzierung politischer Parteien, Stiftungen oder verbundener Medien belegt wird, eine Bedrohung für die demokratische Widerstandsfähigkeit, die Integrität von Wahlen und die Legitimität des demokratischen Prozesses darstellt;
- CM. in der Erwägung, dass das Parlament Ziel von Spionage und Einflussnahme aus dem Ausland war, einschließlich des Falls, in dem ein Assistent des ehemaligen Mitglieds des Europäischen Parlaments (MdEP), Maximilian Krah, Mitglied der Partei „Alternative für Deutschland“ (AfD), wegen Spionage für China verurteilt wurde; in der Erwägung, dass MdEP und ihre Bediensteten im Parlament Zugang zu sensiblen Informationen und Dokumenten haben;
- CN. 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;
- CO. in der Erwägung, dass die EU seit 2022 insgesamt 21 Pakete

umfassender und beispielloser Sanktionen als Reaktion auf die militärische Aggression Russlands gegen die Ukraine verhängt hat; in der Erwägung, dass mit diesen Sanktionen der Druck auf die Kriegswirtschaft Russlands erheblich erhöht werden soll und Schlüsselsektoren, insbesondere der Energie-, Finanz- und Verteidigungssektor, Sonderwirtschaftszonen sowie Unterstützer und Nutznießer seines Angriffskriegs ins Visier genommen werden sollen und die Abhängigkeit der EU von Einfuhren fossiler Brennstoffe aus Russland beendet werden soll; in der Erwägung, dass die EU außerdem Sanktionen gegen Belarus, Iran und Nordkorea verhängt hat, weil sie den Angriffskrieg Russlands gegen die Ukraine unterstützen; in der Erwägung, dass die Wirksamkeit solcher Maßnahmen gestärkt und Schlupflöcher, die ihre Umgehung ermöglichen, geschlossen werden sollten;

- CP. in der Erwägung, dass seit dem 8. Oktober 2024 der Sanktionsrahmen der EU ausgeweitet wurde und die Bekämpfung einer Vielzahl hybrider Aktivitäten Russlands ermöglicht, darunter die Beeinträchtigung von Wahlprozessen und der Funktionsweise demokratischer Einrichtungen, Bedrohungen und Sabotageakte im Zusammenhang mit wirtschaftlichen Aktivitäten, Diensten von öffentlichem Interesse und kritischer 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 dieses Sanktionsregimes nun Vermögenswerte einfrieren, Einreiseverbote verhängen, Rundfunklizenzen aussetzen und Finanz- und Kryptowerttransaktionen im Zusammenhang mit hybriden Aktivitäten untersagen kann;
- CQ. in der Erwägung, dass Vergeltungsmaßnahmen, einschließlich Haftbefehlen und in Abwesenheit geführten Verfahren, vom Moskauer Regime häufig gegen ausländische Staatsangehörige, die in anderen Staaten ansässig sind, ergriffen werden, wobei ihnen vorgeworfen wird, die Politik Moskaus kritisiert oder sich seinem Einfluss widersetzt zu haben; in der Erwägung, dass die Staatsorgane Russlands am 28. Dezember 2024 bekannt gegeben haben, dass sie ihre schwarze Liste von EU-Bürgerinnen und Bürgern, einschließlich Amtsträgern, darunter auch Vertreter von EU-Organen, nationalen Regierungen, Strafverfolgungsbehörden und Handelsorganisationen, erheblich erweitert haben; 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 und falsche rechtliche Anschuldigungen, häufig ohne formelle Benachrichtigung, Begründung oder Recht auf einen Rechtsbehelf, einzuschüchtern und Stimmen zum Schweigen zu bringen; in der Erwägung, dass ein solcher Zwang einem Eskalationsmuster folgt, das mit administrativem Ausschluss beginnt, zu Online-Belästigung führt und in physischer Bedrohung, Überwachung, Einschüchterung von Familienangehörigen oder sogar gewaltsamen Übergriffen mündet; in der Erwägung, dass allein die Gefahr, auf die schwarze Liste gesetzt zu werden, EU-Beamte dazu veranlassen kann, sich in voreilendem Gehorsam in Selbstzensur zu üben und keine politischen Standpunkte einzunehmen; in der Erwägung, dass das Moskauer Regime parallel dazu als Mittel transnationaler Unterdrückung Listen russischer Staatsbürger führt, die außerhalb Russlands leben;

- CR. in der Erwägung, dass die schwarze Liste Russlands als Instrument der hybriden Kriegsführung und des ausländischen Zwangs eingestuft werden sollte; in der Erwägung, dass eine angemessene Reaktion der EU einen verstärkten Austausch nachrichtendienstlicher Erkenntnisse sowie gezielte Sanktionen wie das Einfrieren von Vermögenswerten und Einreiseverbote für ausländische Beamte, Handlanger und Finanzmittler, die für Zwangsmaßnahmen verantwortlich sind, sowie die Unterbindung der finanziellen und logistischen Netze, die diese Vorgänge ermöglichen, einschließlich Kanäle für Kryptowährungen, umfassen sollte;
- CS. in der Erwägung, dass die EU ein Instrument gegen Zwangsmaßnahmen verabschiedet hat, um sich selbst und ihre Mitgliedstaaten vor wirtschaftlichem Zwang durch Drittländer zu schützen;
- CT. 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, von Institutionen und der Wirtschaft insgesamt auswirken, eine zentrale Herausforderung für die inneren Angelegenheiten der EU darstellen und die demokratischen Einrichtungen in allen Mitgliedstaaten destabilisieren sowie die Zukunft Europas insgesamt gefährden, wie der Angriffskrieg Russlands gegen die Ukraine gezeigt hat;
- CU. in der Erwägung, dass zivile und militärische Vorsorge eines umfassenden gesamtgesellschaftlichen, gesamtstaatlichen und gefahrenübergreifenden Ansatzes bedarf, in dessen Rahmen die Zusammenarbeit nationaler Behörden der Mitgliedstaaten mit den Organen, Einrichtungen und sonstigen Stellen der EU sowie

Unternehmen, Hochschulen, der Zivilgesellschaft und einzelnen Bürgerinnen und Bürgern erleichtert wird bzw. diese Akteure einbezogen werden; in der Erwägung, dass der Europäische Schutzschild für die Demokratie eine einzigartige Gelegenheit bietet, diesen Ansatz zu etablieren; in der Erwägung, dass diese Bemühungen mit langfristigen Investitionen einhergehen müssen, die auf realistische Weise dem Ausmaß der Herausforderung gerecht werden, sowie mit einem wirksamen koordinierten Einsatz von Mitteln, einer strategischen Vorausschau und der Verankerung der Resilienz in der Politikgestaltung, der Infrastrukturentwicklung, den Bildungssystemen und den Lieferketten; in der Erwägung, dass die Initiativen der EU im Zusammenhang mit Verteidigung und Vorsorge aufeinander abgestimmt und synergetisch umgesetzt werden sollten;

- CV. in der Erwägung, dass die Stärkung der Handlungskompetenz der Bürgerinnen und Bürger durch Wissen, Bildung, Medienkompetenz und digitale Kompetenz, kritisches Denken und Zugang zu zuverlässigen Informationen von entscheidender Bedeutung für die gesellschaftliche Resilienz ist, da dadurch sichergestellt wird, dass alle Bürgerinnen und Bürger Risiken antizipieren, Manipulation erkennen, in Notfällen angemessen reagieren und aktiv zur kollektiven Resilienz demokratischer Gesellschaften beitragen können; in der Erwägung, dass der terrestrische Rundfunk in der gesamten EU verfügbar ist und einen zuverlässigen und sicheren Weg darstellt, die Bürgerinnen und Bürger im Falle von Naturkatastrophen oder von Menschen verursachten Katastrophen, insbesondere bei Ausfällen des Internets und anderer Kommunikationsmittel, zu informieren; in der Erwägung, 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 in allen Alters- und Gesellschaftsschichten umfassen muss;
- CW. in der Erwägung, dass die zivil-militärische Zusammenarbeit, Fähigkeiten mit doppeltem Verwendungszweck und die Einbeziehung der Vorsorge in Bildungsprogramme zusammen mit praktischen Fähigkeiten und Wissen im Bereich des Zivilschutzes 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; in der Erwägung, dass die staatsbürgerliche Verantwortung, das Bewusstsein für Bedrohungen und das Verständnis für die Rolle der Bürgerinnen und Bürger bei der Gewährleistung der Sicherheit gefördert werden müssen;
- CX. 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; in der Erwägung, dass europäische Telekommunikationsunternehmen Ziel von Cyberspionage sind, was durch die jüngsten Beispiele der mit China verbundenen Gruppe „Salt Typhoon“ bestätigt wird; in der Erwägung, dass der Telekommunikationssektor als Eckpfeiler dieser Ökosysteme robuste Cybersicherheits- und Resilienzmaßnahmen erfordert, um sicher und betriebsfähig zu bleiben;

- CY. in der Erwägung, dass die Vorsorge von einer reibungslosen Zusammenarbeit zwischen den Organen, Einrichtungen und sonstigen Stellen der EU, den Mitgliedstaaten und gleichgesinnten internationalen Partnern abhängt, die durch gemeinsame Übungen und Schulungen, gemeinsame Plattformen zur Lageerfassung und einen raschen Informationsaustausch unterstützt wird; in der Erwägung, dass Taiwan, ein führender Partner im Hinblick auf die Lageerfassung, umfassende Übungen zur zivilen Verteidigung und Resilienz organisiert hat, um Chinas zunehmende, sich in der Grauzone bewegenden Kriegsführungstaktiken zu bekämpfen und seine Militärübungen zu ergänzen; in der Erwägung, dass der gesamtgesellschaftliche Ansatz und die bewährten Verfahren Taiwans dazu beitragen können, in der EU ein Vorsorgekonzept zu entwickeln sowie die gemeinsame Lageerfassung, die Frühwarnkapazitäten und die allgemeine Wirksamkeit des Europäischen Schutzschilds für die Demokratie zu stärken;
- CZ. 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 – insbesondere im digitalen Bereich – zu verringern; in der Erwägung, dass für diese Bemühungen neue gezielte Finanzierungsmechanismen erkundet werden müssen;

Einleitung

1. begrüßt die gemeinsame Mitteilung zum Europäischen Schutzschild 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 inmitten der sich ständig wandelnden Bedrohungslage zu schützen und letztlich zum Schutz der in Artikel 2 EUV verankerten Werte beizutragen; ist der Ansicht, dass die in der Mitteilung dargelegten Maßnahmen das Maß an Ambition, die Vorausschau und die Kapazitäten, die erforderlich sind, nicht vollständig widerspiegeln und im Laufe der Zeit weiterentwickelt und schrittweise verstärkt werden sollten, um die wirksame

Einführung robuster und verbindlicher Maßnahmen zum Schutz der Demokratie im Einklang mit dem Ausmaß der ermittelten Herausforderungen sicherzustellen und gleichzeitig die in den Verträgen verankerte Aufteilung der Zuständigkeiten der EU zu achten; betont, dass weiche politische Maßnahmen häufig unzureichend sind, wenn demokratische Werte absichtlich untergraben werden, und dass die Bekämpfung von Einflussnahme aus dem Ausland, hybriden Bedrohungen und Desinformation Ambition und entschlossenes Handeln erfordert; vertritt den Standpunkt, dass die Glaubwürdigkeit des Europäischen Schutzschildes für die Demokratie auch vom Willen und der Entschlossenheit abhängt, die bestehenden EU-Rechtsvorschriften, die für die Verteidigung der Demokratie von Bedeutung sind, durchzusetzen; weist ferner darauf hin, dass die Fragmentierung der EU nach wie vor eine Schwachstelle bei der Verteidigung der Demokratie darstellt;

2. nimmt mit Besorgnis die zunehmend komplexe und sich wandelnde Bedrohungslage zur Kenntnis, in deren Rahmen die demokratischen Prozesse und Organe in der EU und ihren Mitgliedstaaten untergraben werden und die durch ausländische Informationsmanipulation und Einmischung, hybride Angriffe und Desinformationskampagnen böswilliger Akteure aus Drittländern und ihren Handlangern in der EU gekennzeichnet ist; betont, dass hybride Kriegsführung über Angriffe im Cyber- und Informationsbereich allein hinausgeht und die wirtschaftliche, technologische und gesellschaftliche Dimension von strategischer Konfrontation umfasst; betont, dass dies auch die Realität von vielen gleichgesinnten Partnern der EU in ihrer Nachbarschaft und weltweit ist;
3. betont, dass der soziale Zusammenhalt und das Vertrauen in öffentliche Einrichtungen Eckpfeiler der demokratischen Resilienz sind; betont, dass Schwächen im Hinblick auf die Rechtsstaatlichkeit, insbesondere in Bereichen wie Unabhängigkeit der Justiz, Medienpluralismus und Wirksamkeit der Rahmen für die Korruptionsbekämpfung, das Vertrauen der Öffentlichkeit gefährden und sowohl von internen als auch von externen Akteuren instrumentalisiert werden könnten, um den demokratischen Konsens zu schwächen und die gesellschaftliche Polarisierung zu verschärfen; betont, dass ein umfassender Ansatz erforderlich ist, der darauf abzielt, Bedenken im Zusammenhang mit der Rechtsstaatlichkeit auszuräumen und den sozialen Zusammenhalt, die demokratische Legitimität und das gesellschaftliche Vertrauen in der gesamten EU und ihren Mitgliedstaaten zu stärken; weist ferner darauf hin, dass es von entscheidender Bedeutung ist, die Rechtsstaatlichkeit in Bewerberländern zu stärken, um ihre Angleichung an die Werte der EU zu unterstützen und die demokratische Resilienz Europas insgesamt zu stärken;

4. betrachtet Russland als die größte externe Bedrohung für die Sicherheit und demokratische Integrität Europas und bekräftigt seine Auffassung, dass Russland ein dem Terrorismus Vorschub leistender Staat ist; betont, dass eine umfassende und zukunftsorientierte Strategie erforderlich ist, um die europäische Demokratie zu schützen;
5. betont, dass die in der Initiative „Europäischer Schutzschild für die Demokratie“ dargelegten wichtigsten 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 unabhängiger Medien und eines investigativen Journalismus – im kommenden MFR mit ausreichenden Mitteln ausgestattet werden müssen; betont, dass Investitionen in die demokratische Resilienz für die Sicherheit, die Souveränität und den Wohlstand der EU von entscheidender Bedeutung sind; bringt seine Unterstützung für die Zusage der Kommission zum Ausdruck, die demokratische Resilienz in allen Finanzierungsprogrammen der EU durchgängig zu berücksichtigen; betont in diesem Zusammenhang, dass verschiedene Aspekte der hybriden Verteidigung in die Verteidigungsinitiativen der EU einbezogen werden müssen; betont jedoch, dass klare Ziele mit messbaren Maßnahmen und Ergebnissen erforderlich sind, um die Ressourcen der EU und der Mitgliedstaaten effektiv zu nutzen und Verschwendung oder fragmentierte Finanzierung zu vermeiden;
6. verurteilt die Einmischung von Drittstaaten in bestimmte Gebiete in äußerster Randlage und überseeische Länder und Gebiete, deren Auswirkungen aufgrund ihrer Abgelegenheit und geografischen Entfernung vom europäischen Kontinent noch verstärkt werden können;

Europäisches Zentrum für demokratische Resilienz

7. 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 vollständig aufnehmen kann;

stellt jedoch fest, dass klare Angaben zum Zeitplan und zu den konkreten Etappenzielen für die schrittweise Umsetzung des Zentrums fehlen, da der Verweis auf eine „schrittweise“ Umsetzung auf der Grundlage der freiwilligen Beteiligung der Mitgliedstaaten keine ausreichende Vorhersehbarkeit, Rechenschaftspflicht oder operative Sicherheit bietet; 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;

8. bedauert jedoch, dass es dem Zentrum, wie im Vorschlag dargelegt, an einem klaren Mandat und einer Befugnisübertragung durch einen Rechtsakt sowie an zweckgebundenen Haushaltsmitteln und Personal, einer spezifischen Governance-Struktur 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; betont, dass das Zentrum einen Mehrwert schaffen sollte, der über die bestehenden Strukturen hinausgeht, und nicht zu einem weiteren Drehkreuz, Netzwerk oder Rahmen oder einer weiteren Plattform unter anderen werden sollte, wodurch die Fähigkeit der EU, das gesamte Spektrum der derzeit verfügbaren Instrumente effizient zu nutzen, weiter eingeschränkt wird, indem es bei Tätigkeiten zu Überschneidungen kommt, die institutionelle Unklarheit verstärkt und die Fragmentierung verschärft wird und die Haushaltsmittel auf mehrere Stellen aufgeteilt werden; ist daher der festen Überzeugung, dass das Zentrum als Aggregator und Konsolidator bestehender Maßnahmen auf EU-Ebene fungieren und nationale Maßnahmen unterstützen, verstärken, ergänzen und, falls möglich, koordinieren sollte;
9. 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 bis zum Ende des Jahres 2026 abgeschlossen sein soll; fordert, dass die Integration die operative Verantwortung für ein verbessertes Schnellwarnsystem umfasst, mit dem gegen Informationsmanipulation in Echtzeit vorgegangen werden kann, sowie die Einrichtung und den Betrieb einer einheitlichen Informationsdatenbank zu ausländischer Informationsmanipulation und Einmischung, wodurch die Ressource EUvsDisinfo weiterentwickelt wird, unter anderem durch die Kartierung von

Plattformen, die zur Verbreitung von ausländischer Informationsmanipulation und Einmischung und Desinformation genutzt werden, das ECNE und die Taskforce der Kommission für Desinformation und strategische Kommunikation; fordert die Kommission auf, dafür zu sorgen, dass das Zentrum in der Lage ist, koordinierte Angriffe auf die Informationsintegrität zu bewerten; betont, dass das Zentrum in der Lage sein muss, Einflussnahme aus dem Ausland und hybride Bedrohungen zu verfolgen, zu überwachen und darauf zu reagieren, wobei sicherzustellen ist, dass alle eingebundenen Organisationen ihre Unabhängigkeit wahren, insbesondere gegenüber Big-Tech-Unternehmen;

10. begrüßt, dass die Kommission die Notwendigkeit anerkannt hat, sich mit den Mitgliedstaaten und dem Parlament über das Mandat, die Struktur und die Arbeitsmethoden des Zentrums zu beraten, und fordert die Kommission als nächsten Schritt auf, einen Rechtsakt zur Einrichtung des Zentrums als eine strukturell unabhängige EU-Einrichtung mit einer klaren institutionellen Satzung und einer klaren Positionierung, einer klaren Verwaltungsstruktur und klaren parlamentarischen Kontrollmechanismen vorzuschlagen; betont, dass institutionelle Klarheit unerlässlich ist, damit das Zentrum entschlossen handeln und gleichzeitig rechenschaftspflichtig bleiben kann; ist der Ansicht, dass die Einrichtung des Zentrums in Form einer dauerhaften Struktur durch einen Rechtsakt einen qualitativen Wandel von einer fragmentierten Koordinierung hin zu einer stärker integrierten, operativen und strategischen Kapazität auf EU-Ebene darstellen würde; betont, dass es einen ehrgeizigen Zeitplan für die Einrichtung des Zentrums durch einen Rechtsakt geben sollte, um angesichts sich rasch verändernder Gegebenheiten ein kohärentes und rechtzeitiges Handeln in der gesamten EU sicherzustellen;
11. fordert, dass an der Leitung des Zentrums Vertreter jedes Mitgliedstaats beteiligt werden; stellt fest, dass die in der Mitteilung der Kommission vorgeschlagene freiwillige Beteiligung der Mitgliedstaaten die Gefahr birgt, dass die Struktur ineffizient und fragmentiert bleibt und im Hinblick auf gemeinsame Bedrohungen in der gesamten EU weiterhin mit unterschiedlichen Schutzniveaus und Reaktionen darauf zu rechnen ist; stellt fest, dass ohne eine Vertretung aller Mitgliedstaaten in den Leitungsgremien die Gefahr einer Struktur besteht, die auf der Grundlage eines kleinsten gemeinsamen Nenners funktioniert;
12. betont, dass verstärkte Maßnahmen auf EU-Ebene zum Schutz der Demokratie mit einer starken demokratischen Kontrolle einhergehen müssen; fordert die Kommission auf, dem Europäischen Parlament regelmäßig über die Tätigkeiten des Zentrums Bericht zu erstatten, einschließlich dessen haushaltstechnischen, operativen und strategischen Dimensionen; betont, dass die Leitung des Zentrums Vertreter des Europäischen Parlaments umfassen sollte, um seine demokratische Legitimität zu stärken;

13. fordert die Kommission auf, das Zentrum mit einem klaren Mandat, Entscheidungsmechanismen und Befugnissen auszustatten, damit es als unabhängiges Exzellenzzentrum für die Aufdeckung, Analyse und Bekämpfung von ausländischer Informationsmanipulation und Einmischung und von Desinformationsoperationen, als Plattform für den Kapazitätsaufbau, die zur Festlegung gemeinsamer Definitionen, Standards, Schulungen und technischer Instrumente in der gesamten EU beiträgt, und als operatives Rückgrat für die Umsetzung von Bedrohungsanalysen und Frühwarnungen in konkrete, rechtzeitige und evidenzbasierte operative Ergebnisse sowie für die Echtzeitkoordinierung der technischen Unterstützung bei der Bekämpfung aktiver Informationsmanipulationskampagnen fungieren kann, und zwar in enger Zusammenarbeit mit den nationalen Behörden und den zuständigen EU-Stellen; betont, dass das Zentrum in der Lage sein muss, in Krisensituationen, insbesondere im Vorfeld von und während Wahlen, rasch zu handeln, um die Lageerfassung in wirksame Maßnahmen umzusetzen; stellt fest, dass sich die Einmischungstaktiken böswilliger Akteure im Laufe der Zeit parallel zum technologischen Fortschritt weiterentwickeln werden und dass das Mandat des Zentrums Flexibilität ermöglichen sollte, um neuen Herausforderungen begegnen zu können; betont, dass das Zentrum mit stabilem, multidisziplinärem Personal ausgestattet sein muss, darunter Analysten im Bereich ausländische Informationsmanipulation und Einmischung, Experten auf dem Gebiet der Informationsgewinnung aus frei zugänglichen Quellen sowie Spezialisten für Cybersicherheit und Finanzverfolgung, und dass es über die Befugnis verfügen muss, grenzübergreifende Taskforces mit den zuständigen Behörden der Mitgliedstaaten zu koordinieren;
14. fordert die Kommission auf, dafür zu sorgen, dass die Analyse- und Überwachungskapazitäten des Zentrums formell als Quelle für Beiträge unabhängiger Sachverständiger zu den im Rahmen des Gesetzes über digitale Dienste eingerichteten Verfahren zur Bewertung systemischer Risiken strukturiert sind, auch mit den Koordinatoren für digitale Dienste in jedem Mitgliedstaat und im Rahmen des Europäischen Medienfreiheitsgesetzes, der Verordnung über die Transparenz und das Targeting politischer Werbung und der Verordnung über künstliche Intelligenz, indem unter anderem bei der Erhebung, Sicherung und Analyse von Beweismitteln im Zusammenhang mit ausländischer Informationsmanipulation und Einmischung und Desinformation zusammengearbeitet wird, wobei die Erkenntnisse direkt in Durchsetzungsmaßnahmen einfließen, und indem zeitnah Berichte über Bedrohungsanalysen, Analysen von ausländischer Informationsmanipulation und Einmischung und Indikatoren für Demokratierisiken bereitgestellt werden; betont, dass die Rolle des Zentrums bei diesen Vorgängen beratender und analytischer Natur bleiben muss, um die Unabhängigkeit der Entscheidungsfindung in Regulierungsfragen zu wahren; betont, dass in Fällen, in denen durch ausländische

Informationsmanipulation und Einmischung und Desinformationstätigkeiten das EU-Recht untergraben wird, über die Koordinierungsfunktion des Zentrums eine direkte Verbindung zu Stellen gewährleistet werden sollte, die zur Einleitung von Ermittlungen und Gerichtsverfahren befugt sind; fordert, dass maßgebliche Feststellungen zu systemischen Mängeln oder wiederkehrenden Schwachstellen gebührend berücksichtigt und im jährlichen Bericht der Kommission über die Rechtsstaatlichkeit in speziellen Unterabschnitten berücksichtigt werden, in denen es um Desinformation und die Integrität der Medien im Rahmen der Säule des Medienpluralismus und der Medienfreiheit sowie um die Integrität von Wahlen und Schutzmaßnahmen gegen unzulässige Einflussnahme im Rahmen der Säule der Gewaltenteilung geht; stellt fest, dass das Zentrum auch zur Schulung der Koordinatoren für digitale Dienste und des Personals der nationalen Medienregulierungsbehörden zum Thema ausländische Informationsmanipulation und Einmischung und Desinformation beitragen könnte;

15. begrüßt das Konzept einer Plattform für Interessenträger; stellt jedoch fest, dass ihr Zweck, ihre Struktur und ihr Mehrwert nach wie vor nicht hinreichend definiert sind, einschließlich im Zusammenhang mit bestehenden Netzwerken und Initiativen; erkennt den Mehrwert des Beitrags der Zivilgesellschaft bei der Entwicklung des Mandats des Zentrums an; fordert die Kommission auf, dafür zu sorgen, dass die Koordinierung durch das Zentrum die bestehenden Bemühungen der Zivilgesellschaft und der Wissenschaft im Rahmen der vorgeschlagenen Plattform umfasst; weist nachdrücklich darauf hin, dass das Zentrum außerdem Regierungen und unterschiedlichen Interessenträgern Möglichkeiten bieten muss, über Grenzen hinweg Kontakte zu knüpfen und voneinander zu lernen;
16. fordert die Kommission auf, dafür zu sorgen, dass das Zentrum auch 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 und die Verbesserung der Integrität von Wahlen erschöpft; stellt fest, dass koordinierte Informationsmanipulationskampagnen häufig auf den Informationsraum der EU als Ganzes abzielen, was spezielle operative Kapazitäten auf EU-Ebene zum Schutz demokratischer Prozesse über rein nationale Kontexte hinaus rechtfertigt; 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; betont, dass Arbeitsmethoden und Datennutzung zwischen den auf EU- und nationaler Ebene bestehenden Strukturen vollständig interoperabel sein müssen; betont in diesem Zusammenhang, dass es gemeinsamer Open-Source-Methoden und einer wirksamen Zusammenarbeit zwischen Netzwerken von Akteuren, darunter Forschende auf dem Gebiet der Informationsgewinnung aus frei zugänglichen Quellen, Journalisten, Kommunikationsbeauftragte und politische Entscheidungsträger, bedarf;

17. 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 und ein Evaluierungsverfahren für den Aufbau von Kapazitäten in den Mitgliedstaaten zu erstellen; betont, dass ein solches Vorgehen eine Grundlage für eine schrittweise Anhebung der Zielvorgaben des Zentrums bieten würde;
18. fordert die Kommission auf, zu prüfen, ob das Zentrum ermächtigt werden kann, zweckgebundene EU-Mittel im Rahmen des derzeitigen und künftigen MFR und der einschlägigen EU-Programme zu verwalten, wenn sie die Bekämpfung von ausländischer Informationsmanipulation und Einmischung, die Stärkung der demokratischen Widerstandsfähigkeit und die Förderung der Informationsintegrität betreffen; fordert die Kommission auf, eine Programmplanung zu vermeiden, die zu einer Zerstreung und Fragmentierung der Bemühungen führt oder kleine Initiativen hervorbringt, die befristet und nicht nachhaltig sind, und vielmehr den Schwerpunkt auf koordinierte, strategisch skalierbare Maßnahmen zu legen, die nachhaltige Wirkung für alle beteiligten Akteure entfalten;
19. fordert die Kommission auf, ausreichende und vorhersehbare Mittel für das Zentrum und seine Tätigkeiten, einschließlich ausreichender personeller und finanzieller Ressourcen im Rahmen des nächsten MFR, sowie eine eigene EU-Haushaltslinie für die Tätigkeiten des Zentrums mit einer klaren Trennung zwischen operativer Finanzierung und allgemeinen Koordinierungskosten bereitzustellen; fordert die Kommission ferner auf, ausreichende personelle Ressourcen sicherzustellen und die Finanzierung aus bestehenden Haushalten zu überbrücken, um die vorbereitenden Arbeiten vor dem MFR 2028-2034 zu ermöglichen;
20. fordert die Kommission auf, die Durchführbarkeit der Einrichtung eines Finanzierungsmechanismus zur Ergänzung der speziellen Haushaltslinie für die Tätigkeiten des Zentrums zu prüfen; vertritt den Standpunkt, dass ein solcher Mechanismus zu seinen Beitragszahlern große Anbieter von Diensten der

Informationsgesellschaft zählen sollte, deren Tätigkeiten ein systemisches Risiko für die demokratische Integrität darstellen; betont, dass ein solcher Mechanismus mit möglichst strengen Garantien für Unabhängigkeit und der vollständigen Vermeidung von Interessenkonflikten einhergehen muss;

Digitale Resilienz

21. fordert die vollständige Umsetzung und wirksame Durchsetzung des gesamten Besitzstands der EU im Bereich Digitales, einschließlich wichtiger Rechtsvorschriften wie des Gesetzes über digitale Dienste, des Gesetzes über digitale Märkte, der Verordnung über die Transparenz und das Targeting politischer Werbung, der Verordnung über künstliche Intelligenz und des Europäischen Medienfreiheitsgesetzes, in allen Mitgliedstaaten und unter uneingeschränkter Achtung der Grundrechte; betont, dass die konsequente, einheitliche, systematische und zeitnahe Durchsetzung eine wesentliche Säule der europäischen digitalen Souveränität und der Abschreckung ist und eine Voraussetzung für die Tätigkeit im Binnenmarkt sein muss; fordert die Kommission nachdrücklich auf, regelmäßig über die Durchsetzung und Anwendung des EU-Rechts, insbesondere des Gesetzes über digitale Dienste, Bericht zu erstatten, übermäßige Verzögerungen bei Untersuchungen zu vermeiden und strenge Sanktionen für anhaltende Verstöße sehr großer Online-Plattformen und sehr großer Online-Suchmaschinen zu verhängen; vertritt den Standpunkt, dass bei der weiteren Umsetzung der Rechtsvorschriften im digitalen Bereich der Schwerpunkt stärker auf die Bekämpfung von ausländischer Informationsmanipulation und Einmischung und Desinformation im Internet, die Gewährleistung der Informationsintegrität und den Schutz des demokratischen Diskurses während und außerhalb des Wahlkampfs gelegt werden sollte;
22. ist zutiefst besorgt darüber, dass die auf dem Nutzerverhalten basierenden Empfehlungssysteme bestimmter sehr großer Online-Plattformen häufig ein systemisches Risiko für den gesellschaftlichen Diskurs und Wahlprozesse darstellen, da sie spaltende, polarisierende oder irreführende Inhalte verstärken, häufig Desinformation von ausländischen und inländischen Akteuren befeuern und sensationslüsterne Inhalte gegenüber faktenbasierten Inhalten unverhältnismäßig bevorzugen; weist darauf hin, dass sehr große Online-Plattformen gemäß den Artikeln 34 und 35 des Gesetzes über digitale Dienste verpflichtet sind, diese Risiken zu bewerten und zu mindern; vertritt die Auffassung, dass mit wirksamen Risikominderungsmaßnahmen auch sichergestellt werden sollte, dass synthetische oder manipulierte Inhalte wie Deepfakes klar von authentischen Inhalten unterschieden werden können und dass redaktionell unabhängige und pluralistische Medien und verifizierte Quellen gebührende Beachtung finden; fordert die Kommission auf, die Einhaltung der Verpflichtungen aus dem Gesetz

über digitale Dienste in dieser Hinsicht zu prüfen und geeignete Maßnahmen zu ergreifen, einschließlich der Verhängung einstweiliger Maßnahmen; schlägt vor, dass solche einstweiligen Maßnahmen erforderlichenfalls die Beschränkung von auf dem Nutzerverhalten basierenden Empfehlungssystemen umfassen, die ein systemisches Risiko darstellen; fordert die Kommission ferner auf, mehr Transparenz und größere Rechenschaftspflicht bei der Gestaltung algorithmischer Empfehlungs- und Werbesysteme zu fördern, insbesondere zusammen mit anderen algorithmischen Systemen, um die Wahlmöglichkeiten der Nutzer zu verbessern und nicht manipulative Standardeinstellungen sicherzustellen und gleichzeitig die Meinungs- und Informationsfreiheit zu fördern; weist sehr große Online-Plattformen in diesem Zusammenhang auf ihre Verpflichtung gemäß Artikel 35 Absatz 1 Buchstabe d und Artikel 38 des Gesetzes über digitale Dienste hin, systemische Risiken zu mindern, wozu auch die Erprobung und Anpassung ihrer algorithmischen Systeme, einschließlich ihrer Empfehlungssysteme, gehören können, sowie mindestens eine Option für jedes ihrer Empfehlungssysteme bereitzustellen, die nicht auf Profiling beruht; fordert die Kommission ferner auf, in Zusammenarbeit mit den Koordinatoren für digitale Dienste und unter Einbeziehung unabhängiger Dritter im Rahmen öffentlicher Konsultationen dafür zu sorgen, dass es aktuelle Leitlinien für die Minderung systemischer Risiken gibt und es eine einheitliche Durchsetzung und ein hohes Maß an Schutz vor Manipulation in großem Maßstab gibt;

23. verurteilt die gezielten Sanktionen und Versuche der US-Regierung, Druck auf EU-Akteure auszuüben, die an der Gestaltung und Durchsetzung des Gesetzes über digitale Dienste und anderer digitaler Vorschriften beteiligt sind, insbesondere auf ein ehemaliges Kommissionsmitglied; fordert, dass diese Maßnahmen umgehend aufgehoben werden; fordert die Kommission und die Mitgliedstaaten nachdrücklich auf, diesem Druck standzuhalten, die EU-Rechtsvorschriften aufrechtzuerhalten und das Recht auf Selbstverwaltung und digitale Souveränität zu verteidigen; betont, dass das Recht auf freie Meinungsäußerung ein Grundrecht in Europa und ein Grundwert ist, den die Vereinigten Staaten und gleichgesinnte Partner in der gesamten demokratischen Welt teilen; betont, dass politische und handelspolitische Erwägungen sowie der Druck von Drittländern oder großen Technologieunternehmen die Durchsetzung der EU-Rechtsvorschriften im digitalen Bereich nicht unangemessen beeinflussen sollten; betont, dass Entscheidungen über die Anwendung der Vorschriften der EU im digitalen Bereich ausschließlich vom EU-Recht und dem Schutz demokratischer Interessen geleitet werden dürfen und dass die EU als offener und regelbasierter Binnenmarkt das souveräne Recht behält, ihre Wirtschaftstätigkeit im Einklang mit demokratischen Werten und internationalen Verpflichtungen zu regulieren; fordert die Kommission und die Mitgliedstaaten auf, dafür zu sorgen, dass die Schutz- und Rechtsbehelfsmechanismen im Rahmen der EU-

Rechtsvorschriften im digitalen Bereich vor Eingriffen geschützt werden, die ihre Unabhängigkeit oder Wirksamkeit beeinträchtigen könnten, und solide Schutzvorkehrungen gegen solche Risiken zu treffen;

24. fordert die Kommission auf, die Bemühungen um die Förderung und Angleichung des Gesetzes über digitale Dienste und anderer wichtiger Rechtsakte der EU im digitalen Bereich in Bewerberländern und potenziellen Bewerberländern zu verstärken und sicherzustellen, dass diese Länder über die Unterstützung, Instrumente und Leitlinien verfügen, die für die Umsetzung solcher Gesetze erforderlich sind, um gegebenenfalls eine schrittweise Integration in die einschlägigen Durchsetzungs- und Kooperationsmechanismen der EU zu ermöglichen; betont, dass Bemühungen zur Unterbindung von Desinformation ausdrücklich Bewerberländer und potenzielle Bewerberländer umfassen sollten, um Regulierungslücken und grenzüberschreitende Ausstrahlungseffekte zu verhindern; betont, dass die in Bewerberländern und potenziellen Bewerberländern beobachteten Trends bei der Durchführung von Tätigkeiten im Zusammenhang mit Wahlen im Rahmen des Verhaltenskodex zur Bekämpfung von Desinformation besonders berücksichtigt werden müssen;
25. nimmt die offizielle Integration des freiwilligen Verhaltenskodex zur Bekämpfung von Desinformation in den Rahmen des Gesetzes über digitale Dienste als ein Verhaltenskodex zur Bekämpfung von Desinformation zur Kenntnis, der zu einem relevanten Maßstab für die Feststellung der Einhaltung der Bestimmungen des Gesetzes über digitale Dienste in Bezug auf Desinformationsrisiken geworden ist, um andere wirksame Risikominderungsmaßnahmen sehr großer Online-Plattformen und sehr großer Online-Suchmaschinen zu ergänzen, um gegen systemische Risiken für demokratische Prozesse vorzugehen; stellt fest, dass die Auswirkungen eines möglichen Verstoßes gegen den Kodex auf die Einhaltung und Durchsetzung des Gesetzes über digitale Dienste weiter erläutert werden könnten; betont, dass der Kodex ein dynamisches Instrument bleiben sollte, das den jüngsten Trends folgt, und dass die Kommission die wirksame Umsetzung durch die Unterzeichner weiterhin überwachen sollte; ist der Ansicht, dass bei der Umsetzung des Gesetzes über digitale Dienste gegen die koordinierte, nicht authentische Nutzung von Online-Plattformen vorgegangen werden sollte, z. B. durch Bots, Scheinkonten, polarisierende Algorithmen sowie künstliche Steuerung und Verstärkung, wodurch die Illusion öffentlicher Unterstützung entsteht; ist der Ansicht, dass diese Phänomene zu den größten Risiken für einen freien, authentischen und offenen Diskurs im Internet gehören, insbesondere in Zeiten von Wahlen; betont, dass autoritäre Akteure aus dem Ausland, insbesondere Russland, Strategien zur Desinformation entwickelt haben, deren Auswirkungen bei den jüngsten Wahlen in ganz Europa zunehmend sichtbar geworden sind; 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;

26. begrüßt die Zusage der Kommission, ein Protokoll über Vorfälle und Krisen im Zusammenhang mit dem Gesetz über digitale Dienste auszuarbeiten, einschließlich klarer Verfahren für die Koordinierung zwischen den maßgeblichen Behörden, um weiter gegen größere Vorfälle und Störungen im Informationsumfeld vorzugehen; ist der Ansicht, dass bei diesem Protokoll die Beteiligung von Online-Plattformen und Online-Suchmaschinen gefördert werden sollte, und dass mit diesem unter anderem gegen die Einflussnahme auf Wahlen durch koordiniertes, nicht authentisches Verhalten im Online-Raum vorgegangen werden sollte, insbesondere botbasierte Verstärkung und Steuerung, die einen echten öffentlichen Diskurs wirksam verzerren; betont, dass Plattformen rasch und wirksam mit Präventiv- und Korrekturmaßnahmen auf solche Eingriffe reagieren müssen und dass die Behörden bei Verstößen rasch reagieren müssen, anstatt Ex-post-Maßnahmen zu ergreifen und eine verspätete Durchsetzung zu verlassen; begrüßt in diesem Zusammenhang, dass Google im Jahr 2025 proaktiv fast 11 000 YouTube-Kanäle und -Konten entfernt hat, die mit staatlich unterstützter Propaganda aus China, Russland und von anderen böswilligen Akteuren in Verbindung standen, und fordert alle Plattformen nachdrücklich auf, systematisch gegen solche Bedrohungen vorzugehen;
27. begrüßt, 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, und begrüßt die Entscheidung der Kommission, die Einbindung der KI-Anwendung Grok in die Plattform X zu untersuchen und die bestehenden Untersuchungen auf die Empfehlungssysteme von X auszuweiten; fordert die Kommission nachdrücklich auf, die verbleibenden Untersuchungen, auch in Bezug auf Meta, zu beschleunigen, insbesondere angesichts der vorläufigen Feststellungen zu Verstößen gegen die Transparenz- und Nutzerschutzpflichten und angesichts von Berichten, in denen auf anhaltende Probleme im Zusammenhang mit betrügerischer Werbung und der Umgehung von Rechtsvorschriften hingewiesen wird; betont, dass in Fällen von Wahleinmischung, anhaltender algorithmischer Undurchsichtigkeit und der massiven Verbreitung von Scheinkonten und Bot-Netzwerken, die den öffentlichen Diskurs verzerren, Durchsetzungsmaßnahmen ergriffen werden müssen; fordert die Kommission vor diesem Hintergrund auf, die Untersuchungen zur Einhaltung des Gesetzes über digitale Dienste durch TikTok im Zusammenhang mit Einflussnahme aus dem Ausland auf die rumänische Präsidentschaftswahl 2024, bei der in

besorgniserregender Weise aufgezeigt wurde, wie Empfehlungssysteme und Bot-Netzwerke ausgenutzt werden können, sowie die Untersuchungen im Zusammenhang mit der Verpflichtung von TikTok, systemische Risiken für demokratische Prozesse zu mindern und für Abschreckung während Wahlzeiträumen zu sorgen, rasch abzuschließen; nimmt zudem die vorläufige Bewertung der Kommission zur Kenntnis, wonach TikTok aufgrund seines suchterzeugenden Designs gegen das Gesetz über digitale Dienste verstößt;

28. betont, dass mehr Transparenz in Bezug auf Akteure, die hinter Online-Inhalten und Konten stehen, erforderlich ist, insbesondere bei Werbezwecken; betont, dass Maßnahmen zur Bekämpfung koordinierten unauthentischen Verhaltens ohne Abschaffung der Anonymität im Internet von wesentlicher Bedeutung sind, um ausländische Informationsmanipulation und Einmischung, Bot-Farmen und verdeckte politische Kampagnen zu verhindern; fordert die Kommission auf, mögliche Maßnahmen zu prüfen, mit denen Online-Plattformen dabei unterstützt würden, verhältnismäßige Schritte zu ergreifen, um zu überprüfen, ob ein Mensch hinter einem Konto steht, und so den Aktivitäten von Bot-Konten entgegenzuwirken; fordert die Plattformen auf, der Entwicklung wirksamer Mechanismen zur Ermittlung, Prüfung und erforderlichenfalls Sperrung nicht authentischer Konten, insbesondere derjenigen, die an koordiniertem Vorgehen zur Einflussnahme beteiligt sind, Vorrang einzuräumen; betont, dass Maßnahmen, die auf nicht authentische Konten abzielen, nicht dazu führen dürfen, dass die Anonymität im Internet verloren geht, was für den Schutz von Journalisten, Aktivisten, marginalisierten Gemeinschaften und Einzelpersonen in prekären Situationen (wie Hinweisgebern, Dissidenten und politischen Gegnern autokratischer Regime) von wesentlicher Bedeutung ist, und dass weiterhin Raum für Konten mit satirischen und humorvollen Inhalten verbleiben sollten;
29. fordert die Kommission und die zuständigen Regulierungsbehörden auf, verdeckte Desinformationskampagnen, die darauf abzielen, generative KI-Systeme auszunutzen, einschließlich koordinierter Propagandanetzwerke und Netzwerke zur Manipulation von Narrativen, wie die Aktivitäten des in Moskau ansässigen Netzwerks „Prawda“ und die explizite Manipulation von Grok (xAI), systematisch zu untersuchen und diese Kampagnen auf solche Weise öffentlich bekannt zu machen, dass ihre Verbreitung nicht gefördert wird; betont, dass es wichtig ist, die genauen Verpflichtungen der Anbieter und Betreiber in Bezug auf die Kennzeichnungsanforderungen für durch KI erzeugte Inhalte gemäß Artikel 50 der Verordnung über künstliche Intelligenz und dem Verhaltenskodex zur Bekämpfung von Desinformation zu präzisieren und festzulegen, in welchem Umfang Endnutzer und Plattformen unter diesen Rahmen fallen; fordert Anbieter von KI-Systemen

nachdrücklich auf, dieses Phänomen durch ihre KI-Risikomanagementsysteme angemessen anzugehen und zu mindern; fordert darüber hinaus das Büro für Künstliche Intelligenz auf, seine Bemühungen um die Überwachung der Sicherheitslandschaft von KI-Modellen zu verstärken und zur Entwicklung von Methoden für KI, einschließlich großer Sprachmodelle (LLM), beizutragen, um für mehr Transparenz und die Wahrung der persönlichen Integrität beim Training von Datenquellen zu sorgen;

30. fordert die Kommission – wie bereits zuvor im Hinblick auf WhatsApp – auf, ihre Bewertung der Nutzerbasis und Funktionalität von Telegram gemeinsam mit der belgischen Regulierungsbehörde dringend abzuschließen, um über seine Einstufung als sehr große Online-Plattform im Rahmen des Gesetzes über digitale Dienste zu entscheiden und mögliche neue Beweise oder Änderungen beim Nutzerverhalten zu berücksichtigen; fordert die Kommission und die zuständigen Behörden nachdrücklich auf, die mögliche Rolle von Telegram bei der Erleichterung krimineller Aktivitäten, der Einflussnahme bei Wahlen und der Verbreitung von Desinformation sowie extremistischen und terroristischen Inhalten in der EU zu untersuchen und seine möglichen Verbindungen zu russischen Nachrichtendiensten sowie die Sicherheit seiner Server und Datenverarbeitungspraktiken zu klären; betont, dass alle verfügbaren Durchsetzungsmaßnahmen zu ergreifen sind, damit Telegram alle geltenden EU-Vorschriften in Bezug auf Transparenz, die Moderation von Inhalten und Datenzugang vollständig einhält, um gleiche Wettbewerbsbedingungen zu gewährleisten und das Vertrauen der Bürgerinnen und Bürger in den digitalen Informationsraum zu wahren; fordert Telegram ferner nachdrücklich auf, sich dem freiwilligen Verhaltenskodex zur Bekämpfung von Desinformation anzuschließen;
31. 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; begrüßt die Zusage der Kommission, die Rolle von Online-Influencern bei der anstehenden Bewertung der Richtlinie über audiovisuelle Mediendienste oder im Rahmen des bevorstehenden Rechtsakts über digitale Fairness zu bewerten; betont in diesem Zusammenhang, dass Leitlinien und strenge Standards für die Transparenz, auch bei durch Plattformen ermöglichter Finanzierung, von Vergütungs- und Sponsoringvereinbarungen, für die Unterscheidung zwischen Werbeinhalten und organischen Inhalten sowie für die 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 die Tätigkeit von Influencern verantwortungsvoller und transparenter zu machen; schlägt vor, dass ethische Standards und Verpflichtungen für Journalisten als Inspiration für die Ausarbeitung von Standards für Influencer dienen könnten; fordert die Kommission ferner auf, die Verordnung über die Transparenz und das Targeting politischer Werbung weiterhin durchzusetzen, insbesondere in Bezug auf Online-Plattformen, und Influencern die Einhaltung der Vorschriften über das geplante EU-Netz von Influencern zu erleichtern;

32. fordert nachdrücklich die Entwicklung von Reallaboren und Finanzierungsmechanismen zur Unterstützung von EU-Start-ups im Bereich Technologie und werteorientierten europäischen Alternativen auf der Grundlage einer fairen Vergütung, wie sie beispielsweise in den Niederlanden entstehen, um strategische Abhängigkeiten zu verringern; begrüßt die EU-Open-Source-Strategie der Kommission; unterstützt ferner die langfristige Vision von EU-Social-Media-Plattformen, die im Einklang mit den EU-Werten Transparenz, Datenschutz, Grundrechten, Meinungsfreiheit und demokratische Rechenschaftspflicht gestaltet sind;
33. betont, dass Werbepraktiken und Praktiken der Einnahmenteilung Anreize für die Verbreitung manipulativer oder schädlicher Inhalte schaffen, die Integrität von Wahlen untergraben und zum Aufkommen neuer Desinformationsakteure und -netzwerke führen können; weist darauf hin, dass Desinformation nicht entmonetarisiert werden kann, ohne dass die bestehenden Monetarisierungspraktiken hinreichend transparent sind; fordert die Kommission, die digitalen Regulierungsbehörden der EU, die zuständigen nationalen Behörden und Online-Plattformen auf, zusammenzuarbeiten, um illegale Finanzierung aufzudecken und zu verhindern und für Transparenz bei Programmen zur Umverteilung von Einnahmen, Werbestrategien und anderen Monetarisierungsdiensten zu sorgen, die es Akteuren im Bereich der ausländischen Informationsmanipulation und Einmischung oder sogar sanktionierten Einrichtungen ermöglichen könnten, Einnahmen oder andere Vorteile zu erzielen; fordert die Plattformen auf, die Vergütungsströme und ihre Begünstigten mindestens einmal jährlich offenzulegen; 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; ist der Ansicht, dass die Monetarisierung von Inhalten von sanktionierten Einrichtungen ein systemisches Risiko darstellt, das rasche Korrekturmaßnahmen wie die Aussetzung der Einnahmenteilung erfordert; betont, dass echte Urheber und Medienunternehmen im Falle einer irrtümlichen oder unfairen Entmonetarisierung für ihre Verluste entschädigt werden sollten; ist besorgt über die allmähliche Rücknahme der

Verpflichtungen von Unternehmen in Bezug auf Initiativen zur Freiheit des Internets;

34. nimmt mit Besorgnis die Feststellungen der niederländischen Datenschutzbehörde zur Kenntnis, die auf weitreichendere Bedenken in der gesamten EU schließen lassen, wonach KI-Chatbots voreingenommene und unzuverlässige Wahlempfehlungen geben können, wodurch die Integrität von Wahlen gefährdet wird; fordert das Büro für Künstliche Intelligenz auf, eine Untersuchung darüber durchzuführen, inwieweit solche Praktiken gegen geltendes Recht, insbesondere gegen die Verordnung über künstliche Intelligenz, verstoßen, und seiner Verpflichtung nachzukommen, Leitlinien für die Anwendung von KI in Wahlprozessen zu erstellen, um eine verantwortungsvolle Nutzung von KI sicherzustellen;

Meinungsfreiheit

35. 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 am stärksten geschützt werden und dass Unternehmen, die in der EU tätig sind und europäische Kunden anziehen möchten, gemeinsam für die Achtung und Wahrung dieser Rechte verantwortlich sind; betont daher, dass sehr große Online-Plattformen und sehr große Online-Suchmaschinen die weitreichenden gesellschaftlichen und demokratischen Folgen ihrer Dienste im Einklang mit dem Unionsrecht anerkennen und wirksam gegensteuern müssen, unter anderem durch solide systemische Maßnahmen im Bereich Risikobewertung und Risikominderung; stellt in diesem Zusammenhang fest, dass die Verstärkung bestimmter Inhalte oder Meinungen und das Unterdrücken anderer ein systemisches Risiko für den gesellschaftlichen Diskurs und Wahlprozesse oder für eine Verletzung der Meinungsfreiheit, insbesondere der Freiheit, Informationen und Ideen frei zu empfangen und weiterzugeben, darstellen können; fordert die Kommission auf, dafür zu sorgen, dass Plattformen diesbezüglich im Rahmen des Gesetzes über digitale Dienste zur Rechenschaft gezogen werden können; betont in diesem Zusammenhang, dass die EU weiterhin aktiv gegen falsche Narrative vorgehen muss, in deren Rahmen behauptet wird, dass ihre Rechtsvorschriften im Bereich Digitales und Demokratie die Meinungsfreiheit untergraben; betont, dass die Meinungs- und Informationsfreiheit so konzipiert wurde, dass sie den Menschen und nicht Maschinen oder Software schützt, die nicht authentisch agieren, wie KI und botbasierte Verstärkung und Steuerung sowie automatisierte Softwareprogramme, die repetitive Aufgaben über ein Netzwerk ausführen, um echte Nutzer nachzuahmen; betont ferner, dass das Bekenntnis zur Meinungsfreiheit nicht als Vorwand genutzt werden darf, um illegale Inhalte oder hybride Operationen autoritärer Regime zu tolerieren, die darauf abzielen, die EU und

ihre demokratischen Prozesse zu destabilisieren;

36. weist darauf hin, dass Online-Plattformen eine wesentliche Rolle dabei spielen, eine offene öffentliche Debatte, journalistische Tätigkeit und politischen Pluralismus zu ermöglichen; stellt daher fest, dass wirksame Schutzmaßnahmen für Nutzer bei der Ausübung ihrer demokratischen Rechte wichtig sind, darunter die Möglichkeit, Entscheidungen der Plattformen über die Moderation von Inhalten und die Monetarisierung, auch vor Verwaltungsbehörden und Justizbehörden, anzufechten, und die Verpflichtungen der Online-Plattformen, Nutzer zu informieren, wenn ihre Inhalte entfernt oder eingeschränkt werden, durchzusetzen; betont in diesem Zusammenhang, dass es wichtig ist, auf einen Zugang zu einer hochwertigen Moderation von Inhalten in allen europäischen Sprachen hinzuwirken; erinnert daran, dass Online-Plattformen gemäß dem Gesetz über digitale Dienste verpflichtet sind, zu diesem Zweck vollständig transparent zu agieren und einen gesonderten Mechanismus für die Bearbeitung von Beschwerden bereitzustellen und dafür zu sorgen, dass die Beschwerdemechanismen leicht zugänglich und benutzerfreundlich bleiben; stellt fest, dass nicht alle Online-Plattformen solche Mechanismen im Einklang mit den Bestimmungen des Gesetzes über digitale Dienste umgesetzt haben, und fordert die Kommission und die Mitgliedstaaten nachdrücklich auf, Durchsetzungsmaßnahmen vollständig umzusetzen; 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

37. ist der Ansicht, dass Maßnahmen zur Förderung und Unterstützung freier, glaubwürdiger und redaktionell unabhängiger Medien, einschließlich von Medien auf lokaler und regionaler Ebene, ein zentraler Bestandteil der Verwirklichung der Ziele des Europäischen Schutzschildes für die Demokratie sind; betont ferner, dass der Schutz des Mediensektors vor politischer, wirtschaftlicher oder struktureller Vereinnahmung eine Voraussetzung für die Sicherstellung der demokratischen Resilienz ist; stellt fest, dass der Schutz unabhängiger Medien für die Abwehr hybrider Bedrohungen durch feindselige Akteure von entscheidender Bedeutung ist; stellt in diesem Zusammenhang zudem fest, dass durch das derzeitige digitale Informationsumfeld häufig Medienakteure benachteiligt werden, die redaktionelle Verantwortung und Verpflichtungen im öffentlichen Interesse übernehmen, und stattdessen Intermediäre begünstigt werden, die keine vergleichbaren Pflichten haben; begrüßt die bahnbrechenden gemeinsamen Mindeststandards für Medienfreiheit und -pluralismus, die durch die Annahme des Europäischen Medienfreiheitsgesetzes eingeführt wurden; erinnert die Mitgliedstaaten an die darin enthaltenen Verpflichtungen, die Medien vor ungebührlichen Zusammenschlüssen auf dem

Medienmarkt zu schützen; weist jedoch darauf hin, dass die Bedeutung des Gesetzes nur anhand seiner Umsetzung in der Praxis beurteilt werden kann; fordert die Mitgliedstaaten auf, das Europäische Medienfreiheitsgesetz rasch umzusetzen, und fordert die Kommission auf, für eine konsequente Durchsetzung seiner Bestimmungen zu sorgen, einschließlich der Ergreifung von Maßnahmen, wenn Verpflichtungen, insbesondere sehr großer Online-Plattformen, mit denen redaktionelle Inhalte vor ungerechtfertigter Entfernung oder Einschränkung der Sichtbarkeit geschützt werden sollen, nicht eingehalten werden; begrüßt die neuen Verpflichtungen im Bereich Medienförderung, die im Rahmen des Programms für Medienresilienz angekündigt wurden, und fordert entsprechende langfristige Verpflichtungen im kommenden MFR; betont ferner, dass die Finanzierungskrise, mit der die europäischen Medien konfrontiert sind, darauf hindeutet, dass neue Finanzierungslösungen geprüft werden müssen;

38. betont, dass die potenziellen Auswirkungen der EU-Initiativen auf den Journalismus und die redaktionellen Medien sorgfältig geprüft werden müssen, insbesondere im Hinblick auf die Sicherung des Medienpluralismus und der Nachhaltigkeit der Geschäftsmodelle von Medienunternehmen; fordert, dass im Vorfeld von Initiativen, die sich auf die Rentabilität europäischer Medienunternehmen auswirken können, evidenzbasierte Folgenabschätzungen und eine angemessene Konsultation der Interessenträger im Medienbereich durchgeführt werden; betont in diesem Zusammenhang, dass es wichtig ist, die Entwicklungen zu überwachen, die sich auf die Medienfreiheit und den Medienpluralismus in der gesamten EU auswirken, und betrachtet den jährlichen Bericht über die Rechtsstaatlichkeit mit seinem Kapitel über Medienfreiheit und Medienpluralismus als zentrales Instrument bei diesen Bemühungen; fordert die Kommission auf, diese Säule des Berichts weiter zu entwickeln, um neue Herausforderungen besser zu erfassen;
39. betont in Bezug auf Medienunternehmen, die Abonnements über Apps anbieten, dass es wichtig ist, das Gesetz über digitale Märkte vollständig umzusetzen und wirksam durchzusetzen; nimmt den Beschluss der Kommission vom 23. April 2025 über Verstöße durch Apple und Meta sowie die laufenden Untersuchungen der Kommission zu einem potenziellen Verstoß gegen das Gesetz über digitale Märkte durch Google aufgrund der Herabstufung der Inhalte von Medienverlagen in Suchergebnissen zur Kenntnis; betont, dass die strikte und zeitnahe Durchsetzung des Gesetzes über digitale Märkte von entscheidender Bedeutung ist, um Fairness, Bestreitbarkeit und Pluralismus im digitalen Umfeld der EU sicherzustellen und gegen strukturelle Abhängigkeiten und Marktkonzentrationen vorzugehen, auch im Zusammenhang mit KI-gestützten Diensten;
40. 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 Sachverständigengruppe „Medienkompetenz“, einschließlich der Einrichtung eines neuen Expertennetzes für Medienkompetenz, sowie aktualisierte Leitlinien für Lehrkräfte und pädagogische Fachkräfte; weist darauf hin, dass die derzeitigen Initiativen zur Medienkompetenz in der EU nach wie vor fragmentiert sind; fordert kohärentere, EU-weite Ansätze und die Prüfung ergänzender Maßnahmen, einschließlich der Schaffung digitaler Instrumente und Plattformen auf EU-Ebene; spricht sich für den systematischen Austausch bewährter Verfahren zwischen nationalen Behörden aus, unter anderem im Rahmen der verstärkten Expertengruppe für Medienkompetenz und die Europäische Beobachtungsstelle für digitale Medien; hebt ferner die Rolle der kulturellen Bildung bei der Stärkung der demokratischen Kompetenz und der Widerstandsfähigkeit gegen Desinformation hervor; 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; betont, dass es wichtig ist, im Rahmen umfassenderer Bemühungen um Medienkompetenz und digitale Kompetenz ein kritisches Verständnis von KI-generierten Inhalten zu fördern;

41. begrüßt die angekündigte Aktualisierung der Empfehlung der Kommission zur Sicherheit von Journalisten⁶² und die bevorstehende Überprüfung der Empfehlung zur Bekämpfung von SLAPP-Klagen⁶³; betont, dass bei diesen Aktualisierungen und Überprüfungen der sich wandelnden und wiederkehrenden Seite von Bedrohungen, Gewalt, Sabotage und anderen Maßnahmen Rechnung getragen werden muss, die darauf abzielen, die journalistische Arbeit zu behindern, einschließlich neuer Herausforderungen wie Identitätsdiebstahl und koordinierter Deepfake-Kampagnen, die die Sicherheit und Unabhängigkeit von Journalisten gefährden können; betont, dass den erschreckenden Auswirkungen, die durch ein anhaltendes Klima der Angst, politischen Drucks oder unzulässiger Einmischung durch öffentliche oder private Akteure entstehen, besondere Aufmerksamkeit gewidmet werden sollte; fordert die

⁶² 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>).

⁶³ 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>).

Mitgliedstaaten auf, im Einklang mit ihren nationalen Rechtsrahmen und bewährten Verfahren die Einführung bestimmter erschwerender Umstände im Strafrecht für Straftaten zu prüfen, die gegenüber Journalisten begangen werden, wenn diese Handlungen durch deren berufliche Tätigkeit motiviert sind oder damit in Zusammenhang stehen; stellt ferner fest, dass es wichtig sein könnte, Unterstützungsmaßnahmen zu entwickeln, um Journalisten beim Umgang mit neu auftretenden Problemen wie Identitätsbetrug mithilfe von KI und Deepfake-Inhalten zu unterstützen;

42. betont, dass Journalisten vor missbräuchlichen Klagen geschützt werden müssen; begrüßt in diesem Zusammenhang die Annahme der Richtlinie zur Bekämpfung von SLAPP-Klagen 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 und vorrangig für die vollständige und fristgerechte Umsetzung der Richtlinie zu sorgen; fordert die Kommission auf, einen umfassenden Evaluierungsbericht über die Erfolge der Umsetzung auszuarbeiten; fordert die EU und die Mitgliedstaaten ferner auf, zusätzliche Maßnahmen zur Ergänzung der Richtlinie in Erwägung zu ziehen, um Journalisten zu schützen, die investigativ tätig sind, insbesondere in grenzüberschreitenden oder sensiblen Kontexten; hebt in diesem Zusammenhang die laufende Diskussion über die Schaffung eines europäischen Schutzstatus für investigative Journalisten als einen möglichen Weg hervor, den es zu prüfen gilt;
43. erkennt die wesentliche Rolle der öffentlich-rechtlichen Medien an, wenn es darum geht, sicherzustellen, dass alle Bürgerinnen und Bürger, auch diejenigen in abgelegenen Gemeinschaften und Bewerberländern oder diejenigen, die Minderheiten angehören, über verschiedene Plattformen sowie in verschiedenen Formaten und Sprachen Zugang zu zuverlässigen, unparteiischen und vielfältigen Nachrichten haben, wodurch das Problem von Nachrichtenwüsten angegangen wird; betont ferner, dass der Zugang zu hochwertigen und verlässlichen Informationen für die Bekämpfung von Fehlinformationen und Desinformation von entscheidender Bedeutung ist; bekräftigt, dass der Schutz der öffentlich-rechtlichen Medien vor politischer Einflussnahme und Vereinnahmung von grundlegender Bedeutung ist, um die demokratische Rechenschaftspflicht und die Rechtsstaatlichkeit zu wahren; betont, dass die Glaubwürdigkeit der öffentlich-rechtlichen Medien im Einklang mit Artikel 5 des Europäischen Medienfreiheitsgesetzes von der vollständigen redaktionellen und organisatorischen Autonomie abhängt, und fordert die Kommission auf, Bedrohungen der Unabhängigkeit der öffentlich-rechtlichen Medien aktiv zu überwachen und wirksame Maßnahmen gegen Praktiken zu ergreifen, die die Medienfreiheit beeinträchtigen; stellt in diesem Zusammenhang fest, dass Versuche, die Unabhängigkeit der

öffentlich-rechtlichen Medien zu untergraben, frühe Indikatoren für demokratische Rückschritte sein können;

44. betont besonders, dass sichergestellt werden muss, dass Journalisten und andere Medienakteure bestmöglich vor rechtswidriger Spyware, intrusiven Überwachungstechnologien und anderen Formen digitaler Bedrohungen geschützt werden; weist darauf hin, dass es den Mitgliedstaaten gemäß dem Europäischen Medienfreiheitsgesetz streng untersagt ist, intrusive Überwachungssoftware auf Materialien, digitalen Geräten, Maschinen oder Werkzeugen einzusetzen, die von Mediendienstleistern oder ihrem redaktionellen Personal verwendet werden, mit Ausnahme von Fällen im Zusammenhang mit der nationalen Sicherheit; betont zudem, dass die Überwachung von Journalisten in die in den Artikeln 7, 8 und 11 der Charta der Grundrechte der Europäischen Union garantierten Rechte eingreift; stellt fest, dass der Einsatz von Spähsoftware die Arbeit von Journalisten gefährdet, indem das Vertrauen ihrer Quellen in sie untergraben wird, und dass das Versäumnis, EU-Rechtsvorschriften wirksam durchzusetzen, eine ernsthafte Bedrohung für die Informationsfreiheit darstellt;
45. bekräftigt, wie wichtig Transparenz, fairer Wettbewerb und die Nachhaltigkeit der europäischen redaktionellen Medien innerhalb des bestehenden Rechtsrahmens, einschließlich des Gesetzes über digitale Dienste, des Gesetzes über digitale Märkte, des Europäischen Medienfreiheitsgesetzes und der Verordnung über die Transparenz und das Targeting politischer Werbung, sind; stellt fest, dass mit diesen Instrumenten gegen Manipulation, Einflussnahme aus dem Ausland und wettbewerbswidrige Praktiken vorgegangen wird und gleichzeitig die redaktionelle Verantwortung und die freie Meinungsäußerung gewahrt werden; fordert die Kommission auf, zu prüfen, wie diese Instrumente am besten für diese Zwecke eingesetzt werden können; fordert sehr große Online-Plattformen und sehr große Online-Suchmaschinen auf, rechtmäßige europäische redaktionelle Medieninhalte nicht ungerechtfertigt aus dem Verzeichnis zu streichen, herabzustufen oder auf andere Weise deren Sichtbarkeit und faire Einstufung zu beeinträchtigen und dafür zu sorgen, dass die Einstufungssysteme transparent und diskriminierungsfrei bleiben;
46. fordert die Kommission auf, weitere Maßnahmen zur Verbesserung der Wettbewerbsfähigkeit, Zugänglichkeit und Fairness in der Online-Werbung für alle Akteure der Wertschöpfungskette, einschließlich der redaktionellen Medien, zu prüfen und gegebenenfalls in Erwägung zu ziehen; stellt fest, dass redaktionell unabhängiger, hochwertiger und faktenbasierter Journalismus mit Herausforderungen konfrontiert ist, die von interaktionsgesteuerten Empfehlungssystemen und KI-basierten Suchfunktionen sehr großer Online-Plattformen ausgehen, die die Sichtbarkeit hochwertiger Inhalte verringern und die Zugriffe auf Websites von Medien

begrenzen; stellt mit Besorgnis fest, dass die Zugriffszahlen im Zusammenhang mit der Einführung von KI-Zusammenfassungen von Google zurückgegangen sind, in einem untersuchten Fall sogar bis zu 70 %; fordert Anreize für Werbetreibende, vertrauenswürdige europäische Medien zu unterstützen, die Verwendung kontextbezogener Werbung anstelle von verhaltensorientiertem Targeting sowie eine stärkere Rückverfolgbarkeit und Transparenz in der Lieferkette für Online-Werbung, um Marktverzerrungen zu bekämpfen und böswillige Akteure daran zu hindern, Desinformationsinhalte zu monetarisieren und die Gesellschaft in der EU gezielt zu destabilisieren; fordert die Kommission in diesem Zusammenhang auf, mögliche Maßnahmen zur Förderung der Entwicklung und Nutzung der europäischen Infrastruktur für kontextbezogene Online-Werbung zu prüfen;

47. begrüßt die kürzlich angenommene Verordnung über ausländische Direktinvestitionen⁶⁴, 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; betont in diesem Zusammenhang, dass Investitionen in europäische Nachrichtenunternehmen transparenter gestaltet sein müssen; weist ferner darauf hin, dass audiovisuelle Medien mit Sitz in der EU strengeren Anforderungen unterliegen als Medien mit Sitz außerhalb der EU, die Zielgruppen in der EU über andere Verbreitungswege zur Verfügung stehen; betont, dass sichergestellt sein muss, dass Medien, die für Zielgruppen in der EU zugänglich sind, Standards für faire und pluralistische Informationen einhalten;
48. 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, unter anderem durch den Einsatz des Instruments „Europa in der Welt“; begrüßt die Soforthilfe der EU für RFE/RL; fordert die Ausarbeitung einer Lösung, um RFE/RL mit einer stabilen, langfristigen Finanzierung auszustatten; fordert die Kommission auf, neue Wege zur Unterstützung freier und redaktionell unabhängiger Medien in der Nachbarschaft der EU auszuloten, insbesondere in Regionen, die unverhältnismäßig stark von russischer

⁶⁴ 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>).

Desinformation und Propaganda betroffen sind, wie dem Westbalkanraum;

49. betont, dass gesellschaftsbasierte, unabhängige Faktenprüfnetzwerke bei der Aufdeckung und Bekämpfung von Desinformationskampagnen mitwirken und wertvolle Erkenntnisse für Risikobewertungen und -minderung im Rahmen der Verordnung über digitale Dienste liefern können; hält fest, dass unabhängige Faktenprüforganisationen für ihre Arbeit technische Unterstützung und gleichbleibende Bedingungen benötigen; ist der Ansicht, dass das von der Kommission 2025 angekündigte Europäische Netz von Faktenprüfern ein nützliches Instrument sein könnte, um das zu erreichen; betont, dass Faktenprüforganisationen strenge Standards hinsichtlich politischer Neutralität, Unabhängigkeit von den Anbietern von Online-Plattformen und methodischer Objektivität einhalten müssen, um vertrauenswürdig und überzeugend zu sein; betont den Stellenwert der Zusammenarbeit zwischen Faktenprüfern, OSINT-Rechercheuren, Journalisten, Kommunikationsbeauftragten und politischen Entscheidungsträgern; hebt außerdem hervor, dass es wichtig ist, Netzwerke von Faktenprüfern in Bewerberländern und möglichen Bewerberländern zu unterstützen;

Zivilgesellschaft, akademisches Umfeld, Kultur und Bürgerbeteiligung

50. betont, dass eine aktive, dynamische und unabhängige Zivilgesellschaft als einer der Grundpfeiler bei der Verteidigung unserer Demokratie eine entscheidende Rolle spielt, und zwar nicht nur indem sie böswillige Einflussnahme auf demokratische Prozesse als wachsame Instanz aufdeckt und aktiv bekämpft, sondern auch indem sie als elementare Kraft bei den langfristigen Bemühungen um den Aufbau stärkerer und widerstandsfähigerer Gesellschaften mitwirkt; hebt insbesondere hervor, dass die Zivilgesellschaft einen wichtigen Beitrag zur Wahrung der in Artikel 2 EUV verankerten Werte leistet;
51. begrüßt die EU-Strategie für die Zivilgesellschaft der Kommission, die zusammen mit der Gemeinsamen Mitteilung über den Europäischen Schutzschild für die Demokratie veröffentlicht wurde; begrüßt den Ansatz der Kommission, diese Strategie mit ihrer Arbeit am Europäischen Schutzschild für die Demokratie zu verknüpfen und damit das bürgerschaftliche Engagement weiter zu stärken; hält die Strategie für einen wichtigen ersten Schritt, da sie den ersten umfassenden Ansatz der EU für die Zivilgesellschaft darstellt, stellt jedoch fest, dass die nächsten Schritte einen ambitionierteren Ansatz umfassen müssen, der Maßnahmen zur effektiven Wahrung der Rolle der Zivilgesellschaft in demokratischen Prozessen einschließt; betont, dass künftige Initiativen in diesem Bereich auf das Schrumpfen des zivilgesellschaftlichen Raums reagieren sollten,

wobei auch anzuerkennen ist, dass Organisationen der Zivilgesellschaft und Menschenrechtsverteidiger besonders gefährdet sind, und betont, dass dies insbesondere für Organisationen gilt, die sich mit bestimmten Themen wie LGBTIQ+, Gleichstellung der Geschlechter und Bekämpfung von Rassismus befassen;

52. 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 möglicherweise einen Beitrag zur Koordinierung der Aktivitäten von Organisationen der Zivilgesellschaft im Bereich des Schutzes der Demokratie und der Bekämpfung von hybriden Bedrohungen, von ausländischer Informationsmanipulation und Einmischung und von transnationaler Repression leistet und das Situationsbewusstsein verbessert; betont in diesem Zusammenhang den Stellenwert von auf die Diaspora ausgerichtetem bürgerschaftlichem Engagement; weist ferner darauf hin, dass Teile der Zivilgesellschaft über umfassende Erfahrungen mit Einflussnahme aus dem Ausland verfügen und im Rahmen des zivilgesellschaftlichen Dialogs in die Gestaltung der diesbezüglichen Politik einbezogen werden sollten;
53. hebt die Rolle und Verantwortung hervor, die die Zivilgesellschaft in demokratischen Prozessen in den Bewerberländern übernommen hat; fordert die Kommission auf, mit zivilgesellschaftlichen Organisationen aus Bewerberländern und möglichen Bewerberländern über gegenwärtige und künftige Initiativen im Rahmen der EU-Strategie für die Zivilgesellschaft in Austausch zu treten, insbesondere mit jenen Organisationen, die sich konsequent für die Förderung der digitalen Angleichung, der Informationsintegrität, der Integrität von Wahlen und der demokratischen Resilienz einsetzen;
54. fordert die Mitgliedstaaten auf, für Organisationen der Zivilgesellschaft eine nachhaltige und diversifizierte Finanzierung, die dauerhafte operative Unterstützung und Maßnahmen zum Kapazitätsaufbau umfasst, sicherzustellen und dabei ihre wesentliche Rolle bei der Wahrung demokratischer Werte anzuerkennen und dafür zu sorgen, dass sie effektiv und unabhängig arbeiten können; betont, dass konkrete EU-Finanzierungsprogramme wie das Programm „Bürgerinnen und Bürger, Gleichstellung, Rechte und Werte“ (CERV) wichtig sind, um diese Bemühungen zu ergänzen; begrüßt, dass die Kommission beabsichtigt, das CERV-Programm beizubehalten, indem es in das neue Programm AgoraEU für den Zeitraum 2028-2034 eingebunden wird; fordert die

gesetzgebenden Organe auf, dafür Sorge zu tragen, dass umfangreiche und berechenbare Mittel für diesen Aktionsbereich von AgoraEU zur Verfügung stehen, die den Bedürfnissen der Organisationen der Zivilgesellschaft entsprechen und in direkter Mittelverwaltung durch die Kommission ausgeführt werden;

55. betont, dass Kultur eine strategische Säule des europäischen Projekts ist, da kulturelle Freiheit, kulturelles Erbe und Kreativität demokratische Teilhabe, kritisches Denken und Vertrauen in die Institutionen fördern; unterstreicht, dass Programme wie AgoraEU eine Schlüsselrolle bei der Umsetzung dieser Werte in konkrete Unterstützung spielen können; stellt mit Besorgnis fest, dass Angriffe auf die liberale Demokratie zunehmend gegen kulturelle Akteure und Einrichtungen gerichtet sind, insbesondere in Form von politischem Druck unterschiedlicher Ausprägung; betont daher, dass der Erhalt der künstlerischen Freiheit und von Kultureinrichtungen für die Verteidigung der Demokratie in der EU unverzichtbar ist;
56. hebt hervor, dass es wichtig ist, die kulturelle Geschichte und das kollektive Gedächtnis Europas zu bewahren und der Manipulation und Fälschung historischer Fakten entgegenzuwirken, um die demokratische Resilienz zu stärken; betont in diesem Zusammenhang, dass eine gemeinsame europäische Erinnerungskultur gestärkt werden muss, und bekräftigt, dass es eine gesamteuropäische Gedenkstätte für die Opfer totalitärer Regime des 20. Jahrhunderts sowie einen Bericht der Kommission über das europäische Gedenken bis Anfang 2027 befürwortet; verurteilt den Geschichtsrevisionismus des russischen Regimes und dass dieses verzerrte Narrative einsetzt, um die Souveränität ehemals unterjochter Nationen zu leugnen und eine Einflussnahme von außen zu rechtfertigen;
57. weist darauf hin, dass verschiedene Interessenvertreter, darunter Organisationen der Zivilgesellschaft, Thinktanks und Dachverbände, von böswilligen Akteuren aus Drittländern als Vehikel unrechtmäßiger Einflussnahme auf demokratische Prozesse in der EU und ihren Mitgliedstaaten genutzt werden können und bereits genutzt wurden; unterstreicht, dass Maßnahmen für finanzielle Transparenz – wenn sie angemessen konzipiert sind und mit Schutzmaßnahmen entsprechend der Größe der Organisationen einhergehen – dazu beitragen können, das Risiko künftiger unzulässiger Einflussnahme durch autoritäre Staaten zu mindern; betont, dass das Parlament als Organ eine besondere Verantwortung für die Stärkung der Standards in Bezug auf Integrität, Transparenz und Rechenschaftspflicht trägt, insbesondere angesichts der Lehren, die aus früheren Fällen von Korruption und ausländischer Einflussnahme gezogen wurden; hebt jedoch hervor, dass Maßnahmen zur Auseinandersetzung mit dieser Frage so konzipiert sein sollten, dass sie nicht dazu missbraucht werden können, die rechtmäßigen Aktivitäten der Zivilgesellschaft und deren

maßgebliche Rolle bei der Stärkung unserer Demokratien zu stigmatisieren;

58. betont den Stellenwert des Vorschlags der Kommission für eine Richtlinie über die Interessenvertretung im Auftrag von Drittländern, die einen zentralen 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; unterstreicht, dass gemeinsame diesbezügliche Vorschriften zu Rechenschaftspflicht und Vertrauen in die Entscheidungsfindung der EU beitragen können, indem sie Transparenz in Bezug auf die Einflussnahme von Drittländern schaffen; fordert die gesetzgebenden Organe auf, das Gesetzgebungsverfahren unverzüglich abzuschließen; betont, dass die Mitgliedstaaten sicherstellen sollten, dass die Einhaltung dieser Richtlinie nicht zu einer Einschränkung der Grundrechte führt;
59. 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 wirkungsvolle Kommunikation zu sorgen, wenn es um die Initiativen geht, die sie erarbeitet, um die Nutzung von Instrumenten zur Bürgerbeteiligung, die zugänglich, nutzerfreundlich, mehrsprachig und so konzipiert sind, dass sie weite Kreise von Bürgerinnen und Bürgern erreichen, zu fördern und auszuweiten; 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; betont in diesem Zusammenhang, dass junge Menschen aktiv in das demokratische Leben einbezogen werden müssen, und würdigt, dass sie wichtige Akteure bei der Stärkung der Bürgerbeteiligung und der politischen Teilhabe sind, unter anderem durch die Entwicklung partizipativer digitaler Plattformen und von Jugendräten, um für eine substanzielle Beteiligung an Entscheidungsprozessen auf lokaler, nationaler und EU-Ebene zu sorgen;
60. hebt hervor, dass die akademische Freiheit, einschließlich der Freiheit der Forschung, der Lehre und der wissenschaftlichen Meinungsäußerung, eine tragende Säule demokratischer Gesellschaften ist; verurteilt Angriffe auf die akademische Freiheit und betont, dass die Unabhängigkeit der europäischen Forschung und ihre Widerstandsfähigkeit gegenüber Einflussnahme aus dem Ausland gestärkt werden müssen; warnt insbesondere vor der Geschichtsmanipulation durch externe Akteure; fordert die Kommission erneut auf, einen Legislativvorschlag zum Schutz der Grundfreiheit der wissenschaftlichen Forschung vorzulegen, der Mindeststandards für die Rechte, das ethische Verhalten, die Integrität und die institutionelle Unabhängigkeit von Forschenden

beinhaltet und durch wirksame Überwachungsmechanismen gestützt ist;

Schutz kritischer Infrastruktur

61. vertritt den Standpunkt, dass der Schutz der EU und ihrer Mitgliedstaaten vor physischen und Cybersabotageakten gegen kritische Infrastruktur ein wesentlicher Aspekt der Wahrung der demokratischen Resilienz ist; fordert eine proaktive Strategie zur Abwehr von Bedrohungen, die Einführung solider Präventivmaßnahmen, eine verstärkte grenzüberschreitende Zusammenarbeit und eine verbesserte Fähigkeit der EU, derartige feindselige Aktivitäten aufzudecken, zu verhindern und auf sie zu reagieren; betont, dass ausländisches, in Verbindung mit dem Staat stehendes Eigentum an kritischer Infrastruktur eine größere Gefährdung aufgrund von Sicherheitsrisiken bedeutet und verstärkte Kontrolle rechtfertigt, insbesondere in Bezug auf Kommunikationsinfrastruktur, digitale Infrastruktur, Unterseekabel, Energieinfrastruktur, Verkehrsknotenpunkte, Krankenhäuser und Infrastruktur für öffentliche Dienstleistungen;
62. 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, Häfen, Militärstützpunkte, Industriecluster, Grenzschutzinfrastruktur 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; fordert die Kommission und die Mitgliedstaaten nachdrücklich auf, an Programmen für den Wissenstransfer mit der Ukraine und an der gemeinsamen Ausbildung und Zertifizierung von Drohnenpiloten angesichts des in der Ukraine erworbenen Wissens über die Umsetzung einer modernen Kriegsführung zu arbeiten;
63. betont, dass die EU-Agenturen bei der Gewährleistung des Schutzes grenzüberschreitender kritischer Infrastruktur in der EU und ihren Mitgliedstaaten eine strategische Rolle übernehmen und dass es erforderlich ist, die Zusammenarbeit in Bezug auf Seehäfen, Flughäfen und Landgrenzübergänge zu stärken, unter anderem durch gemeinsame Schwachstellenbeurteilungen; weist insbesondere auf Bedrohungen durch GPS-Störung und Spoofing durch Russland und Belarus hin und darauf, dass diese potenziell das Funktionieren kritischer Infrastruktur behindern, die Schiffsverkehrssicherheit gefährden und die Kontinuität und Resilienz wesentlicher grenzüberschreitender Dienste beeinträchtigen können;
64. 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; hält fest, dass Russland anfällig für Cyberangriffe ist, wie der Hackerangriff auf die russische Fluggesellschaft Aeroflot durch Cyber Partisans gezeigt hat; unterstreicht, dass die Ukraine über umfangreiche Erfahrungen in Bezug auf die Schwächung der russischen Fähigkeiten verfügt und dass die Unterstützung für die Ukraine zur Stärkung ihrer offensiv ausgerichteten Cyberfähigkeiten schneller bereitgestellt werden muss;

65. betont, dass die grenzüberschreitende Koordinierung bei der Abwehr hybrider Bedrohungen in Meeresgebieten weiter intensiviert und durch zweckgebundene und angemessene EU-Mittel gestützt werden sollte und dass die EU ihre operative Reaktion verstärken muss, insbesondere mit Blick auf Bedrohungen im Zusammenhang mit der russischen Schattenflotte; fordert die Kommission und die Mitgliedstaaten in dieser Hinsicht auf, für eine koordinierte, EU-weite Auslegung des Seerechtsübereinkommens der Vereinten Nationen (SRÜ) zu sorgen, um ein kohärentes Vorgehen gegen hybride Aktivitäten, Sabotageakte, illegale, ungemeldete und unregulierte Fischerei und Verletzungen der Hoheitsrechte in den Meeresgebieten der EU, insbesondere in der Ostsee, sicherzustellen, und weist gleichzeitig darauf hin, dass der Zweck des SRÜ die Sicherstellung der friedlichen Nutzung der Meere ist; begrüßt außerdem die Empfehlung der Kommission über sichere und resiliente Seekabelinfrastrukturen⁶⁵ und den EU-Aktionsplan für Kabelsicherheit; fordert die Kommission und die Mitgliedstaaten nachdrücklich auf, die Umsetzung dieser Initiativen zu beschleunigen, indem sie die Kabelinfrastruktur erfassen, koordinierte Risikobewertungen und Stresstests entwickeln, Abhilfemaßnahmen ergreifen und die Reaktions- und Reparaturkapazitäten bei Sicherheitsvorfällen stärken, und zwar unter anderem indem sie modulare Reparaturausrüstung fördern

⁶⁵ Empfehlung (EU) 2024/779 der Kommission vom 26. Februar 2024 über sichere und resiliente Seekabelinfrastrukturen (ABl. L, 2024/779, 8.3.2024, ELI: <http://data.europa.eu/eli/reco/2024/779/oj>).

und strategische Lagerbestände an essenziellen Ersatzteilen halten;

66. fordert, dass hybride Aktivitäten und Sabotageakte, einschließlich Angriffen auf Seekabel und -verbindungen, wirksam unter Strafe gestellt werden und diesbezügliche Abschreckung erfolgt; fordert die Kommission und die Mitgliedstaaten auf, vom Beispiel Australiens zu lernen, das „Kabelschutzzonen“ eingerichtet, rechtliche Schutzmaßnahmen ergriffen und die Beschädigung von Seekabeln außerhalb der Hoheitsgewässergrenze von 12 Seemeilen unter Strafe gestellt hat, was von einer aktiven Beobachtung, Überwachung und Reaktion in Zusammenarbeit mit den relevanten Partnern aus Drittländern flankiert wird;
67. fordert die Mitgliedstaaten auf, die Nutzung des Mandats der Sicherheitsinitiative zur Unterbindung der Verbreitung von Massenvernichtungswaffen zu prüfen, um an Bord von Schiffen zu gehen, die mit Schattenflotten in Verbindung stehen, und fordert die Arbeitsgruppe „Bekämpfung der Geldwäsche und der Terrorismusfinanzierung“ auf, im Rahmen ihrer gegenseitigen Evaluierung und ihrer Verfahren zur Aufnahme in die Graue Liste eine aktivere Rolle bei der Prüfung der Governance der Flaggenreister zu übernehmen;
68. bekräftigt seine Forderung nach der Einrichtung europäischer Plattformen für maritime Sicherheit im Schwarzen Meer, in der Nordsee und in der Ostsee als Reaktion auf den Angriffskrieg Russlands gegen die Ukraine und hebt hervor, dass solche Knotenpunkte die maritime Lageerfassung verbessern, eine Echtzeitüberwachung vom Weltraum bis zum Meeresboden ermöglichen und die Frühwarnkapazitäten sowie die Reaktionen auf die zunehmende Bedrohung durch die russische Schattenflotte stärken sollten, wobei Umweltaspekte einzubeziehen sind und für die Sicherheit der Handelswege zu sorgen ist; fordert die Kommission und die Mitgliedstaaten auf, zu verhindern, dass die Schattenflotte in europäische Gewässer eindringt, und häufige und sorgfältige Kontrollen durchzuführen, um sicherzustellen, dass die Schattenflotte keine Rechtsvorschriften verletzt und keine Gefahr von ihr ausgeht;
69. betont nachdrücklich, dass bestehende strukturelle Abhängigkeiten durch Marktkonzentration und ausländische Kontrolle, einschließlich der Dominanz US-amerikanischer Big-Tech-Unternehmen, bei der digitalen Infrastruktur der EU und bei Betriebssystemen, Rechenzentren, Halbleiterherstellung, KI, datengesteuerten Tools zur Entscheidungsfindung, Zahlungsinfrastruktur, Cybersicherheit, Cloud-Computing und verschiedenen Online-Plattformen und -Diensten ein hohes Risiko für Demokratie, Freiheit, Sicherheit und Wettbewerbsfähigkeit in der EU bergen; bedauert die jüngsten Vorfälle, bei denen Microsoft, Visa und Mastercard ihre Dienste ausgesetzt und die Transaktionen von Mitarbeitenden des

Internationalen Strafgerichtshofs, die von den USA mit Sanktionen belegt wurden, blockiert haben; hebt in diesem Zusammenhang hervor, dass die EU durch derartige Entscheidungen von außen gefährdet ist, da diese öffentliche Dienstleistungen und Wirtschaftstätigkeiten stören könnten; fordert die Kommission auf, den Abbau von Abhängigkeiten und den Aufbau europäischer industrieller Kapazitäten systematisch in die Umsetzung des Europäischen Schutzschildes für die Demokratie einzubeziehen;

70. hält eine widerstandsfähige, wettbewerbsfähige digitale Infrastruktur der EU – die auch sichere lokale Rechenzentren, eine souveräne Cloud der EU, Edge-Computing-Kapazitäten und Gigabit-Netze umfasst – für eine strategische Säule der digitalen Resilienz, mit der für Offenheit, Wettbewerb und globale Interoperabilität gesorgt wird; betont, dass diese Infrastruktur dazu beitragen sollte, die sensiblen Daten der EU-Bürgerinnen und -Bürger zu schützen, wenn es um Risiken im Zusammenhang mit der Speicherung im Ausland und die Gefahr, Rechtsvorschriften von Drittländern zu unterliegen, geht, und der Komplexität im Zusammenhang mit ausländischem Eigentum und Investitionen in wesentliche Infrastrukturen zu begegnen, und zwar unter anderem durch Belastungstests hinsichtlich digitaler Autonomie, um Abhängigkeiten von großen kommerziellen Technologieunternehmen bei grundlegenden öffentlichen Dienstleistungen zu erfassen; bedauert, dass das europäische System für die Cybersicherheitszertifizierung von Cloud-Diensten (EUCS) nach sechs Jahren Ausarbeitungsphase immer noch keine Zertifizierung mit einer Vertrauenswürdigkeitsstufe bieten kann, die es europäischen Cloud-Anbietern erlauben würde, den größtmöglichen Schutz strategischer Daten vor nichteuropäischen Rechtssystemen zu garantieren, und betont, dass eine solide Cybersicherheitszertifizierung für die Integrität und Resilienz digitaler Dienste, die demokratischen Prozessen zugrunde liegen, unerlässlich ist; unterstreicht, dass angesichts des Rechtsakts über Cloud- und KI-Entwicklung und des überarbeiteten Rechtsakts zur Cybersicherheit die Arbeit am EUCS wieder aufgenommen werden sollte; begrüßt die Einführung gestaffelter EU-Vertrauenswürdigkeitsstufen in dem Vorschlag für den Rechtsakt über Cloud- und KI-Entwicklung und fordert ein Höchstmaß an Sicherheit, um einen wirksamen Schutz der sensibelsten und strategisch wertvollsten Daten vor dem Zugriff aus Drittländern, die anderen Rechtssystemen unterliegen, zu gewährleisten und gleichzeitig unnötige Hindernisse für Innovation und Investitionen zu vermeiden;
71. betont, dass Risiken angegangen werden müssen, die im Zusammenhang mit strategischen und sensiblen vernetzten Hardware- und Softwarekomponenten und -diensten stehen, über die ein Fernzugriff, eine Datenübertragung oder eine Systemsteuerung erfolgen können und die aus Drittländern mit hohem Risiko, darunter China, stammen; nimmt mit Besorgnis zur Kenntnis, dass Risiken in

Verbindung mit der Dominanz chinesischer Solarwechselrichter und anderer Komponenten bestehen, die in bestimmten Fällen über staatlich unterstützte, nicht marktorientierte Praktiken zu künstlich niedrigen Preisen auf dem EU-Markt in Verkehr gebracht werden; begrüßt in diesem Zusammenhang die Tatsache, dass der überarbeitete Rechtsakt zur Cybersicherheit in der vorgeschlagenen Fassung darauf abzielt, einen Rahmen für das Verbot vernetzter Komponenten wie Wechselrichter, mit denen ein Fernzugriff durch Hochrisikoanbieter möglich ist, zu schaffen, und dass der Strategische Fahrplan für Digitalisierung und KI im Energiesektor eine Risikobewertung für Solaranlagen und eine Überprüfung des Rahmens für die Energieversorgungssicherheit vorsieht; fordert die rasche Annahme dieser Maßnahmen, um kritische Energieinfrastruktur vor Manipulation über Fernzugriff, Stromausfällen und Risiken in der Lieferkette zu schützen; fordert die Kommission und die Mitgliedstaaten auf, sichere, in der EU ansässige und in der EU hergestellte Alternativen zu fördern, die derzeitigen Vergabevorschriften zu prüfen, um zu beurteilen, ob sie die digitale Souveränität behindern, und eine umfassende EU-Agenda für technologische Souveränität mit klaren Resilienzstandards und -kriterien für die Entwicklung bzw. Beschaffung von Technologie oder digitaler Infrastruktur zu verfolgen, wobei sichergestellt sein sollte, dass die Regelungsrahmen und die handels- und wettbewerbspolitischen Maßnahmen unlautere Marktpraktiken effektiv unterbinden und die Abhängigkeit von Anbietern aus Drittländern verringern; betont, dass der digitale Erfolg von Wettbewerb, Offenheit und technologischer Exzellenz bestimmt ist und dass die EU eine Strategie haben sollte, um für kritische Technologien attraktiv zu sein, sie zu erhalten und beizubehalten, wobei Faktoren im Zusammenhang mit Übernahmen durch ausländische Akteure gebührend zu berücksichtigen sind; bekräftigt, dass bei der Anschaffung kritischer Infrastruktur generell europäischen Produkten Vorrang eingeräumt werden muss und dieser Grundsatz in ausgewogener und verhältnismäßiger Weise ausgearbeitet und umgesetzt werden sollte; befürwortet eine souveräne digitale Infrastruktur der EU, die mit Technologien zum besseren Schutz der Privatsphäre und einem auf Programmierschnittstellen (API) basierenden Ökosystem der EU ausgestattet ist und für die nichtfossile Energie für Rechenzentren und Cloud-Infrastruktur genutzt wird, unter anderem über marktgesteuerte und öffentlich-private Initiativen wie Joint Ventures oder dem Verbund aus Netzwerken in Bereichen wie KI, Gigafabriken und Cloud-Dienste;

72. begrüßt die Ziele, die in der europäischen Verordnung zu kritischen Rohstoffen hinsichtlich der Gewinnung, der Verarbeitung, dem Recycling und der Reduktion des Verbrauchs von kritischen Rohstoffen festgelegt sind, und betont, dass sich die Abhängigkeit von Seltenen Erden aus China in Zeiten plötzlicher Krisen möglicherweise als genauso nachteilig erweist wie die Abhängigkeit

von kohlenstoffbasierten Ressourcen aus Russland; bekräftigt, dass es notwendig ist, die europäische Verordnung zu kritischen Rohstoffen vollständig umzusetzen, Vorräte von kritischen Rohstoffen anzulegen, diese zu recyceln und zu ersetzen, die Diversifizierung der Versorgung mit kritischen Rohstoffen aus China hin zu zuverlässigeren Partnern zu beschleunigen, die EU-eigene Gewinnung und Verarbeitung zu steigern und die Ressourcen effizienter zu verwenden;

73. fordert die formale Anerkennung von in Auftrag gegebenen Hackerangriffen („hack-for-hire operations“) als eigenständige Bedrohung für demokratische Institutionen und Prozesse, auf die besser mittels einer Anpassung der Definitionen im Strafrecht reagiert werden könnte; fordert die Kommission und die Mitgliedstaaten auf, eine koordinierte internationale Initiative ins Leben zu rufen, um gegen sogenannte nicht angreifbare Hosting-Anbieter („bulletproof hosting providers“) vorzugehen, die wesentlich Infrastruktur an Cyberkriminelle vermieten, und zwar unter anderem durch die Sperrung und Filterung missbräuchlich verwendeter autonomer Systemnummern, um wirksam einzuschränken, ausgehend von welchen Staaten derartige Anbieter operieren können; hebt hervor, dass eine anhaltende Gefahr durch den Handel mit Schwachstellen von Unternehmen im Darknet besteht, wodurch digitale Kommunikationssysteme und -geräte Einflussnahme aus dem Ausland ausgesetzt sind;
74. betont, dass für eine stärkere Integration und strategische Koordinierung zwischen dem Ausbau der digitalen Infrastruktur, Maßnahmen zur Bekämpfung von ausländischer Informationsmanipulation und Einmischung und Desinformation sowie der Cybersicherheits- und Verteidigungspolitik gesorgt werden muss, um die strategische Autonomie der EU voranzubringen; unterstreicht, dass Infrastruktur mit doppeltem Verwendungszweck, wie z. B. resiliente, über die gesamte EU verteilte Rechenzentren, genutzt werden muss, um für operative Kontinuität angesichts von Naturkatastrophen und hybriden oder kriegsbedingten Bedrohungen zu sorgen; hebt ferner hervor, dass die Investitionen in militärische Mobilität und sichere Kommunikationswege erhöht werden müssen, unter anderem in den dringlichen und vorrangigen Einsatz von Gigabit-Netzen und weltraumgestützten Fähigkeiten wie IRIS², um verschlüsselte Kommunikationsdienste für die öffentliche Nutzung und für Verteidigungszwecke bereitzustellen; fordert, dass diese kritischen Kommunikationskapazitäten der Ukraine und Taiwan zur Verfügung gestellt werden;
75. betont, dass die Investitionen in sichere, interoperable und widerstandsfähige Systeme für den Informationsaustausch und in lokale Rechenzentren, die keinen extraterritorialen Rechtsvorschriften unterliegen, erhöht werden müssen; hebt hervor, dass diese Investitionen unerlässlich sind, um eine schnellere und

zuverlässigere Kommunikation zwischen den zuständigen Behörden auf nationaler und EU-Ebene zu gewährleisten, den Schutz vor Cyberangriffen und Datenschutzverletzungen zu stärken und die Integrität, Verfügbarkeit und Vertraulichkeit sensibler Daten sicherzustellen, und zwar unter anderem in Form verbesserter Cybersicherheitskapazitäten und einer modernen digitalen Infrastruktur der EU; unterstreicht, dass Redundanzen für die Gewährleistung der operativen Sicherheit und der Kommunikationssicherheit von entscheidender Bedeutung sind, beispielsweise durch bodengestützte sichere Kommunikationssysteme oder Trägheitsnavigationseinheiten;

76. betont, dass Cybersicherheitsrahmen wie die NIS-2-Richtlinie, die Cyberresilienz-Verordnung⁶⁶ und die Cybersolidaritätsverordnung⁶⁷ aufeinander abgestimmt funktionieren müssen, um Standards zu stützen, die dem Prinzip „Sicherheit durch Design“ folgen, und um eine regulatorische Fragmentierung zu vermeiden; nimmt in diesem Zusammenhang die gezielte Überarbeitung der NIS-2-Richtlinie zur Kenntnis; begrüßt den Vorschlag der Kommission, das operative Mandat und die Ressourcen der ENISA durch den überarbeiteten Rechtsakt zur Cybersicherheit erheblich zu stärken und auszuweiten; fordert, dass Experten für ausländische Informationsmanipulation und Einmischung ausdrücklich in die Gruppe der Interessenträger aufgenommen werden, die in der ENISA-Beratungsgruppe vertreten sind; fordert die Kommission auf, im Rahmen des MFR 2028-2034 hinreichende Finanzmittel bereitzustellen, damit Unternehmen, insbesondere im IKT-Sektor, die zusätzlichen Investitionen, die sich aus dem überarbeiteten Rechtsakt zur Cybersicherheit ergeben, finanzieren können; betont ferner, dass kleine und mittlere Unternehmen neben Ausnahmen, mit denen gewährleistet sein sollte, dass ihre Sicherheit und folglich die kollektive Cybersicherheit nicht geschwächt werden, auch Unterstützung bei der Einhaltung der Vorschriften benötigen;
77. weist darauf hin, dass die NIS-2-Richtlinie nur in geringem Maße umgesetzt wurde; bedauert, dass die Kommission nach Ablauf der

⁶⁶ 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>).

⁶⁷ 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>).

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 diese 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; fordert die Kommission und die Mitgliedstaaten auf, sich mit den Lücken zu befassen, die in Bezug auf Lagebewusstsein, Risikominderung und koordinierte übergreifende Maßnahmen bei Cyberbedrohungen, hybriden Bedrohungen und Informationsbedrohungen bestehen;

Zusammenarbeit in den Bereichen Justiz und Inneres

78. 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; betont, dass die zuständigen nationalen Behörden mit angemessenen Instrumenten und Kooperationskanälen ausgestattet werden müssen, um Straftaten im Zusammenhang mit ausländischer Einflussnahme zu verhindern, zu untersuchen, aufzudecken und strafrechtlich zu verfolgen; ist der Ansicht, dass Korruption und Einschüchterung gewählter und öffentlicher Amtsträger im Rahmen krimineller Netzwerke durch eine verstärkte Zusammenarbeit zwischen spezialisierten Antikorruptionsbehörden, Strafverfolgungsbehörden und relevanten Einrichtungen der EU als Teil der Reaktion der EU auf hybride Bedrohungen angegangen werden sollten; fordert die Kommission auf, zu beurteilen, ob es einen Mehrwert bringt, Mindestvorschriften im Unionsrecht für die Definition des Straftatbestands der wissentlichen Beteiligung an organisierten Aktivitäten zur Einflussnahme im Namen ausländischer Mächte und für diesbezügliche Sanktionen festzulegen; stellt fest, dass die anstehende Überarbeitung des Mandats einer Reihe von EU-Einrichtungen im Bereich Justiz und Inneres eine Gelegenheit zur Stärkung der operativen Dimension des Europäischen Schutzschilds für die Demokratie bieten könnte; 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;
79. 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 gesetzgebenden Organe auf, während der fortlaufenden Überarbeitung der Mandate von Europol und Eurojust sorgfältig die rechtlichen Lücken und Einschränkungen zu beurteilen, die die Agenturen derzeit daran hindern, den mit hybriden Bedrohungen konfrontierten Mitgliedstaaten uneingeschränkte Unterstützung zu leisten, und Möglichkeiten zu prüfen, diese Lücken unter Wahrung der Grundrechte und der im Vertrag verankerten Zuständigkeiten zu schließen; ist der Ansicht, dass die Aufnahme hybrider Bedrohungen in Anhang I der Europol-Verordnung⁶⁸ den Rechtsrahmen eindeutiger gestalten und die Arbeit von Europol in diesem Bereich erleichtern würde; betont außerdem, dass Europol und Eurojust mit ausreichenden finanziellen und personellen Ressourcen ausgestattet werden müssen, um die bevorstehende Stärkung ihrer Mandate wirksam umsetzen zu können;

80. ist der Ansicht, dass transnationale Repression eine wachsende und ernsthafte Bedrohung für die Demokratie und die innere Sicherheit in der EU darstellt; betont, dass transnationale Repression durch Hass- und Verleumdungskampagnen und die Verbreitung illegaler Inhalte online erfolgen kann, sie aber auch zu körperlichen Übergriffen und Mord führen kann; 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; betont, dass solche Praktiken ein nicht hinnehmbarer Akt der Einflussnahme aus dem Ausland sind, der sich potenziell destabilisierend auf unsere Gesellschaften auswirkt; hebt in diesem Zusammenhang hervor, dass die verbleibenden Schlupflöcher im Unionsrecht geschlossen werden müssen und im Bereich der Strafgerichtsbarkeit und der Strafverfolgung auf EU-Ebene eine noch stärkere Koordinierung erfolgen muss, indem ein Rahmen für die polizeiliche und justizielle Zusammenarbeit, der transnationaler Repression gewidmet ist, als Teil des Europäischen Schutzschilds für die Demokratie genutzt wird, wobei gezielt betroffene Personen und Gruppen einzubeziehen sind und ihr Schutz sicherzustellen ist; weist darauf hin, dass dringend gegen die missbräuchliche Verwendung von roten Ausschreibungen von Interpol zu politisch motivierten Zwecken

⁶⁸ Verordnung (EU) 2016/794 des Europäischen Parlaments und des Rates vom 11. Mai 2016 über die Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung (Europol) und zur Ersetzung und Aufhebung der Beschlüsse 2009/371/JI, 2009/934/JI, 2009/935/JI, 2009/936/JI und 2009/968/JI des Rates (ABl. L 135 vom 24.5.2016, S. 53, ELI: <http://data.europa.eu/eli/reg/2016/794/oj>).

vorgegangen werden muss;

81. verurteilt aufs Schärfste die Instrumentalisierung der Migration durch Drittländer oder feindselige nichtstaatliche Akteure mit dem Ziel, einen Mitgliedstaat oder die EU zu destabilisieren; vertritt den Standpunkt, dass dieses Phänomen einen inakzeptablen Versuch darstellt, politischen Druck auf Mitgliedstaaten an den Außengrenzen und die EU auszuüben; betont, dass derartige Praktiken auch eine schwere Misshandlung schutzbedürftiger Personen darstellen, die möglicherweise Anspruch auf internationalen Schutz haben, und dass diese Praktiken das Recht, Asyl zu beantragen, nicht einschränken sollten; nimmt die spezifischen Bestimmungen über die Instrumentalisierung der Migration zur Kenntnis, die kürzlich in wichtige EU-Rechtsvorschriften aufgenommen wurden; begrüßt ferner die jüngste Überarbeitung des EU-Rechtsrahmens, mit der hybride Bedrohungen in die Gründe für die Auslösung des Visa-Aussetzungsmechanismus der EU aufgenommen wurden; betont, dass eine praktikable und wirksame Reaktion der EU auch auf einer engen Koordinierung und loyalen Zusammenarbeit zwischen benachbarten Mitgliedstaaten sowie zwischen ihnen und den EU-Organen im Geiste der Loyalität und der gegenseitigen Solidarität und auf verbesserten technologischen und operativen Fähigkeiten beim Grenzmanagement beruhen muss, wobei die Integrität des Schengen-Raums zu wahren und die uneingeschränkte Achtung der Grundwerte der EU sicherzustellen ist;
82. nimmt die von der Kommission angekündigte Überarbeitung des Mandats von Frontex zur Kenntnis; betont, dass die Überarbeitung die erforderliche Rechtsgrundlage, Analysefähigkeiten und angemessene personelle, finanzielle und technische Ressourcen vorsehen sollte, um eine wirksame Unterstützung der Mitgliedstaaten beim Management und Schutz der Außengrenzen im Einklang mit dem einschlägigen Unionsrecht, einschließlich der Grundrechte, zu ermöglichen; betont in dieser Hinsicht, dass die Fähigkeit der EU, die Mitgliedstaaten in Angelegenheiten im Zusammenhang mit dem Bereich Inneres im Rahmen des MFR 2028-2034 zu unterstützen, weiter gestärkt werden muss, auch bezüglich der Reaktion auf Bedrohungen hybrider Art;

Externe Dimension

83. betont, dass der Europäische Schutzschild für die Demokratie eine starke externe Dimension haben muss, und begrüßt Maßnahmen zur Unterstützung von Ländern außerhalb der EU, insbesondere durch den Aufbau von Kapazitäten zur Stärkung der Resilienz von Bewerberländern und möglichen Bewerberländern angesichts ausländischer Informationsmanipulation und Einmischung, hybrider Einflussnahme und transnationaler Repression, durch die Unterstützung von unabhängigen Medien und unabhängigem

Journalismus und durch eine verbesserte Fähigkeit, Desinformation vor und während Wahlen aufzudecken und zu bekämpfen; unterstreicht, dass es eine angemessene Finanzierung von unabhängigen Medien in Nachbarländern braucht, einschließlich einer Kernfinanzierung über das Instrument „Europa in der Welt“; stellt fest, dass die Kapazitäten und Zusagen der Bewerberländer unterschiedlich sind, was eine differenzierte, kontextabhängige Umsetzung des Europäischen Schutzschilds für die Demokratie unter uneingeschränkter Achtung der Werte der EU erfordert; betont, dass die Stärkung der demokratischen Resilienz sowohl für die Glaubwürdigkeit der Erweiterung als auch für die Sicherheit und Stabilität der EU von entscheidender Bedeutung ist; fordert die systematische Einbeziehung der Bewerberländer in entsprechende Maßnahmen, Unterstützungsmechanismen und Expertennetzwerke im Rahmen der externen Dimension;

84. fordert, dass der Europäische Schutzschild für die Demokratie als wechselseitiger Mechanismus für Fachwissen dient, bei dem die EU erfolgreiche Krisenreaktionsmodelle, zivil-militärische Kooperationsrahmen und Echtzeit-Erkennungstechniken integriert, und weist auf die Expertise von Partnern an vorderster Front hin, die Aggression und Einflussnahme aus Russland ausgesetzt sind; betont, dass die EU ausgesprochen viel von der Widerstandsfähigkeit der Republik Moldau und der Ukraine lernen kann;
85. nimmt die führende Rolle Taiwans in der Entwicklung von Produkten der Hochtechnologie und seine umfangreichen Erfahrung bei der Abwehr von hybriden Angriffen, Informationsmanipulation und Einmischung durch China zur Kenntnis; fordert einen regelmäßigen Austausch über relevante Sicherheitsfragen sowie eine engere Zusammenarbeit mit gleichgesinnten Partnern in Ostasien, einschließlich Taiwan, Japan und Südkorea, bei der Bekämpfung von ausländischer Informationsmanipulation und Einmischung und von Sabotage von Unterseekabeln;
86. fordert die Entwicklung einer umfassenden Strategie in prioritären Regionen, mit der die EU-Delegationen und die Missionen und Operationen im Rahmen der Gemeinsamen Sicherheits- und Verteidigungspolitik (GSVP) in enger Abstimmung mit den diplomatischen Vertretungen der EU-Mitgliedstaaten mobilisiert werden, um ein besseres Verständnis der lokalen Gegebenheiten, die möglicherweise zu Einflussnahme aus dem Ausland führen, zu erlangen und angepasst zu reagieren; stellt fest, dass die EU-Delegationen und die Botschaften der Mitgliedstaaten die Organisation von Sensibilisierungskampagnen in den Gastländern unterstützen können; ist der Ansicht, dass verstärkte Kapazitäten für strategische Kommunikation und öffentliche Diplomatie innerhalb der EU-Delegationen unerlässlich sind und der Schwerpunkt darauf liegen sollte, faktenbasierte Narrative, bürgerschaftliches Engagement und Vertrauensbildung, insbesondere bei jungen

Menschen und Lehrkräften, zu stützen; ist daher besorgt über Berichte hinsichtlich einer möglicherweise drohenden Verkleinerung der EU-Delegationen und ihrer Personalausstattung, insbesondere vor dem Hintergrund der zunehmenden internationalen Herausforderungen und geopolitischen Spannungen;

87. betont, dass 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 ausländische Informationsmanipulation und Einmischung umfasst; fordert, dass die Vorteile, Präsenz und Rolle der GSVP-Missionen und -Operationen weltweit deutlicher sichtbar gemacht und stärker strategisch kommuniziert werden, insbesondere in der unmittelbaren Nachbarschaft Europas und in Bewerberländern und möglichen Bewerberländern; 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 ausländische Informationsmanipulation und Einmischung in GSVP-Missionen einzubeziehen, für Schulungen im Bereich ausländische Informationsmanipulation und Einmischung bei allen relevanten derzeitigen und künftigen Missionen und Operationen Sorge zu tragen und die Koordinierung zwischen zivilen und militärischen Operationen zu stärken, um hybriden Einflüssen entgegenzuwirken;
88. betont den Stellenwert gemeinsamer Übungen, Kapazitätsaufbau und technischer Hilfe für Partnerländer, die anhaltendem hybridem Druck ausgesetzt sind; fordert die Mitgliedstaaten und den EAD auf, Maßnahmen zum Kapazitätsaufbau und Schulungen zu hybriden Bedrohungen in die Mandate einzelner Missionen und Operationen aufzunehmen, damit die Partnerländer besser gewappnet sind; begrüßt die Entsendung von EU-Teams für die rasche Reaktion auf hybride Bedrohungen und von Teams für die rasche Reaktion auf Cybervorfälle als zweckdienlichen Weg, um Kapazitäten und Resilienz in jenen Ländern aufzubauen, die Ziel von Cyberangriffen, hybriden Angriffen und Angriffen in Form von ausländischer Informationsmanipulation und Einmischung sind, wie das jüngste Beispiel Moldaus zeigt; nimmt in diesem Zusammenhang die Präsenz von Frontex in mehreren relevanten Drittländern und den potenziellen Mehrwert der Kapazitäten der Agentur in dieser Hinsicht zur Kenntnis;
89. betont, dass wiederholte Versuche, die Beziehungen zu Russland zu normalisieren, ohne sich mit den grundlegenden Wesensmerkmalen des russischen Staates und seinen imperialen strategischen Zielen zu befassen, zu erhöhter Instabilität beigetragen, die Abschreckung geschwächt und die europäische und globale Sicherheit untergraben haben; betont, dass die künftige Politik der EU und der Mitgliedstaaten auf einer realistischen Bewertung dieser

historischen Kontinuität beruhen muss, wobei der Abschreckung, der Widerstandsfähigkeit und der Sicherheit der Länder in der Nachbarschaft Russlands Vorrang vor kurzfristigen wirtschaftlichen oder politischen Erwägungen einzuräumen ist; begrüßt die Bemühungen der letzten Jahre, die Wirtschaft der EU von der Abhängigkeit von fossilen Brennstoffen aus Russland zu entkoppeln; betont ferner, dass der vollständige und unumkehrbare Abbau dieser Abhängigkeit eine strategische Priorität für die EU und ihre Mitgliedstaaten darstellen sollte;

90. begrüßt das verstärkte Bekenntnis zum Aufbau von Kapazitäten für offensive Informationsoperationen, 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 und verstärkte Informationsmaßnahmen festigt, um Destabilisierungsanstrengungen sowie anderen Formen feindseliger staatlicher und staatlich geförderter koordinierter Informationsmanipulation, Operationen kognitiver Kriegsführung und Kampagnen zur feindseligen Einflussnahme durch autoritäre oder böswillige Akteure entgegenzuwirken; unterstreicht, dass Menschen, die unter autoritären Regimen und insbesondere in Russland und Belarus leben, sachliche und vertrauenswürdige Informationen zur Verfügung gestellt werden müssen, um die destruktiven Herrschaftspraktiken der Regierenden aufzudecken, zumal diese die Freiheit und den Frieden nicht nur in den Nachbarländern, sondern in erster Linie in ihrem eigenen Land 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;
91. stellt mit großer Besorgnis fest, dass in einigen Mitgliedstaaten staatliche Maßnahmen und strategische Entscheidungen immer wieder den Interessen Russlands dienen; weist erneut auf den Fall der ehemaligen, von der Fidesz-Partei geführten Regierung Ungarns als besonders eindeutiges Beispiel hin, an dem unter anderem offenkundig wurde, wie es verabsäumt wurde, das Eindringen russischer, mit dem Staat verbundener Cyberakteure ordnungsgemäß zu melden und zu untersuchen, wie langfristige Gasverträge mit Russland zu Preisen über dem Marktniveau abgeschlossen wurden, wie die EU-Hilfe für die Ukraine systematisch blockiert wurde und wie bei wichtigen außen- und sicherheitspolitischen Entscheidungen der EU eine Ausrichtung an den Standpunkten Russlands erfolgte; fordert die ordnungsgemäße Meldung und Untersuchung von Aktivitäten und Kampagnen, die möglicherweise mit Einflussnahme und Einmischung aus dem Ausland in Verbindung stehen; fordert mehr Wachsamkeit, eine verstärkte Überwachung und den umfassenden Einsatz der

Instrumente der EU, um die EU vor internen Faktoren, die Einflussnahme und Einmischung aus dem Ausland begünstigen, zu schützen;

92. stellt fest, dass die Bewerberländer und möglichen Bewerberländer sowie die Nachbarländer der EU, insbesondere die Westbalkanländer, Moldau, die Ukraine, Armenien und Georgien, eindeutig im Fokus der von Russland betriebenen ausländischen Informationsmanipulation und Einmischung stehen, bei der eines der Ziele darin besteht, die EU zu diskreditieren und den Wert der EU-Integration in der öffentlichen Wahrnehmung zu schmälern; fordert die Kommission und den EAD auf, die Zusammenarbeit mit den relevanten Akteuren in diesen Ländern in den Bereichen Informationsresilienz, Cybersicherheit und hybride Bedrohungen zu vertiefen und von Ad-hoc-Unterstützung zu systematischer, langfristiger Unterstützung überzugehen, die auf den Aufbau institutioneller, rechtlicher und bürgerschaftlicher Widerstandsfähigkeit abzielt; fordert, dass EU-Mittel für regionale Koordinierungszentren zur Abwehr von Bedrohungen der Integrität von Online-Informationen und von ausländischer Informationsmanipulation und Einmischung in relevanten Teilen der Nachbarschaft der EU bereitgestellt werden und dass die Unterstützung für investigativen Journalismus und Medienregulierungsbehörden verstärkt wird; betont, dass ein besonderer Schwerpunkt auf unterstützenden Maßnahmen für die Integrität von Wahlen in Bewerberländern oder möglichen Bewerberländern liegen muss, und zwar auch vor dem Hintergrund der Streichung von USAID-Mitteln, die insbesondere den Westbalkanraum trifft;
93. betont, dass die Bemühungen der EU, die Bewerberländer bei der Stärkung ihrer Resilienz gegen Einflussnahme aus dem Ausland zu unterstützen, mit der nachweislichen Umsetzung entsprechender Reformen und greifbaren Ergebnissen auf Seite dieser Länder einhergehen sollten; fordert die Kommission auf, bei ihrer Prüfung der Fortschritte der Bewerberländer im Rahmen der Beitrittskapitel weiterhin einen rigorosen Ansatz zu verfolgen; betont, dass Mängel bei der Bewältigung zentraler Probleme wie Korruption, das Fehlen von unabhängigen Medien, Menschenrechtsverletzungen und Schwachstellen in demokratischen Prozessen das Vertrauen der Bürgerinnen und Bürger in die nationalen Einrichtungen und EU-Organen untergraben und so EU-feindliche Narrative entstehen lassen, die möglicherweise von Drittländern und Akteuren, die ausländische Informationsmanipulation und Einmischung betreiben, ausgenutzt werden;
94. fordert die Kommission auf, regionale EDMO-Zentren einzurichten, die für relevante EU-Bewerberländer, mögliche Bewerberländer und Nachbarländer zuständig sind, und dabei das bestehende Zentrum für die Republik Moldau zum Vorbild zu nehmen;

95. fordert die Kommission auf, Medienkompetenzprogramme zu einem festen Bestandteil der Heranführungshilfe und des Europäischen Nachbarschaftsinstruments zu machen; betont, dass die kulturelle Zusammenarbeit integraler Bestandteil dieser Instrumente sein sollte, um den gesellschaftlichen Zusammenhalt, gemeinsame Werte und direkte zwischenmenschliche Kontakte in Bewerber- und Nachbarländern zu stärken; betont, dass aufgrund der Streichung der thematischen Programme und der entsprechenden Finanzaufweisungen für Menschenrechte und Demokratie sowie für Organisationen der Zivilgesellschaft – wie im Vorschlag der Kommission für den MFR 2028-2034 und im Vorschlag für ein neues Instrument „Europa in der Welt“ vorgesehen – erhebliche Unsicherheit darüber besteht, wie diese im EU-Vertrag verankerten Verpflichtungen tatsächlich durchgehend berücksichtigt, in die Praxis übertragen und überwacht werden sollen; fordert die Kommission erneut auf, jene Programme zu stärken, die darauf abzielen, die Zivilgesellschaft, Menschenrechtsverteidiger, Journalisten und investigative Medien in Drittländern in beutendem Maße einzubinden und zu unterstützen; drängt darauf, dass im Rahmen des neuen MFR planbare Finanzmittel bereitgestellt werden, die eine rasche Reaktion auf Bedrohungen der Grundfreiheiten ermöglichen und lokale Initiativen unterstützen;
96. fordert mit Nachdruck, dass sich die EU darum bemüht, die Partnerländer in ihrer östlichen und südlichen Nachbarschaft sowie vorrangige Länder in Subsahara-Afrika, im asiatisch-pazifischen Raum und in Lateinamerika dabei zu unterstützen, Resilienz gegenüber ausländischer Informationsmanipulation und Einmischung aufzubauen, demokratische Prozesse zu stärken und die Integrität von Wahlen sicherzustellen, und zwar unter anderem im Wege zweckgebundener Finanzierung im Rahmen des nächsten MFR; betont insbesondere, dass sich der Wandel, der sich in Nordafrika und der Sahelzone vollzieht, unmittelbar auf die Sicherheit und die demokratische Widerstandsfähigkeit der EU auswirkt, und hält fest, dass diese Regionen besonders anfällig für ausländische Informationsmanipulation und Einmischung sind, vor allem aufgrund politischer Instabilität und fragiler Informationsökosysteme; betont, dass Russland und China zunehmend zusammenarbeiten, um revisionistische Narrative über den mutmaßlichen Niedergang des Westens und den „Neokolonialismus“ in diesen Regionen zu verstärken, was eine strategische Kommunikationslücke offenkundig macht, die die Glaubwürdigkeit und den Einfluss der EU untergräbt; betont insbesondere, dass neben Mechanismen zur finanziellen Unterstützung weiterhin gezielte Maßnahmen zur Stärkung der Widerstandsfähigkeit dieser Regionen gegenüber ausländischer Informationsmanipulation und Einmischung ausgearbeitet werden müssen, und zwar unter anderem in Form von Unterstützung unabhängiger Medien, der Zivilgesellschaft, der Digital- und KI-Kompetenzen, der strategischen Kommunikation in lokalen Sprachen

und verbesserter Überwachungs- und Reaktionsmechanismen wie dem Leitprojekt EUvsDisinfo;

97. 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 Cyberbedrohungen, hybriden Bedrohungen und Bedrohungen durch ausländische Informationsmanipulation und Einmischung übernehmen 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; ist der Auffassung, dass solche Vereinbarungen vorrangig mit Ländern geschlossen werden sollten, deren innere Instabilität sich unmittelbar auf die Sicherheit der EU auswirkt; nimmt die Parlamentswahl in der Republik Moldau vom 28. September 2025 sowie die Präsidentschaftswahl vom 3. November 2024 und den klaren Sieg der proeuropäischen Kräfte zur Kenntnis, die erfolgten, obwohl Russland erhebliche Anstrengungen unternommen und bedeutende Ressourcen eingesetzt hat, um die Lage in der Republik Moldau zu destabilisieren und sie von ihrem europäischen und euro-atlantischen Weg abzubringen;
98. stellt mit Besorgnis fest, dass sich in Armenien die mit Russland verbundenen hybriden Bedrohungen verschärft haben, mit denen das Ergebnis der Wahl vom Juni 2026 beeinflusst und die demokratischen Prozesse, der soziale Zusammenhalt und die Bemühungen um Friedenskonsolidierung im Land beeinträchtigt werden sollten, was auch böswillige Cyberaktivitäten, koordinierte Informationsmanipulation, Einmischung in Wahlen, wirtschaftlichen Zwang und offene und verdeckte Drohungen durch hochrangige russische Amtsträger sowie die Aktivierung von Einflussnetzwerken umfasste; weist darauf hin, dass der armenische Auslandsnachrichtendienst über den Einsatz offener und verdeckter Informationsoperationen, verzerrender Narrative und von Bemühungen berichtet hat, den öffentlichen Diskurs in einer Weise zu manipulieren, die den nationalen Interessen Armeniens abträglich ist, und betont, dass an der Ausübung dieses hybriden Drucks möglicherweise sowohl staatliche als auch nichtstaatliche Akteure, darunter Sprachrohre im Inland wie gewisse religiöse Akteure und oligarchische Netzwerke, beteiligt sind, die mit umfassenderen russischen Strategien der Einflussnahme in der Region in Verbindung stehen; begrüßt die Einrichtung der EUPM Armenia, durch die armenischen Institutionen strategische Beratung und Kapazitätsaufbau hinsichtlich der Bekämpfung von ausländischer Informationsmanipulation und Einmischung, Cyberangriffen und illegalen Finanzströmen geboten wird; fordert die EU-Mission in Armenien (EUMA) auf, als Teil ihres Beitrags zur demokratischen Resilienz ihre Kontakte zu lokalen demokratischen Akteuren,

Gemeinschaftsorganisationen und unabhängigen Medien zu verstärken; weist darauf hin, dass Armenien nach wie vor Mitglied der von Russland geführten Organisation des Vertrags über kollektive Sicherheit ist, und fordert Armenien auf, diese vollständig zu verlassen;

99. bringt sein tiefes Bedauern über den Beschluss des US-Präsidenten vom 7. Januar 2026 zum Ausdruck, mit dem der Rückzug aus einer erheblichen Zahl internationaler Organisationen, einschließlich zahlreicher Gremien der Vereinten Nationen, eine Aussetzung der Beteiligung an ihnen bzw. eine Beendigung der Zusammenarbeit mit ihnen erfolgte; ist zutiefst besorgt darüber, dass ein solcher Schritt die finanzielle Tragfähigkeit des Systems der Vereinten Nationen schmälert, die multilaterale Zusammenarbeit in einer Zeit, in der sie am dringendsten notwendig ist, schwächt und autoritäre und revisionistische Akteure, die in der Vergangenheit versucht haben, jedweden Rückzug oder Ausstieg westlicher Mächte aus internationalen Organisationen auszunutzen, bestärkt; betont daher, dass die EU ihre Führungsrolle bei der Unterstützung und Stärkung multilateraler Organisationen ausbauen und die demokratischen Institutionen aufrechterhalten muss; fordert die US-Regierung auf, ihre Entscheidung zu überdenken und ihr Bekenntnis zu den Vereinten Nationen und der multilateralen Zusammenarbeit zu beteuern;
100. bringt seine entschiedene Ablehnung der aktuellen nationalen Sicherheitsstrategie der USA zum Ausdruck, insbesondere was die negative Charakterisierung der EU und ihrer Herausforderungen und Risiken und die Vorstellung betrifft, dass internationale Beziehungen auf Einflussphären aufbauen; verurteilt alle Versuche, die demokratischen Prozesse in der EU zu beeinflussen oder zu beeinträchtigen; betont, dass es wichtig ist, die Integrität der EU-Organen und die Beschlussfassung der EU zu wahren; erklärt sich besorgt darüber, dass bestimmte Elemente der Strategie deutlich zu kurz greifen, um der von Russland ausgehenden Bedrohung, insbesondere für die Sicherheit Europas und damit auch Amerikas, angemessen zu begegnen; bedauert darüber hinaus, dass die EU als politisches System in der Strategie fehlerhaft bewertet wird und eine unbegründete ablehnende Haltung gegenüber der EU darin zum Ausdruck kommt; ist der Ansicht, dass es angesichts der Strategie umso wichtiger ist, dass die EU ihre strategische Autonomie stärkt, Abhängigkeiten abbaut und Partnerschaften diversifiziert;
101. 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; fordert die Weiterentwicklung von gemeinsamen Open-Source-Standards, Rahmen für die Sicherheit

hochmoderner KI, Datenmodellen, Methoden und Taxonomien zusammen mit gleichgesinnten Partnern, um eine erfolgreichere Zusammenarbeit zu ermöglichen; bekräftigt, dass die NATO bei der Bekämpfung hybrider Kriegsführung gegen demokratische Institutionen eine Schlüsselrolle innehat und weist erneut auf ihre diesbezüglichen speziellen Instrumente und Strategien hin, und zwar insbesondere im Rahmen ihres Exzellenzzentrums für strategische Kommunikation; hebt hervor, dass nach dem Beitritt Finnlands und Schwedens 23 der 27 EU-Mitgliedstaaten auch NATO-Verbündete sind, und betont, dass es ein belastbares Zusammenwirken der Strategien der EU und der NATO braucht; begrüßt die in bilateralen und multilateralen Rahmen bereits unternommenen Schritte, darunter der Verhaltenskodex der Vereinten Nationen für die Informationsintegrität auf digitalen Plattformen, die in der Erklärung des Europarats von Reykjavik eingegangenen Verpflichtungen zum Schutz der Wahlsysteme vor Einflussnahme aus dem Ausland, die fortgesetzten Bemühungen im Rahmen des Krisenreaktionsmechanismus der G7 und die Etablierung von Sicherheits- und Verteidigungspartnerschaften, insbesondere jener, deren Schwerpunkt auf der Bekämpfung von Cyberangriffen, hybriden Bedrohungen und ausländischer Informationsmanipulation und Einmischung sowie auf dem Schutz kritischer Infrastruktur liegt; bekräftigt in diesem Zusammenhang seine aufrichtige Wertschätzung für das weiterhin bestehende Bekenntnis des Vereinigten Königreichs zur europäischen Sicherheit;

Wahlsysteme und Resilienz bei Wahlen

102. betont, dass es ein Kernziel des Europäischen Schutzschilds für die Demokratie sein sollte, die Integrität von Wahlen auf lokaler, regionaler, nationaler und EU-Ebene und in Bewerberländern zu schützen; fordert die Kommission und die Mitgliedstaaten auf, unter uneingeschränkter Achtung des Subsidiaritätsprinzips und in dem in den Verträgen bestimmten Rahmen bei der Umsetzung von Reformen, mit denen die Resilienz von Wahlprozessen in Europa gestärkt wird, zusammenzuarbeiten und dabei einen besonderen Schwerpunkt auf Maßnahmen zur Verhinderung ausländischer Einflussnahme zu legen; nimmt zur Kenntnis, dass Angriffe auf die Integrität von Wahlen vielschichtig, ganzheitlich und langfristig ausgerichtet sind und sich in ein Ökosystem von Bedrohungen einschreiben, dem im Wege eines gesamtgesellschaftlichen Ansatzes begegnet werden muss; regt an, dass die Initiative „Europäischer Schutzschild für die Demokratie“ die Koordinierung der Bemühungen, die sowohl online als auch offline unternommen werden, unterstützen sollte, um die Integrität von Wahlen in Europa zu wahren, was auch Bemühungen im Hinblick auf hybride Bedrohungen, Cyberbedrohungen und die Finanzierung von Einmischung und Informationsmanipulation einschließt;

103. 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; fordert die Kommission und die Mitgliedstaaten auf, sich um die systematische Entwicklung und Ausweitung von Stresstests mit Schwerpunkt auf Wahlen auf nationaler und grenzüberschreitender Ebene zu bemühen, bei denen auf praktischen Erfahrungen und Lehren aus früheren Wahlzyklen aufgebaut wird, damit Risiken im Zusammenhang mit Manipulation von Informationen, Einmischung mit Mitteln des Internets und plattformgesteuerter Verbreitungen besser vorausgesehen, simuliert und abgemildert werden können;

104. 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;
105. ist der Ansicht, dass Hasskampagnen, Einschüchterung 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 derartige Bedrohungen durch Versuche von Drittländern, die EU zu destabilisieren, befeuert werden können, unter anderem durch Desinformationstaktiken wie Deepfakes, die reale politische Kandidaten falsch darstellen und bewusst darauf ausgelegt sind, die Wähler irrezuführen; 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;
106. betont, dass der Schutz und die Sicherheit von Frauen im politischen Leben Voraussetzungen für eine gleichberechtigte Vertretung und eine widerstandsfähige Demokratie sind; verurteilt Desinformationskampagnen – auch solche, bei denen Deepfakes und nicht einvernehmliche sexuelle Inhalte zum Einsatz kommen –, die dazu dienen, Kandidatinnen zu schikanieren, zu bedrohen und einzuschüchtern, wobei sie sich häufig auf Narrative stützen, mit denen deren Kompetenz, Glaubwürdigkeit und moralische Integrität infrage gestellt werden, was Frauen von politischer Teilhabe abhält und das Vertrauen in demokratische Institutionen untergräbt; begrüßt das gezielte Verbot von „Nudify-Apps“ in der Verordnung über künstliche Intelligenz und weist darauf hin, dass geschlechtsspezifische Gewalt und der Schutz von Minderjährigen im Gesetz über digitale Dienste als systemisches Risiko eingestuft

werden; fordert die Kommission auf, in die anstehenden Empfehlungen zur Sicherheit in der Politik spezifische Bestimmungen über die Überwachung, Prävention und Bekämpfung von Desinformationskampagnen, die sich gezielt gegen Kandidatinnen richten, aufzunehmen;

107. verurteilt betrügerische Werbung, in der Personen vorkommen, die sich fälschlicherweise als bestimmte Politiker, politische Kandidaten und andere Persönlichkeiten des öffentlichen Lebens ausgeben und in denen deren Identität missbräuchlich verwendet wird; weist warnend darauf hin, dass der Hauptzweck eines solchen Betrugs zwar oft finanzieller Gewinn ist, die unbefugte Verwendung des Abbilds und der Gestalt einer Person des öffentlichen Lebens mit dem Ziel, Authentizität oder Zustimmung vorzutäuschen, jedoch möglicherweise zu Rufschädigung führt und zum Verwischen der Grenze zwischen authentischen Informationen und gefälschten Inhalten beiträgt sowie das Vertrauen der Öffentlichkeit in demokratische Prozesse und politische Akteure weiter untergräbt; fordert die Kommission und die Mitgliedstaaten auf, zu untersuchen, ob Online-Plattformen hinsichtlich ihres Vorgehens zur Entfernung widerrechtlicher Werbung die Vorschriften einhalten;
108. hebt hervor, dass das ECNE bei der Förderung des Austauschs bewährter Verfahren für die Resilienz bei Wahlen in der gesamten EU und ihren Mitgliedstaaten eine zentrale Funktion innehat, nimmt jedoch die derzeitigen Limitierungen des ECNE zur Kenntnis und begrüßt die Zusage der Kommission, es zu stärken; fordert eine ambitionierte Reform des ECNE, die auch eine Überprüfung seiner Ressourcen und Personalausstattung, eine Weiterentwicklung des gemeinsamen Mechanismus zur Stärkung der Resilienz bei Wahlen und mehr Einbeziehung der Bewerberländer umfasst; fordert die Kommission auf, eine ständige Überwachungsgruppe im Rahmen des ECNE einzurichten, die für die Aufsicht über die Umsetzung der Empfehlungen der Kommission zu inklusiven und stabilen Wahlprozessen 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; fordert ferner, dass das Parlament und die Behörde für europäische politische Parteien und europäische politische Stiftungen (APPF) als ständige Partner in alle Sitzungen des ECNE einbezogen werden;
109. betont, dass die Wahlinfrastruktur eine grundlegende Komponente der demokratischen Resilienz der EU darstellt und wirksam vor zunehmenden physischen Bedrohungen und Cyberbedrohungen geschützt werden muss; 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 in der Richtlinie enthaltene Liste der wesentlichen Dienste im Bereich der öffentlichen Verwaltung aufgenommen wird; fordert die Kommission auf, dafür zu sorgen, dass diese Aufnahme anschließend in der NIS-2-Richtlinie und den ENISA-Leitlinien aufgegriffen wird;

110. 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; ist besorgt über anhaltende Mängel bei den bestehenden Registern wirtschaftlicher Eigentümer in den Mitgliedstaaten, auch was die Qualität der Daten bzw. die Gefahr betrifft, dass der Zugang für Personen mit berechtigtem Interesse wie Journalisten oder Organisationen der Zivilgesellschaft übermäßig eingeschränkt wird; fordert die Mitgliedstaaten nachdrücklich auf, die Geldwäscherichtlinie⁶⁹, mit der die Vorschriften über den Zugang zu Registern wirtschaftlicher Eigentümer harmonisiert werden, vollständig und getreu umzusetzen; betont ferner, dass politische Werbung und politische Kommunikation im Online-Umfeld im Einklang mit den Transparenzvorschriften der EU vollständig transparent in Bezug auf die Identität des Sponsors und die Finanzierungsquelle sein müssen; fordert die strikte Durchsetzung der bestehenden Maßnahmen, um eine Finanzierung durch Stellvertreter in der Politik zu verhindern; betont, dass eine wirksame EU-weite Überwachung und Zusammenarbeit zwischen den Behörden wichtig sind, um die Einhaltung der Transparenzverpflichtungen sicherzustellen; fordert die Kommission und die Mitgliedstaaten in diesem Sinne auf, zu prüfen, welche Möglichkeiten es gibt, um die Zusammenarbeit zwischen den für die Korruptionsbekämpfung zuständigen Behörden und den unabhängigen Wahlkommissionen in den Mitgliedstaaten zu verbessern;
111. nimmt mit Besorgnis die zunehmenden Beweise für Einflussnahme aus dem Ausland und Spionage, die sich gegen politische

⁶⁹ Richtlinie (EU) 2015/849 des Europäischen Parlaments und des Rates vom 20. Mai 2015 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung, zur Änderung der Verordnung (EU) Nr. 648/2012 des Europäischen Parlaments und des Rates und zur Aufhebung der Richtlinie 2005/60/EG des Europäischen Parlaments und des Rates und der Richtlinie 2006/70/EG der Kommission (ABl. L 141 vom 5.6.2015, S. 73, ELI: <http://data.europa.eu/eli/dir/2015/849/oj>).

Institutionen und Prozesse sowohl auf Ebene der EU als auch auf Ebene der Mitgliedstaaten richten, zur Kenntnis; begrüßt die Ermittlungen in mehreren Mitgliedstaaten, die zu Verurteilungen geführt haben, und die anhängigen Verfahren zu Bestechung, Spionage und Aktivitäten zur Einflussnahme aus dem Ausland; hebt die ernsthaften Risiken hervor, die durch unzureichende Sicherheitsmaßnahmen bei der Rekrutierung von Personal und Partnern mit engen Verbindungen zu autoritären Regimen entstehen; betont, dass es zum Schutz der Integrität und des Funktionierens der EU-Organe solider Maßnahmen gegen Spionage und Infiltration bedarf; unterstreicht außerdem, dass die schwerwiegenden und sich ausweitenden Vorwürfe untersucht werden müssen, wonach ungarische Amtsträger im Dienst der vorherigen, von der Fidesz-Partei geführten Regierung Ungarns auf die EU-Organe ausgerichtete Spionageaktivitäten durchgeführt haben, wobei es auch Berichte gab, dass sensible Informationen aus EU-Treffen russischen Amtskollegen mitgeteilt wurden, wodurch Bedenken aufgeworfen werden, was Verstöße gegen die Vertraulichkeitspflicht, die Weitergabe nachrichtendienstlicher Erkenntnisse und die Integrität der Entscheidungsprozesse der EU betrifft;

112. 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, insbesondere, was den Umstand anbelangt, dass Parteien aus Drittländern weder Vetorechte noch Kontrolle über europäische Parteien haben sollten; fordert die gesetzgebenden Organe auf, für die vollumfängliche und wirksame Durchsetzung der Verordnung zu sorgen;
113. fordert die Kommission erneut auf, den jährlichen Bericht über die Rechtsstaatlichkeit zu festigen und Demokratien gegen Einflussnahme aus dem Ausland zu stärken, unter anderem indem die Themen freie und faire Wahlen, solide rechtliche Garantien, Kontrollen und Gegenkontrollen sowie das Funktionieren demokratischer Institutionen behandelt werden, um ein vollständigeres Bild der Rechtsstaatsstandards in der gesamten EU zu vermitteln;
114. stellt fest, dass die rasanten Entwicklungen im Bereich der Kryptowährungen – was auch Plattformen bzw. Dienstleister einschließt, die außerhalb der EU tätig sind – eine potenzielle Sicherheitslücke schaffen, da keine ausreichende Transparenz herrscht und die Finanzierung politischer Parteien und Bewegungen in Europa nicht eingehend geprüft werden kann; betont die Tatsache, dass es bei Kryptowerten schwierig sein kann, die Herkunft von Spenden an politische Parteien zu ermitteln und mögliche Einflussnahme aus dem Ausland auf demokratische

Prozesse einzudämmen, da Kryptowerte einen pseudonymisierten Charakter und globale Reichweite haben und für sie Anonymisierungstechniken und -dienste zur Verfügung stehen; hebt hervor, dass Spenden an politische Parteien unter Verwendung von Kryptowerten dem Grundsatz des bekannten Spenders unterliegen und für sie dieselben Transparenz- und Rechenschaftsstandards wie bei traditionellen finanziellen Zuwendungen gelten sollten; nimmt die Zusage der Kommission zur Kenntnis, unter dem Dach des ECNE und in enger Zusammenarbeit mit anderen EU-Netzen und Interessenträgern nationale Sachverständige zusammenbringen, um bewährte Verfahren auszutauschen, mögliche Leitlinien auszuarbeiten und gemeinsame Maßnahmen zu fördern; fordert die Kommission in diesem Zusammenhang auf, die Umsetzung des Pakets zur Bekämpfung der Geldwäsche und der Verordnung über Märkte für Kryptowerte (MiCAR) weiterhin zu überwachen, um für eine wirksame und konsequente Durchsetzung zu sorgen und etwaige Lücken, die möglicherweise noch in den Rechtsvorschriften bestehen, zu schließen; stellt in dieser Hinsicht fest, dass das Marktintegrations- und Aufsichtspaket den Vorschlag für eine Überarbeitung der MiCAR beinhaltet;

115. fordert die Mitgliedstaaten auf, bewährte Verfahren bei der Kontrolle der Finanzierung politischer Parteien auszutauschen; bringt seine Besorgnis darüber zum Ausdruck, dass manche zentralen Meldestellen nicht über das erforderliche Mandat verfügen, um den zuständigen nationalen und europäischen Behörden Informationen über die Einmischung in Wahlen zu übermitteln; fordert die Kommission auf, zu beurteilen, ob es einen Mehrwert bringt, die Funktion, das Mandat und die Ressourcen der APPF auszuweiten, um die Koordinierung der für die Aufsicht über die Finanzierung politischer Parteien zuständigen nationalen Behörden und EU-Behörden weiter zu verbessern; betont in diesem Zusammenhang, dass die Zusammenarbeit zwischen der APPF und dem ECNE gestärkt werden muss;

Die Rolle von Sanktionen beim Schutz der Demokratie

116. ist der Ansicht, dass Sanktionen gegen Personen sowie staatliche und nichtstaatliche Einrichtungen, die Handlungen mit dem Ziel setzen, die demokratische Integrität der EU oder ihrer Mitgliedstaaten zu beeinträchtigen, eine unverzichtbare Komponente des Instrumentariums des Schutzschildes für die Demokratie darstellen; betont ferner, dass effektive Sanktionen basierend auf objektiven und gleichbleibenden Kriterien angenommen werden und ein umfassendes Maßnahmenpaket beinhalten müssen, darunter das Einfrieren und die Einziehung von Vermögenswerten, eine klare Zuweisung und öffentliche Aufdeckung von Verantwortung, Erhöhungen von Kosten und Einschränkungen von Einnahmen, Einfuhr- und Ausfuhrverbote, Reiseverbote, die Verweigerung des Zugangs zu den Märkten und Finanzsystemen der EU und andere

wirksame, robuste und wirkungsvolle restriktive Maßnahmen; fordert den Rat erneut auf, bei Beschlüssen in Angelegenheiten der Gemeinsamen Außen- und Sicherheitspolitik wie Sanktionen schrittweise zur Beschlussfassung mit qualifizierter Mehrheit überzugehen;

117. fordert, dass die nach der Invasion Russlands in die Ukraine angenommenen EU-Sanktionen effizienter gestaltet werden und ihre Wirkung verstärkt wird, um Russland endgültig daran zu hindern, seinen brutalen Angriffskrieg fortzusetzen und die Sicherheit weiterer Nachbarländer zu bedrohen; fordert die Kommission und die Mitgliedstaaten auf, verhängte Sanktionen regelmäßig und sorgfältig im Hinblick auf optimale Effizienz und eine eventuelle neuerliche Ausweitung zu bewerten, was auch Sanktionen gegen Personen und Einrichtungen, die an der aktiven Umgehung von Sanktionen der EU gegen Russland beteiligt sind, einschließt; ist der Ansicht, dass die EU insbesondere im Bereich der hybriden Bedrohungen und destabilisierenden Aktivitäten durch Russland 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, im Nahen Osten und in Lateinamerika, 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, Sanktionen auf Personen und Einrichtungen aus Drittländern – insbesondere aus China – ausweiten sollte, die für die aktive Umgehung von Sanktionen und die Ermöglichung russischer Operationen verantwortlich sind, 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;
118. ist der Ansicht, dass es ein wichtiger Schritt sein könnte, Einzelpersonen oder Unternehmen als Verantwortliche zu benennen und außerdem die Herkunftsländer zu identifizieren und bekannt zu machen, und so anzuerkennen, dass ein Problem hinsichtlich eindeutig systematischer, vielschichtiger und oft staatlich finanzierter Einflussnahme besteht, 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; fordert die Kommission auf, zu prüfen, ob es angemessen wäre, auch Belarus angesichts seines Risikoprofils und seiner Verbindungen zu den politischen und

wirtschaftlichen Strukturen Russlands in die Liste aufzunehmen; weist darauf hin, dass die neue Verordnung zur Bekämpfung der Geldwäsche erweiterte Möglichkeiten für die Identifizierung und Listung von Drittländern mit hohem Risiko bietet; fordert die Kommission auf, mit Unterstützung der Behörde zur Bekämpfung von Geldwäsche ihre Befugnisse in vollem Umfang zu nutzen, um für die Umsetzung gezielter finanzieller Sanktionen zu sorgen;

119. betont, dass die Wirksamkeit und Glaubwürdigkeit der EU-Sanktionen von einer strengen und konsequenten Durchsetzung abhängen; fordert die Mitgliedstaaten daher auf, einen Mechanismus für die wirksame Überwachung der Durchsetzungsmaßnahmen einzurichten, unter anderem in Form eines Zusammenspiels mit der Zivilgesellschaft und der Wissenschaft zur Verbesserung der Koordinierung und zur Zusammenarbeit, um Schlupflöcher zu schließen und die Verfahren zu harmonisieren; begrüßt die Tatsache, 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; betont, dass die Reform mit einer angemessenen Finanzierung einhergehen sollte, damit die EUSTa ihre erweiterten Aufgaben wirksam erfüllen kann;
120. weist darauf hin, dass das Instrument der EU gegen Zwangsmaßnahmen, das seit 2023 in Kraft ist, ein breites Spektrum von EU-Maßnahmen vorsieht, um den Versuchen von Drittländern entgegenzuwirken, wirtschaftlichen Zwang gegenüber der EU oder einem Mitgliedstaat auszuüben; betont, dass das Instrument gegen Zwangsmaßnahmen Teil einer proaktiven Eskalationsstrategie sein sollte, um auf Bedrohungen zu reagieren, die gegen die territoriale Unversehrtheit Europas und die digitale, regulatorische, finanzielle oder wirtschaftliche Souveränität gerichtet sind; weist darauf hin, dass der Zugang zum Binnenmarkt für Betreiber aus Drittländern von der Einhaltung des EU-Rechts abhängt;
121. verurteilt den politisch motivierten Einsatz von schwarzen Listen, Visumsperren und anderen restriktiven Maßnahmen oder Vergeltungsmaßnahmen durch ausländische Regierungen – nicht zuletzt Russland –, die sich gegen EU-Bürgerinnen und -Bürger, Vertreter von staatlichen Stellen und Handelsorganisationen, Journalisten, Akteure der Zivilgesellschaft, humanitäre Organisationen und politische Amtsträger, einschließlich demokratisch gewählter Mitglieder des Europäischen Parlaments, richten; ist besorgt darüber, dass solche Praktiken, mit denen ungebührlicher politischer Druck auf die Regelungsautonomie der EU und den Rahmen der Grundrechte ausgeübt werden soll, diplomatische Normen und den Grundsatz der gegenseitigen Achtung zwischen den Rechtsordnungen beeinträchtigen; fordert neben diplomatischen Bemühungen eine besser koordinierte und entschlossener 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; betont, dass ein System zur kontinuierlichen Bewertung und laufenden Information der betroffenen Personen eingerichtet werden muss – und zwar insbesondere in Bezug auf die schwarze Liste Russlands, die auch Mitglieder des Europäischen Parlaments und ihre Mitarbeiter sowie EU-Beamte umfasst –, um für Transparenz und Schutz zu sorgen;

Krisenvorsorge der EU

122. begrüßt die Europäische 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; begrüßt Initiativen der Mitgliedstaaten zur Stärkung der gesellschaftlichen Vorsorge, der Zusammenarbeit und der klaren Kommunikation über die Verantwortlichkeiten der Bürgerinnen und Bürger, wie sie in Schweden und Finnland gestartet wurden; betont, dass eine wirksame Vorsorgepolitik auf Inklusion über alle Altersgruppen, Gemeinschaften sowie sozialen und wirtschaftlichen Gruppen hinweg beruhen muss; hebt in diesem Zusammenhang die Funktion von Unternehmen, Verbänden und sachkundigen Einzelpersonen als Stütze grundlegender Dienst- und Versorgungsleistungen hervor; betont, dass die Bürgerinnen und Bürger für tatsächliche zivile Resilienz einbezogen und darüber aufgeklärt werden müssen, wie und wann sie einen Beitrag leisten können;
123. fordert die Erstellung eines jährlichen, öffentlich zugänglichen Tätigkeitsberichts der EU über den allgemeinen Stand der Vorsorge in der gesamten EU, der einen umfassenden strukturierten Überblick für jeden Mitgliedstaat beinhaltet; betont, dass in diesem Bericht unter anderem die institutionelle Bereitschaft, der Stand der zivil-militärischen Zusammenarbeit, strategische Fähigkeiten, Präventivmaßnahmen, Reaktionsmechanismen, Schwachstellen und wichtige Trends behandelt werden könnten, wobei Erwägungen der nationalen Sicherheit zu berücksichtigen sind; unterstreicht, dass dieser Bericht zum Austausch bewährter Verfahren beitragen und als Orientierungs- und Beratungsinstrument für die Umsetzung der Vorsorgestrategien der Mitgliedstaaten dienen könnte; hält fest, dass geprüft werden sollte, ob das Europäische Zentrum für demokratische Resilienz eine koordinierende Rolle bei der Ausarbeitung dieses Berichts spielen könnte;

124. fordert die rasche Entwicklung und Einführung einer EU-weiten, interoperablen Krisenwarn-App, die den in der EU niedergelassenen Personen in Notfällen zuverlässige und mehrsprachige Informationen in Echtzeit zur Verfügung stellt; empfiehlt, dass diese App in nationale und EU-Frühwarnsysteme integriert wird, für alle Personen – mit besonderem Schwerpunkt auf schutzbedürftigen Gruppen – zugänglich gemacht und regelmäßig entsprechend dem technologischen Fortschritt und im Einklang mit bewährten Verfahren des Krisenmanagements aktualisiert wird;
125. 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;
126. fordert die Organisation regelmäßiger groß angelegter, von der EU koordinierter Übungen zur Krisenvorsorge, an denen die EU-Organe, die EU-Agenturen, die Mitgliedstaaten, regionale und lokale Behörden, der Privatsektor und die Zivilgesellschaft beteiligt sind; ist der Ansicht, dass die Vorbereitung auf Szenarien, die von Überschwemmungen, Waldbränden, Erdbeben und medizinischen Notfällen bis hin zu chemischen, biologischen, radiologischen und nuklearen Vorfällen reichen, möglicherweise auch dazu beiträgt, die Fähigkeit Europas zu stärken, Bedrohungen – wie sie beispielsweise bei der Aggression Russlands gegen die Ukraine und bei hybriden Angriffen auf ganz Europa zutage getreten sind – zu verhindern, ihnen standzuhalten und auf sie zu reagieren; empfiehlt bei diesen Übungen Simulationen von komplexen und realistischen Szenarien durchzuführen, wie beispielsweise von Cyberangriffen, Störung kritischer Infrastruktur, koordinierten Desinformationskampagnen und hybriden Krisen, um die Reaktionskapazitäten zu beurteilen, die Interoperabilität zwischen den Regierungs- und Verwaltungsebenen zu verbessern, bewährte Verfahren auszutauschen und eine Krisenvorsorgekultur auf allen Ebenen zu fördern; betont in diesem Zusammenhang, dass EU-Initiativen zur militärischen Mobilität auch im Hinblick auf die zivile Vorsorge und die Fähigkeit, Hilfsgüter in Notfällen zu transportieren, in hohem Maße relevant sind; fordert außerdem die Einführung eines Europäischen Tags der Krisenvorsorge; schlägt als Tag für diesen Anlass den 24. Februar vor – das Datum der unprovokierten groß angelegten militärischen Invasion Russlands in die Ukraine im Jahr 2022 –, was als Symbol für

die Solidarität der EU mit der Ukraine dienen und daran erinnern soll, dass eine verstärkte zivile und militärische Vorsorge gegen die zunehmenden Bedrohungen durch autoritäre Regime dringend vonnöten ist;

127. fordert die Kommission auf, die Möglichkeit zu prüfen, Erasmus+ oder ähnliche Programme auf grenzüberschreitende Initiativen zu Krisenvorsorgeschulungen von Beschäftigten in kritischen Sektoren wie Feuerwehrleuten, Arbeitskräften im Gesundheitswesen oder freiwilligen Katastrophenschutz Helfern, 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;
128. fordert die beschleunigte Einführung sicherer Kommunikationssysteme, wie IRIS² und des Europäischen Systems für kritische Kommunikation, aufbauend auf bereits bestehenden Systemen auf Ebene der Mitgliedstaaten; 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 Infrastruktur durch harmonisierte Frequenzgenehmigung, Cybersicherheitszertifizierung und Maßnahmen zur Sicherung der IKT-Lieferkette im Einklang mit den Vorschlägen der Kommission für eine Verordnung über digitale Netze und einen Rechtsakt zur Cybersicherheit sichergestellt werden;
129. fordert eine verstärkte Koordinierung zwischen den Organen, Einrichtungen und sonstigen Stellen der EU, den Mitgliedstaaten und den gleichgesinnten 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; hebt in diesem Zusammenhang hervor, dass Vorsorge und Resilienz in die kollektive Verantwortung fallen und daher die Gesellschaft beteiligt sein muss;
130. 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; hält fest, dass in speziellen Finanzierungsströmen auch lokalen Krisenvorsorgemaßnahmen Vorrang eingeräumt werden sollte, insbesondere in den Gebieten, die am stärksten gefährdet und hybriden Bedrohungen – vor allem Informationskriegsführung – besonders ausgesetzt sind;

131. empfiehlt den Entscheidungsorganen der EU, die Strategien und Notfallpläne zu überprüfen und zu optimieren, die sie im Fall eines offenen militärischen Angriffs gegen einen oder mehrere Mitgliedstaaten und in ähnlichen Krisenszenarien umsetzen würden, was auch die Aktivierung von Artikel 42 Absatz 7 EUV umfasst; betont ferner, dass in allen Organen, Einrichtungen und sonstigen Stellen der EU ein Höchstmaß an Sicherheit und Gefahrenabwehr sichergestellt sein muss, auch im Bereich der Cybersicherheit sowie der Sicherheit und Integrität von Informationen, und dass die in dieser Hinsicht erforderlichen Voraussetzungen geschaffen werden müssen, darunter die Einrichtung anerkannter sicherer Kommunikationskanäle und geeigneter Sitzungssäle für Sitzungen unter Ausschluss der Öffentlichkeit; unterstreicht, dass die Vorschriften über Verstöße gegen die Sicherheit und Vertraulichkeit von Informationen – unter anderem durch effektive Ermittlung und strafrechtliche Verfolgung solcher Verstöße – streng durchgesetzt werden müssen, insbesondere vor dem Hintergrund eines erhöhten Risikos von Spionage und Sabotage; fordert in diesem Zusammenhang eine regelmäßige Prüfung der Schwachstellen und Abhängigkeiten – insbesondere im digitalen Raum – in allen Organen, Einrichtungen und sonstigen Stellen der EU; betont, dass hybride Bedrohungen auch abseits von offenen militärischen Konflikten nach wie vor wachsende Risiken für das tägliche Funktionieren der EU darstellen;
132. begrüßt die Bemühungen der Kommission, die physische Sicherheit und die Informationssicherheit innerhalb der Organe, Einrichtungen und sonstigen Stelle der EU zu stärken, wie in der Mitteilung des Managementkontrollgremiums vom Oktober 2025 dargelegt ist – was Pläne für sichere Sitzungssäle, verbesserte Verfahren für die Sicherheitsüberprüfung von Bediensteten, die Verschlusssachen bearbeiten, und die Einrichtung des Sicherheitskollegs zur Bereitstellung regelmäßig aktualisierter Informationen zu Bedrohungsentwicklungen einschließt; 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 Union⁷⁰; 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; begrüßt die Tätigkeit des IT-Notfallteams für die Organe, Einrichtungen und sonstigen Stellen der EU (CERT-EU) und weist mit Nachdruck darauf hin, dass es über ausreichende Haushaltsmittel und eine angemessene Personalausstattung verfügen muss;

133. empfiehlt weitere Maßnahmen zur Stärkung der Sicherheit des Parlaments, seiner Widerstandsfähigkeit gegenüber Einflussnahme aus dem Ausland und seiner Fähigkeit, in Krisen effektiv zu arbeiten, darunter auch verstärkte Unterstützung der Mitglieder und der Bediensteten durch IT- und Sicherheitskontrollen, gezielte Schulungen, Briefings vor Dienstreisen und interdisziplinäre Maßnahmen zum Aufbau von Widerstandsfähigkeit, in die die Themen physische Sicherheit, Informationssicherheit und Cybersicherheit einfließen; betont, dass sein Cybersicherheitsrahmen im Einklang mit der Cybersicherheitsverordnung weiterentwickelt und die operative Reife verbessert werden muss sowie die Fähigkeiten zur Erkennung von Bedrohungen in einem sich wandelnden technologischen Umfeld und einer veränderlichen Bedrohungslage gestärkt werden müssen, während gleichzeitig gezieltere Schulungen für Bedienstete zur Bekämpfung von Informationsmanipulation angeboten und strengere Sicherheitsüberprüfungen für Sitzungen und Missionen mit sensiblen Inhalten erfolgen müssen; stellt fest, dass die Nutzung privater mobiler Geräte und Laptops für die parlamentarische Arbeit eine potenzielle Schwachstelle darstellt, und betont, dass Mitglieder und Bedienstete mit sicheren vom Organ bereitgestellten Geräten ausgestattet sein sollten; begrüßt das bestehende freiwillige Screening auf Spähsoftware und fordert dessen systematische Ausweitung auf alle Geräte, die für die parlamentarische Arbeit verwendet werden; fordert außerdem die Kommission und den EAD auf, das Parlament systematisch in ihre Vorsorgemaßnahmen und

⁷⁰ Vorschlag der Kommission vom 23. März 2022 für eine Verordnung des Europäischen Parlaments und des Rates über die Informationssicherheit in den Organen, Einrichtungen und sonstigen Stellen der Union (COM(2022)0119).

Übungen, wie die Übung „EU Integrated Resolve“, einzubeziehen;

◦

◦

◦

134. beauftragt seine Präsidentin, diese EntschlieÙung 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.